Actes du colloque

« *Raisonner en arithmétique. Est-ce incongru ?* »

Raisonner en arithmétique.

Est-ce incongru ?

Préface

C'est avec un très grand intérêt et beaucoup de plaisir qu'en tant que présidente de l'Adirem j'ai pu participer à ce colloque des Commissions Inter-IREM Collège et Lycée sur Raisonner en arithmétique. En tant que directrice de l'IREM d'Aquitaine, j'ai aussi été ravie que cela se passe à Bordeaux : l'Institut de Mathématiques de Bordeaux est en effet un lieu de recherche très important sur la théorie des nombres. L'arithmétique est en effet un thème extrêmement riche :

- Comme l'indique le titre du colloque, on peut l'aborder à tous les niveaux : dès qu'on commence à additionner et multiplier, on fait déjà de l'arithmétique. La notion de facteurs premiers et de PGCD peut ensuite être utile lorsqu'on additionne des fractions au collège. Au lycée, l'étude des relations de congruence permet de parler de cryptographie.
- Dès l'école primaire, les élèves peuvent naturellement faire des conjectures en observant leurs tables de multiplication, et seront déjà confrontés à des résultats importants.
- C'est aussi un thème historiquement très riche : de l'Antiquité et Euclide, à la cryptographie moderne.
- C'est de plus un sujet de recherche toujours actif, dans lequel certaines questions encore ouvertes peuvent être posées avec un vocabulaire accessible à des collégiens.
- Les raisonnements y sont très variés (disjonction de cas, récurrence, absurde,...) et accessibles pour les élèves. On raisonne sur les nombres, qui sont des objets avec lesquels ils sont bien familiers.
- C'est un magnifique exemple d'une recherche théorique qui s'est développée pour la beauté du savoir pendant des siècles, avant de trouver des applications énormes actuellement, que personne n'aurait pu prédire il y a un siècle.
- Les mathématiciens bordelais le savent bien, puisque l'équipe de théorie des nombres était à l'origine le laboratoire A2X pour Laboratoire d'Algorithmique Arithmétique Expérimentale, l'arithmétique a beaucoup de lien avec l'informatique ! Et bien avant les ordinateurs, il était déjà pertinent de chercher un algorithme pour répondre à des questions d'arithmétique (algorithme d'Euclide, crible d'Eratosthène…).

J'aimerais remercier ici les deux commissions Inter-IREM qui ont su mettre au point un programme qui montre bien toute cette richesse. Ainsi les conférences ont été l'occasion d'entendre parler d'arithmétique bien sûr, en lien avec la didactique et le raisonnement, avec la logique, avec l'algorithmique, avec l'histoire des mathématiques et avec la cryptographie. On peut également remercier ces conférenciers pour la grande qualité de leurs exposés.

Les ateliers sur des thèmes variés, allant du cycle 3 à l'université, ont été l'occasion de nombreux échanges montrant bien l'intérêt des collègues pour ce sujet. Enfin, même si leur travail était en grande partie invisible des participants, je voudrais saluer l'énergie et le temps qu'ont consacré les secrétaires de l'Unité de Formation Mathématiques et Interactions de Bordeaux pour l'organisation du colloque, leur aide a été précieuse.

Si vous avez eu la chance d'assister à ce colloque, ces actes seront pour vous l'occasion de vous replonger dans ces conférences. Sinon, vous pourrez découvrir grâce à Véronique Battie ce que la didactique peut nous dire sur l'intérêt d'utiliser l'arithmétique pour apprendre à raisonner. Vous aurez le

plaisir de lire ce que René Cori a à nous apprendre sur les axiomes de Peano et d'apprendre grâce à Jean-Michel Muller comment les ordinateurs font de l'arithmétique. Vous pourrez aussi grâce à Marc Moyon lire des textes historiques et vous exercer à résoudre les problèmes qu'ils exposent. Enfin vous verrez grâce à Daniel Perrin que les propriétés des nombres premiers utiles en cryptographie peuvent être abordées dès le collège. Enfin, que vous soyez intéressé par l'histoire ou la cryptographie, que vous soyez enseignant dans le premier degré, le second degré ou le supérieur, vous trouverez de quoi satisfaire votre curiosité dans les présentations des ateliers.

Enfin, ce colloque a été pour moi l'occasion, une fois de plus, de constater le formidable outil que sont les IREM : d'une part, ils permettent de rassembler des enseignants de tous niveaux, pour échanger et partager leurs pratiques. Surtout, les ateliers, qui présentent souvent des activités développées dans le cadre de groupes IREM, ont bien montré la qualité de ces travaux. Il faut souligner qu'une bonne partie des ateliers ont été présentés par des enseignants non universitaires. Et si vous êtes intéressé par réfléchir en groupe, sur un temps qui peut être long, sur une thématique, si vous voulez concevoir et tester des activités, les IREM sont là pour vous, n'hésitez pas à nous rejoindre !

Bonne lecture à vous !

Marie-Line Chabanol

Remerciements :

Les commissions Inter-IREM collège et lycée remercient les partenaires pour l'organisation du colloque :

SOMMAIRE

A01 page 114	Laurent Frédéric	L'arithmétique, c'est tout une histoire!
A05 Page 130	Vinatier Stéphane	Conjectures et preuves
A06 Page 146	Damamme Gilles	Calculer une approximation de √2 par des rationnels en faisant du découpage
A07 Page 152	Vandebrouck Fabrice	Raisonner avec le Puzzle de la Division Euclidienne
A08 Page 166	Thomas Meyer	Une activité autour des nombres de Sophie Germain
A10 Page 176	Roux Aurélie et Foulquier Laurianne	Entrée dans la preuve en arithmétique : Un exemple d'usage de la situation du plus grand produit
A11 Page 192	CII Collège	Pièces de Monnaies : Diop
A12 Page 200	Cortella Anne	Raisonner en arithmétique dans un tour de magie: le tour de Gergonne
A13 Page 212	Durand Sébastien et Julien Lavolé	Une activité de modélisation collaborative de problèmes entre classes : Les vitres ", groupe Resco
A14 Page 230	Metin Frédéric	Méthodes et pratiques arithmétiques du XVIe siècle
A15 Page 252	Gardes Denis et Bernard Dominique	Arithmétique et raisonnements mathématiques
A17 Page 280	Gilbert Thérèse et Zimmer Daniel	Conjecturer, débattre, raisonner en arithmétique, en formation initiale des enseignants et au collège
A18 Page 292	Pourtier Jean-Charles	Utilisation du boulier chinois
A19 Page 306	Page Aurel	Cryptologie
AJ1 Page 354	Orozco Jean-Marc et Licitri Timothée	Les jeux du commerce
AJ2 Page 316	Althuisius Laurence	Les jeux revisités
AJ3 Page 317	Audoin Alexandre	Turing Machine
AJ4 Page 318	Schottel Ambre et Darnis Marlène	Escape game « les mystères de la divisibilité
AJ5 Page 320	Muller Anne-Claire	Escape game « Le secret de la bibliothèque »

Comité scientifique

Caroline BULF - Maîtresse de Conférences en didactique des Mathématiques à l'INSPE de l'académie de Bordeaux, Lab E3D, université de Bordeaux

Xavier CARUSO - Directeur de recherche en Mathématiques au CNRS, IMB, université de Bordeaux

Marie-Line CHABANOL – Maîtresse de Conférences en mathématiques à l'Université de Bordeaux, IMB, directrice de l'IREM d'Aquitaine, présidente de l'ADIREM

Anne CORTELLA – Maîtresse de Conférences en mathématiques à l'Université de Montpellier, IMAG, IRES de Montpellier

Laurianne FOULQUIER – Formatrice, INSPE, Université de Bordeaux, IREM d'Aquitaine, Co-responsable Commission Inter-Irem Collège

Guillaume FRANCOIS – Professeur certifié de Mathématiques, formateur, INSPE, Université de Nantes, IREM de Nantes, Co-responsable Commission Inter-Irem Lycée

Christian JUDAS – Professeur certifié de Mathématiques, IREM de Nantes, Co-responsable commission inter-Irem collège

Philippe LAC – Professeur agrégé de Mathématiques, Co-responsable Commission Inter-Irem Lycée

Chantal MENINI – Maîtresse de Conférences en mathématiques à l'Université de Bordeaux, IMB, IREM d'Aquitaine

Comité d'organisation

CII Collège :

Laurianne FOULQUIER – Formatrice, INSPE, Université de Bordeaux, IREM d'Aquitaine, Co-responsable Commission Inter-Irem Collège

- Maëlle JOURAN – Professeure certifiée de Mathématiques, IREM de Rouen

- JUDAS Christian – Professeur certifié de Mathématiques, IREM de Nantes, Co-responsable commission inter-Irem Collège

- Patricia LAMBERT – Formatrice, INSPE, Université de Bordeaux, IREM d'Aquitaine

- LANATA Fabienne – Professeure certifiée de Mathématiques, IREM de Rouen

- PAILLET Vincent – Chef de projet à la DEPP B2.1

- ROUX Aurélie - Formatrice, INSPE, Université de Clermont-Auvergne, IREM de Clermont-Ferrand

CII Lycée :

- FRANÇOIS Guillaume – Professeur certifié de Mathématiques, formateur, INSPE, Université de Nantes, IREM de Nantes, Co-responsable Commission Inter-Irem Lycée

- LAC Philippe - Professeur agrégé de Mathématiques, Co-responsable Commission Inter-Irem Lycée

IREM d'aquitaine :

- CASTAGNOS Nadine - Professeure agrégée de Mathématiques, IREM d'Aquitaine

- CHABANOL Marie-Line – Maîtresse de Conférences en mathématiques à l'Université de Bordeaux, IMB, directrice de l'IREM d'Aquitaine, présidente de l'ADIREM

- GARCIA Adelyne – Référente administrative et financière, UFMI, Université de Bordeaux

- HOCQUARD Hervé – Professeur d'Université, LABRI, Université de Bordeaux, IREM d'Aquitaine

CONFÉRENCES

ARITHMÉTIQUE AU COLLÉGE ET AU LYCÉE : AUTOUR DE LA CRYPTOGRAPHIE ET DES NOMBRES PREMIERS

Daniel PERRIN
Professeur Honoraire
Université Paris-Sud, Orsay
daniel.perrin@universite-paris-saclay.fr

Ce texte est la rédaction d'une conférence faite le 15 juin 2023 lors du colloque : *Raisonner en arithmétique. Est-ce incongru ?* organisé par les commissions Inter-IREM collège et lycée. Je remercie les organisateurs de m'avoir invité à faire cette conférence et particulièrement Laurianne et Patricia pour leur gentillesse, leur dévouement et leur efficacité.

I - CRYPTOGRAPHIE ET NOMBRES PREMIERS

Cette partie est reprise d'une conférence que j'ai faite plus de quatre-vingt fois devant des publics divers : collégiens, lycéens, grand public, notamment lors de la fête de la science, etc. On en trouve des rédactions variées sur ma page web et quelques vidéos sur You Tube.

1. Les nombres premiers : inutiles?

La question de l'utilité des mathématiques est l'une de celles que les collégiens et les lycéens posent le plus souvent et il n'est pas toujours facile d'y répondre, notamment dans le cas de l'arithmétique, dont on a longtemps pensé qu'elle ne servait à rien, témoin ce qu'en dit Descartes dans une lettre à Mersenne datant de 1638 :

Pour ce que les questions d'arithmétique peuvent quelquefois mieux être trouvées par un homme laborieux qui examinera opiniâtrement la suite des nombres, que par l'adresse du plus grand esprit qui puisse être, et que d'ailleurs elles sont très inutiles, je fais profession de ne vouloir pas m'y amuser.

C'est même l'opinion d'un grand spécialiste du sujet, le mathématicien anglais[1] G.H. Hardy, pourtant spécialiste de théorie des nombres (dans une conférence faite en 1915) :

La théorie des nombres a toujours été perçue comme l'une des branches les moins utiles des Mathématiques Pures. On ne pourra guère contester cette accusation, encore moins lorsqu'elle vise les parties de la théorie plus particulièrement liées aux nombres premiers. Une science est qualifiée d'utile si son développement contribue à accentuer les inégalités dans la répartition des richesses ou, lorsqu'il promeut plus directement la destruction de la vie humaine. La théorie des nombres premiers ne vérifie pas de tels critères. Ceux qui l'explorent ne tenteront pas, si toutefois ils sont doués de sagesse, de justifier l'intérêt qu'ils portent à un sujet si futile et isolé.

D'ailleurs, moi-même, à la question : *à quoi servent les nombres premiers ?* j'aurais sans doute répondu en 1970 : à rien, on les étudie *pour l'honneur de l'esprit humain* (comme disait Jacobi vers 1850) et j'aurais peut-

[1] On appréciera l'humour britannique.

être ajouté, comme aurait pu dire notre collègue Roger Godement (mort en juillet 2016) : *au moins, quand on fait de l'arithmétique*[2]*, on ne travaille pas pour la bombe atomique !* Eh bien, nous aurions dit une bêtise, comme l'invention du code RSA le montrera peu après ...

2. La cryptographie

La cryptographie (du grec crypto, caché et graphie, écrire), est la science des codes secrets. Le premier dont l'histoire atteste qu'il utilisait de tels codes est Jules César, qui employait un système d'alphabets décalés. Ainsi, on pourrait imaginer qu'il envoya au Sénat, au soir de la bataille de Zela, le communiqué sibyllin suivant : *TCLG TGBG TGAG* ...

Ce type de codage, ou chaque caractère du message originel correspond à un et un seul caractère du message codé, est appelé codage par substitution. En voici un exemple très simple. Supposons que l'on soit en difficulté et qu'on veuille envoyer un message pour demander du secours, sans que l'ennemi puisse comprendre. On part du message : A L' AIDE, que l'on transcrit[3] en chiffres en remplaçant chaque lettre par son rang dans l'alphabet : 1 12 1 9 4 5, puis, par un procédé ultra-secret et très difficile à décrypter (sic), on code ce message en : 25 14 25 17 22 21 et on peut ensuite le retranscrire en lettres : Y N Y Q V U.

Bien entendu, contrairement à ce que j'ai affirmé ci-dessus, le codage est très facile à déchiffrer, mais, et c'est un point essentiel, même sur un message aussi court, on voit apparaître ce qui va être le défaut rédhibitoire de ce type de codage : la lettre A, deux fois présente dans le message initial, est codée par Y qui apparaît aussi deux fois dans le message final : les fréquences sont conservées. Cela permet de déchiffrer aisément ce type de codage[4], comme on le sait depuis le tragique épisode de Marie Stuart que je relate maintenant.

Marie Stuart est une princesse écossaise, brièvement reine de France (1559-1560, c'était l'épouse de François II) puis reine d'Ecosse. A cette époque, l'Écosse et l'Angleterre étaient ennemies et Marie est capturée par la reine d'Angleterre Élisabeth première en 1568. En 1586 elle participe de sa prison à un complot contre Élisabeth et communique avec ses partisans au moyen de messages codés. Mais son code est décrypté par le linguiste flamand Thomas Phelippes, par la méthode d'analyse de fréquences. Cela permet à Élisabeth de traduire Marie en justice en l'accusant de complot. Elle est condamnée à mort et décapitée en 1587. On pourra consulter, sur ce sujet, http://codes.secrets.free.fr/stuart/stuart5.htm

Pour comprendre la méthode, un exemple littéraire va nous éclairer, il s'agit de la nouvelle *Le scarabée d'or* d'Edgar Poe. Dans ce texte, le personnage principal, William Legrand, décrypte un message du capitaine Kidd (un pirate du XVIII-ième siècle) indiquant l'emplacement d'un trésor. Voici le message :

53‡‡+305))6* ;4826)4‡4‡) ;806* ;48+8 960))85 ;1‡(; :+*8+83(88)5*+ ;46(;88*96 * ? ;8)*‡(;48
5) ;5*+2 :*‡(;4956*2(5*-4)8 98* ;4069285) ;)6+8)4‡‡ ;1(‡9 ;48081 ;8 :8‡ 1 ;48+85 ;4)485+5288
06*81(‡9 ;48 ;(88 ;4 (‡ ?34 ;48)4‡ ;161 ; :188 ;‡ ? ;

[2] Godement disait plutôt cela à propos des groupes d'homotopie des sphères, mais l'idée est la même.

[3] Ce n'est pas du tout ainsi qu'on procède en réalité pour numériser les messages. On peut utiliser par exemple le code ASCII.

[4] Bien qu'on sache depuis 1580 que ce genre de code est vulnérable, il a cependant été utilisé depuis, par les généraux sudistes lors de la guerre de sécession (1861-1865), par les troupes russes au début de la guerre de 1914-1918 et par le mafioso sicilien Bernardo Provenzano en 2006, ce qui a permis son arrestation.

Legrand note d'abord que, comme Kidd est anglais, le message est sans doute écrit dans cette langue. Ensuite, il utilise le fait qu'en anglais, les lettres n'apparaissent pas toutes avec la même fréquence, la plus courante étant E. Comme c'est le signe 8 qui est le plus fréquent dans le message, il en infère qu'on a 8=E et continue ainsi avec les autres lettres. Il constate aussi la présence de plusieurs groupements ; 48 dans le message. Un mot de trois lettres se terminant par E et fréquent en anglais, il n'est pas besoin d'être grand clerc pour penser qu'il s'agit de THE, ce qui donne ;=T et 4=H, etc. Bien entendu, à la fin, il trouve le trésor.

Le lecteur qui voudrait s'exercer déchiffrera le texte suivant[5] :

SALCFCFVHLCNEANVHHPLGNZIPUUANAKNRNHHLBNCFVHNYOANEGLYHKNZKVSOANHU NARNGNHZLHHNVAHGNZFGNHHNZANOHUALYZLPHKNHNHMPFYHYFYOMKVHTVLSPNY HNONYPA UNKPZPOLOPFYH en sachant que les lettres les plus fréquentes en français sont, dans l'ordre : E S A R I N T U O L

Attention, ces fréquences sont statistiques et dans un vrai texte il peut, par exemple, y avoir plus de T que de N.
J'ai moi-même été mis en difficulté par les élèves d'une classe de sixième du collège Alain Fournier à Orsay, qui avaient travaillé sur ce thème et m'avaient envoyé un message codé dont voici la traduction :

Jadis vivait un garçon, dans un camping-car, dans un bois. Il n'avait pas un sou. Mais il avait un voisin. Franck avait un chaton blanc, qui adorait dormir. Pour nourrir son chaton, il ramassa un abricot. Alors Franck a vu son voisin sortir son chiot, jusqu'à un marchand d'animaux pour avoir un chat. Puis alla au parc où il trouva un ami fictif, Yoan. Yoan lui raconta alors sa fiction. Un jour Yoan, alors rugbyman cassa sa FIAT, alors qu'il finissait son rugby match. Il prit donc un taxi. Joris, un ami, qui finissait lui son triathlon, l'aida. Un soir, Romain, un larron, cambriola Yoan, donc il alla au QG du FBI dans un hall pour dormir. Il faisait doux.

J'ai mis un certain temps à comprendre qu'il s'agissait d'un texte « à la Perec », c'est-à-dire sans la lettre E! Inutile de dire qu'ESARINTUOL n'est plus la bonne clé. Pour la trouver on peut faire une statistique sur le livre *La disparition* de Georges Perec, livre de 319 pages, dans lequel ne figure jamais la lettre E.

3. Le code RSA

3.1. Définition

Comme on l'a vu avec l'exemple de Marie Stuart[6], l'histoire de la cryptographie est une longue bataille entre codeurs et déchiffreurs. La problématique qui sous-tend la création du code RSA est la suivante.

Imaginons un espion E, loin de son pays et de son chef C. Il doit transmettre des messages secrets à C. Pour cela, il a besoin d'une clé[7] pour coder ses messages. Cette clé doit lui être transmise par son chef. Le problème, de nos jours, avec tous les satellites espions, c'est qu'on n'est pas sûr du tout que les ennemis n'écoutent pas les messages transmis. Or, avec la plupart des systèmes de codage, si l'on connaît la clé de codage, on sait aussi décoder les messages. Par exemple, imaginons que la clé soit l'opération qui, à une lettre, représentée par un nombre x modulo 26, associe $11x - 7$ (toujours modulo 26), ce qui associe par

[5] D'autres sont donnés en annexe.

[6] Voir aussi le décryptage du code de la machine Enigma des Allemands par Alan Turing pendant la seconde guerre mondiale.

[7] Par exemple, le message SALCFCF…proposé ci-dessus a été codé avec la clé : $x \to 7x+5$ modulo 26.

exemple à la lettre E la lettre V . On calcule alors facilement l'opération inverse[8], ce qui permet de décoder les messages.

Tout l'intérêt du code RSA, inventé en 1978 par Rivest, Shamir et Adleman, c'est, au contraire, qu'il est à sens unique : même si l'on connaît la clé de codage on n'en déduit pas une clé de décodage ! Voici le principe de cette méthode.

Le chef C calcule deux grands nombres premiers p et q (de nos jours, des nombres de l'ordre de 200 chiffres sont nécessaires), il calcule ensuite le produit pq (cela ne représente qu'une fraction de seconde pour une machine). Il choisit aussi un nombre e premier avec $p-1$ et $q-1$ (il y en a beaucoup, par exemple un nombre premier qui ne divise ni $p-1$ ni $q-1$). Il transmet à E la clé de codage, qui est constituée du nombre pq et du nombre e (mais il garde jalousement secrets les deux nombres p et q). La clé est **publique** : peu importe si l'ennemi l'intercepte. Pour coder le message, E n'a besoin que pq et de e, en revanche, pour le décoder, le chef C a besoin des deux nombres p et q. Le principe qui fonde le code RSA c'est qu'il est beaucoup plus facile de fabriquer de grands nombres premiers p et q (et de calculer pq) que de faire l'opération inverse qui consiste à décomposer le nombre pq en le produit de ses facteurs premiers.

Voici précisément la méthode de codage. Le message est un nombre $a < pq$ et premier[9] avec p et q. Pour le coder, E calcule a^e modulo pq (le reste b de a^e dans la division par pq). Là encore, une machine fait cela instantanément, voir ci-dessous. C'est ce nombre b qu'il envoie à son chef.

Comment faire pour retrouver a à partir de b ? Nous l'expliquons en détail au paragraphe suivant. L'idée est la suivante : comme e est premier avec $p-1$ et $q-1$, le théorème de Bézout montre qu'il existe un nombre d tel que $de \equiv 1 \pmod{(p-1)(q-1)}$. On montre que grâce à ce d on peut calculer a en faisant l'opération à l'envers : $a = b^d \pmod{pq}$. Il suffit donc de calculer d. Quand on connaît $(p-1)(q-1)$, trouver d est facile (c'est l'algorithme d'Euclide). Mais voilà : on a $(p-1)(q-1) = pq - p - q + 1$ et pour connaître ce nombre il nous faut $p+q$, donc p et q, mais, pour des nombres de cette taille (400 chiffres) on ne sait pas retrouver p et q à partir de leur produit pq et c'est ce qui assure la sécurité du code RSA. Pour illustrer notre propos, voici un exemple d'un nombre pq de 65 chiffres :

33263290819929542686848148817697305155927928386133083389000759099 7

Le logiciel SAGE répond instantanément qu'il n'est pas premier. En revanche, pour le factoriser, il met environ 20 secondes.

3.2. Quelques résultats arithmétiques

Rappelons d'abord le petit théorème de Fermat (voir par exemple [1] ou **3.14** ci-dessous) :

1.1 Théorème. *Soient p un nombre premier et $a \in \mathbb{Z}$. Alors p divise $a^p - a$ donc on a $a^p \equiv a$ modulo p. Si de plus a est premier avec p, on a $a^{p-1} \equiv 1 \pmod{p}$.*

[8] C'est $x \to 7x+3$, exercice.

[9] Pour être sûr de réaliser cela on prendra des messages plus petits que p et q. Par exemple si pq a 400 chiffres, on prendra des messages de moins de 200 chiffres. Ce seront des messages élémentaires, il en faudra sans doute plusieurs pour faire un message réel.

On a un corollaire de ce théorème :

1.2 Corollaire. *Soient p et q deux nombres premiers distincts et soit a premier avec pq. Alors on a* $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Démonstration. Il suffit de montrer que la congruence est vraie modulo p et modulo q. Pour cela on note que, comme $a^p - 1$ est congru à 1 modulo p, on a aussi $a^{(p-1)(q-1)} = (a^p - 1)^{q-1} \equiv 1^{q-1} = 1 \pmod{p}$. On procède de même pour q.

Le résultat suivant concerne encore les congruences (et c'est aussi la recette pour résoudre des équations du genre $ax \equiv b \pmod{s}$) :

1.3 Proposition. *Soit s un entier > 0 et soit e un entier > 0 premier avec s. Alors il existe un entier d > 0 tel que* $de \equiv 1 \pmod{s}$.

Démonstration. On applique le théorème de Bézout à s et e : il existe des entiers λ et μ avec $\lambda s + \mu e = 1$. Si μ est > 0 il suffit de poser $d = \lambda$. Sinon, on remplace μ par $\mu + sk$ et λ par $\lambda - ek$ avec k assez grand.

Enfin, le dernier résultat est la base de la méthode RSA :

1**.4 Proposition**. *Soient p et q deux nombres premiers distincts et soit a > 0 premier avec pq. Soit e un entier > 0 premier avec* $(p-1)(q-1)$ *et soit d > 0 tel que de soit congru à 1 modulo* $(p-1)(q-1)$ *(un tel entier existe par* ***1.3****).*
Alors, on a $a^{de} \equiv a \pmod{pq}$.

Démonstration. On a $de = 1 + m(p-1)(q-1)$, avec $m > 0$, donc, en vertu de **1.2** :

$$a^{de} = a \times a^{(p-1)(q-1)m} \equiv a \times 1^m = a \pmod{pq}:$$

3.2. Méthodes de calcul

Pour mettre en œuvre le code RSA on a besoin de calculer des puissances modulo pq. Bien entendu, si les nombres sont grands, pour calculer $a^e \pmod{pq}$ on ne peut pas commencer par calculer la puissance, puis la réduire modulo (pq). En effet, le nombre a^e dépasse très vite la capacité des ordinateurs. Une première méthode consiste à réduire modulo (pq) à chaque pas : on calcule a^2, on réduit : $a^2 \equiv b^2 \pmod{pq}$, puis on calcule ab^2, on réduit, etc. Il est très facile d'écrire un programme utilisant cette procédure. En voici un écrit avec le logiciel SAGE[10] :

```
def pw(a,e,p) :
z=1
for k in [1..e] : z= a*z%p
return z
```

[10] Qui utilise le langage Python.

Cette méthode est déjà bien meilleure, mais pas encore optimale. Une méthode plus astucieuse consiste à utiliser les puissances de 2. Elle combine deux types d'opérations simples : l'élévation au carré et la multiplication par a. Le lecteur pourra l'expérimenter en calculant (de tête) 23^{19} modulo 101.

Voici le programme correspondant sur SAGE[11] :

```
def pwr(a,e,p) :
z=1
while e!=0 :
if e%2==0 :
   e=e/2 ; a = a² %p
else :
  e=(e-1)/2 ; z=z*a%p ; a = a² %p
return z
```

Ce programme mérite un mot d'explication. On cherche $b := a^e \pmod p$. On entre a, e, p et on pose $z = 1$. On a donc $a^e z = a^e = b$. Dans le programme, les quantités a, e, z évoluent de telle sorte que $a^e z$ reste constant. En effet, si e est pair, z ne change pas, a devient a^2 et e devient e/2, donc $a^e z$ est invariant. Si e est impair, $e = 2k + 1$, a devient a^2, e devient k et z devient az, donc $a^e z$ devient $(a^2)^k \times az = a^{2k+1}\, z = a^e z$.
À la dernière _étape on a $e = 0$, donc $a^e z = z$ et cette quantité est bien le b cherché.

Avec le programme `pw`, le calcul `pw(642168086464,653246743,875312570876475323578)` prend près de 8 minutes tandis que la variante `pwr` ne prend que 196 milli-secondes.

Pour le décodage, il y a besoin d'expliciter les coefficients de Bézout de deux entiers $a; b$. C'est l'algorithme d'Euclide que SAGE exécute avec la commande `xgcd(a,b)`. Le lecteur qui voudrait en savoir plus sur le type de programme utilisé pourra consulter [2].

4. Fabriquer de grands nombres premiers c'est facile

4.1. Fermat

On a vu que le code RSA requiert de disposer de grands nombres premiers. Bien sûr, on sait depuis Euclide qu'il y a une infinité de nombres premiers mais il n'est pas si facile d'en donner explicitement de très grands. Pierre de Fermat (1601-1665) avait cru trouver une formule donnant à coup sûr des nombres premiers. Voilà ce qu'il dit :

Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme 3, 5, 17, 257, 65537, 4 294 967 297 et le suivant de 20 lettres 18 446 744 073 709 551 617 ; etc. Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par dém établissent ma pensée, que j'aurois peine à me dédire. onstrations infaillibles, et j'ai de si grandes lumières, qui

[11] En fait, si l'on utilise SAGE, il y a une commande power_mod(a, e, p) qui fait exactement ce travail, un tout petit peu plus vite encore.

Traduit en formules, cela signifie que, pour tout entier n, le nombre[12] $Fn = 2^{2^n} + 1$ est premier. C'est effectivement le cas pour n = 0; 1; 2; 3; 4 qui correspondent respectivement aux nombres premiers 3; 5; 17; 257; 65537. On peut d'ailleurs faire le calcul à la main jusqu'à 257, voir **§2.3** quelques techniques pour cela. Pour voir que 65537 est premier, on peut utiliser la fonction is_prime de SAGE. En revanche, on constate, toujours avec SAGE, que $2^{32}+1$, $2^{64}+1$ et $2^{128}+1$ ne le sont pas. (Jusqu'à $2^{8192}+1$ SAGE donne une réponse négative en moins d'une seconde, pour $2^{16384}+1$ il met moins de trois secondes et pour $2^{32768}+1$, 15 secondes.) L'ordinateur factorise instantanément[13] :

$$2^{32}+ + 1 = 641 \times 6700417, \qquad 2^{64}+ + 1 = 274177 \times 67280421310721$$

$$2^{128}+ + 1 = 59649589127497217 \times 5704689200685129054721$$

et il met moins de 5 secondes pour $2^{256}+1$. En revanche, il cale sur le suivant[14], à savoir $2^{512}+1$ (qui a quand même 150 chiffres, c'était il n'y a pas si longtemps le record du monde de factorisation). En tous cas, on constate sur cet exemple que la primalité est plus facile que la factorisation !

On notera qu'à l'heure actuelle on ne sait pas exactement lesquels parmi les Fn sont premiers ou non. La réponse est seulement connue[15] pour un nombre fini de n et, sauf pour les 5 du début, tous les Fn en question sont composés. Cet exemple montre déjà deux choses, d'abord qu'un grand mathématicien peut dire des bêtises, et ensuite qu'il y a des questions, somme toute assez simples, pour lesquelles on n'a pas de réponse.

4.2. Mersenne

Faute de Fermat, on utilise les nombres de Mersenne (1588-1648) : $M_n = 2^n - 1$. Bien sûr, tous ne sont pas premiers, par exemple $2^4 - 1 = 15$ ne l'est pas. On montre (exercice) qu'il faut que l'exposant soit premier, mais cela ne suffit pas (par exemple on a $2^{11} - 1 = 2047 = 23 \times 89$). Cependant, c'est avec ces nombres qu'on obtient les records du plus grand nombre premier connu. Le plus ancien est celui de Cataldi en 1588 avec $M_{19} = 524287$. Il y eut ensuite Lucas (1876) avec M_{127} qui a 39 chiffres. Lucas a inventé un critère de primalité très efficace pour les nombres de Mersenne. Avec ce test, sur mon ordinateur, je montre instantanément que M_{11213} est premier (3376 chiffres, record 1963), ainsi que M_{216091} (en 18 minutes, c'est un nombre de 65050 chiffres, record 1985). Pour une description du test de Lucas, voir :

https://www.imo.universite-paris-saclay.fr/~daniel.perrin/CAPES/arithmetique/Lucas.pdf

Les records actuels sont détenus par d'énormes ordinateurs. Le dernier en date (7 décembre 2018) est $M_{82589933}$ qui a 24 millions de chiffres. Il faudrait pour l'écrire un livre de près de 10000 pages, mais le lecteur montrera, à titre d'exercice que ce nombre commence par 148894 et finit par 902591.

---

[12] Seuls les $2^r + 1$ où r est une puissance de 2 ont une chance d'être premiers à cause de la formule $a^m + 1 = (a+1)(a^{m-1} - a^{m-2} + a^{am-3} - \ldots - a+1)$ lorsque m est impair qui montre que $a+1$ divise $a^m + 1$ (ce qu'on retrouve encore plus simplement grâce aux congruences).

[13] Pour comprendre pourquoi 641 divise F_5 (ce qu'Euler avait montré) et d'où il sort, voir Annexe 6.

[14] J'ai laissé tourner la machine quinze heures sans succès.

[15] Précisément, le plus grand connu est $F_{2747497}$ qui est composé, le plus petit dont on ignore s'il est premier ou non est F_{33}.

5. Factoriser des grands nombres ?

Ce qu'il faut comprendre, c'est que les ordres de grandeur des nombres premiers que l'on sait exhiber, d'une part, et des nombres que l'on sait factoriser, d'autre part, ne sont pas du tout les mêmes, comme on l'a déjà senti à propos des nombres de Fermat. Pendant longtemps, factoriser un nombre de l'ordre d'un milliard était considéré comme à peu près impossible. Ainsi Mersenne, en 1643, avait donné à Fermat, comme un défi, de factoriser le nombre 100895598169. Fermat avait répondu très rapidement :

À cette question je réponds que ce nombre est composé et se fait du produit des deux : 898423 et 112303 *qui sont premiers. Je suis toujours, mon révérend Père, votre très humble et très affectionné serviteur.*

En fait, dans cet exemple, il y avait une sorte de tricherie. En revanche, Fermat savait factoriser 2027651281 et, dans ce cas il a explicité sa méthode. Sur tout cela, voir https://www.imo.universite-paris-saclay.fr/~daniel.perrin/Conferences/BNFredaction.pdf

Le même défi avait été présenté, de manière un peu présomptueuse, comme impossible par Stanley Jevons en 1874 avec le nombre 8616460799. Aujourd'hui, une calculatrice un peu perfectionnée factorise tous ces nombres sans difficulté.

Cependant, le record absolu de factorisation (daté du 2 décembre 2019) est bien loin de celui de primalité, c'est un nombre n de 240 chiffres, produit de deux nombres p et q de 120 chiffres, et encore a-t-il fallu pour trouver p et q faire travailler plusieurs centaines d'ordinateurs en parallèle pendant 2 ans sur un algorithme très complexe, ce qui représente environ 1500 années de temps de calcul pour une machine seule. Voilà ces nombres :

$$124620366781718784065835044608106590434820374651678805754818788883289666801188210855036039570272508747509864768438458621054865537970253930571891217684318286362846948405301614416430468066875699415246993185704183030512549594371372159029236099 =$$
$$509435952285839914555051023580843714132648382024111473186660296521821206469746700620316443478873837606252372049619334517\times$$
$$244624208838318150567813139024002896653802092578931401452041221336558477095178155258218897735030590669041302045908071447$$

On notera tout de même que, dans les années 1980, on estimait qu'il faudrait 50 milliards d'années pour factoriser un nombre de 150 chiffres. Les progrès accomplis par les mathématiciens et les ordinateurs sont donc considérables. Bien entendu, cela ne remet pas en cause la fiabilité du code RSA : si l'on sait factoriser un nombre $n = pq$ de 250 chiffres, il suffit de choisir des nombres p et q plus grands. On a vu qu'il y a de la marge puisqu'on sait expliciter des nombres premiers avec des millions[16] de chiffres. Les banques travaillent déjà avec des clés de l'ordre de 300 chiffres et les militaires avec des clés de 600 chiffres.

Et si un mathématicien améliorait fondamentalement les algorithmes de factorisation et leur permettait de rattraper les tests de primalité ? Alors, pour un temps au moins, il ne serait pas loin d'être le maître du monde[17] !

[16] En fait, les nombres de Mersenne sont proscrits comme clés RSA car ils sont trop particuliers, mais les logiciels comme Pari fournissent sans problème des nombres premiers de 5000 chiffres et SAGE en donne de plus de 1500 chiffres en quelques secondes.

[17] N'ayez pas trop d'espoir tout de même. On pense qu'il y a vraiment une raison profonde qui fait que la factorisation est beaucoup plus difficile que la primalité.

Si vous pensez détenir une méthode, voici deux nombres à factoriser. Pour une poignée de dollars (75 000 $), factoriser le code RSA suivant :

41202343698665954385553136533257594817981169
98443279828454556264338764455652484261980988 7
04231618418792614202471888694925609317763750 33
42113098239748515094490910691026986103186214 88
08669705649029036536588674370413731720813104
10519086425479328260139125762403394637326939 1

Et pour quelques dollars de plus (200 000 $), factoriser :

25195908475657893494027183240048398571429282126204032027777137 83
60436620207075955562640185258807844069182906412495150821892985 591
49176184502808489120072844992687392807287776735971418347270261 896
37501497182469116507761337985909570009733045974880842840179742 9100
64245869181719511874612151517265463228221686998754918242243363 7259
08514186546204357679842338718477444792073993423658482382428119 81638
15010674810451660377306056201619676256133844143603833904414952 634432
19011465754445417842402092461651572335077870774981712577246796292638635637328
99121548314381678998850404453640235273819513786365643912120103971228221207203 57

Ne passez pas trop de temps là-dessus : la société RSA qui mettait sur le marché quelques-uns de ses codes pour vérifier qu'ils étaient solides, en donnant des primes à qui les factoriserait, ne le fait plus depuis déjà quelque temps !

6. Annexe : Euler et les nombres de Fermat

On a vu, grâce à l'ordinateur, que 641 divise $F_5 = 2^{32} + 1$. La question est de savoir comment on peut trouver ce facteur et comment montrer directement qu'il divise F_5.

Le fait que 641 divise F_5 est facile. On pose $p = 641$ (on vérifie que c'est bien un nombre premier). On note les deux formules : $641 = 625 + 16 = 5^4 + 2^4$ et $641 = 640 + 1 = 5 \times 2^7 + 1$. On calcule 2^{32} modulo p. On a $5 \times 2^7 \equiv -1 \pmod{p}$. En élevant cette relation à la puissance 4 on a $5^4 \times 2^{28} \equiv 1 \pmod{p}$. Mais, on a $5^4 \equiv -2^4 \pmod{p}$ et donc $2^{32} \equiv -1 \pmod{p}$. Cela signifie exactement que p divise $2^{32} + 1$.
Une autre question est de trouver le facteur 641. En fait, c'est assez naturel et Fermat était familier de ce type d'arguments[18].
On suppose que F_5 admet un facteur premier p et on travaille dans le groupe multiplicatif $G = (\mathbb{Z}/p\mathbb{Z})^*$. Dans ce groupe on a $2^{32} = -1$, donc $2^{64} = 1$. On voit que 2 est un élément d'ordre 64 de G. Comme l'ordre d'un élément divise l'ordre du groupe, c'est que 64 divise $p - 1$. Cela signifie que p est congru à 1 modulo 64.
On peut même montrer que si p divise $2^{32} + 1$, p est congru à 1 modulo 128. Pour cela, il suffit de montrer que si l'on a $p \equiv 1 \pmod{8}$, 2 est un carré modulo p. En effet, si 2 est le carré de a, on a $2^{32} = a^{64} = -1$ et a est

[18] Il a trouvé ainsi le diviseur 223 de $2^{37}-1$, voir sa lettre à Mersenne de juin 1640. Cela rend son erreur assez mystérieuse. C'est probablement une simple erreur de calcul.

d'ordre[19] 128. Or on sait que F_p^* est cyclique d'ordre $p-1$, donc contient un élément ζ d'ordre 8, qui vérifie donc $\zeta^4 + 1 = 0$, ou encore $\zeta^2 + \zeta^{-2} = 0$, et on voit que $a = \zeta + \zeta^{-1}$ vérifie $a^2 = 2$.

Avec ce raisonnement, il n'y a plus que 641 comme candidat plausible.

II - L'ARITHMÉTIQUE AU COLLÉGE ET AU LYCÉE AUTOUR DE PRIMALITÉ ET FACTORISATION

1. Motivations

1.1. Côté mathématique

On a vu l'importance pour la cryptographie de savoir reconnaître qu'un nombre est premier et de savoir factoriser les nombres qui ne le sont pas. Les suggestions d'exercices ci-dessous se rapportent donc souvent à ces problèmes. Elles ont pour cadre le village[20] de Saint-Tricotin-sur-Pelote (Marne-et-Garonne) ...

Les connaissances mises en jeu ne sont peut-être pas explicitement au niveau du collège, mais peuvent toujours s'y rattacher. Attention, je ne prétends pas que tous ces thèmes peuvent être utilisés dans leur intégralité, ce sont seulement des pistes.

1.2. Des objectifs « philosophiques »

Un objectif essentiel de l'apprentissage des mathématiques est - à mon avis - d'apprendre aux élèves à chercher en les faisant réfléchir sur des problèmes ouverts : comment aborder un problème inconnu notamment par des méthodes expérimentales.

Un deuxième objectif est de leur montrer certains aspects méconnus des mathématiques : les applications, l'existence de questions non résolues, les incertitudes de la recherche, etc.

Un dernier objectif est de montrer qu'on peut s'amuser en faisant des mathématiques ...

1.3. Des objectifs techniques

À ces objectifs s'ajoutent des points plus techniques qu'il est nécessaire de renforcer. On peut citer : le calcul mental, les manipulations algébriques, l'utilisation des outils informatiques et de la programmation.

Du point de vue arithmétique, les exercices utilisent principalement la décomposition en produit de facteurs premiers, mais ils effleurent aussi de nombreux résultats (la division euclidienne, les congruences, Gauss, Bézout, Fermat, etc.).

1.4. Quels intérêts didactiques ?

Les exercices sont le plus souvent à géométrie variable, avec des possibilités d'adaptation, de simplification, d'extension ... Ils permettent d'illustrer l'idée que, même si l'on ne sait pas résoudre entièrement un problème, on peut toutefois s'en approcher.

[19] Avec cette ruse, il y a seulement à éliminer 257 et c'est à peu près évident car c'est lui-même un nombre de Fermat.

[20] Faut-il préciser qu'il est imaginaire ? Cela évite de se poser des questions de vraisemblance.

2. Primalité : dizaines riches ou pauvres

2.2. Dizaines riches

Fortuné Richard, le plus gros propriétaire de Saint-Tricotin-sur-Pelote (Marne-et-Garonne), ne jure que par la richesse. Il sait qu'à partir de 10, les nombres premiers se terminent par 1, 3, 7, 9 et il aime particulièrement les dizaines riches où les quatre possibles sont premiers comme 11, 13, 17, 19.
Il aimerait bien en avoir d'autres, mais il n'est pas très fort en calcul. Pouvez-vous l'aider à en trouver ? Y en a-t-il beaucoup ? une infinité ?

L'examen des premières dizaines montre qu'il n'y a aucune autre dizaine riche jusqu'à 100, mais que 101, 103, 107 et 109 sont premiers. Pour aller plus loin, il vaut mieux écrire quelques lignes de programme et c'est une bonne occasion d'en montrer l'intérêt :

```
def jujumeau(k) :
n=11
while n<k :
        if is prime(n) and is prime(n+2) and is prime(n+6) and is prime(n+8) :
          print (n)
n=n+30
```

(L'instruction $n = n + 30$ est un moyen d'accélérer le programme en notant que, dans deux dizaines sur trois, il y a un multiple de 3 qui se termine par 1, 3, 7 ou 9.)

On trouve alors les dizaines suivantes : 190, 820, 1480, etc. Il y en a 165 jusqu'à 106 et on a le sentiment qu'il doit y en avoir une infinité. Cela étant, et c'est l'intérêt de l'exercice, ce n'est qu'une conjecture, on ignore aujourd'hui encore s'il y a une infinité de dizaines riches[21] : il reste des choses à faire en mathématiques.

2.2. Dizaines pauvres

Pierre Labbé, lui, est plutôt du côté des opprimés. Il s'intéresse aux dizaines pauvres qui ne contiennent pas de nombre premier. En connaissez-vous ?
Sa tâche humanitaire ne s'arrête pas là : il prétend qu'il y a des centaines pauvres et même qu'on peut trouver un million de nombres de suite sans aucun nombre premier. Là, il exagère, non ?

La première dizaine pauvre est celle des 200 : 201 et 207 sont multiples de 3, 203 de 7 et 209 de 11. On peut aussi écrire un programme pour en trouver d'autres, mais ici, le résultat évoqué : *pour tout entier n il existe toujours n nombres consécutifs sans aucun nombre premier* est facile. Bien entendu il faut une idée, celle d'utiliser la factorielle[22] $n!$ et de considérer[23] $n! + 2$, $n! + 3$, ..., $n! + n$.

---

[21] Cette conjecture contient celle de l'infinitude des paires de nombres premiers jumeaux, c'est-à-dire distants de 2, comme 11 et 13, 17 et 19, 29 et 31, toujours ouverte elle aussi. Si la conjecture est vraie on peut montrer que le nombre de dizaines riches $\leq N$ est équivalent à $67:13N=(\ln(10N))^4$:

[22] Qu'on ne vienne pas me dire que cette notion n'est pas enseignée au collège. C'est vrai, mais mon expérience c'est que les collégiens comprennent immédiatement la notion et son utilité pour ce problème.

[23] Exercice : montrer que, si $n > 2$, on obtient n nombres composés consécutifs en ajoutant à ceux-là $n! + 1$ ou $n! + n + 1$. Voir la solution en annexe.

L'intérêt que je vois à ces deux exercices est de montrer l'imprévisibilité de la recherche : avec les dizaines pauvres et riches on a deux énoncés qui semblent voisins et pourtant l'un est inabordable et l'autre élémentaire.

2.3. Fabriquer des nombres premiers

Hortense Aignante, qui enseigne les mathématiques au collège Sainte-Aiguille de Saint- Tricotin a un truc pour fabriquer des nombres premiers : elle les prend sous la forme $a^2 + 1$.
Bien entendu, cela ne marche pas toujours, il faut faire attention au dernier chiffre de a, pourquoi ?
Avec cette précaution, $a^2+ 1$ n'est pas multiple de 2 ni de 5. Il n'est pas non plus multiple de 3. Pourquoi ? Et pour 7, 11, 13 ? Pouvez-vous trouver beaucoup de nombres premiers de la forme $a^2 + 1$? Une infinité ?
Sa cousine Clémence, qui joue la fille d'Euler, préfère utiliser les nombres de la forme $n^2 + n + 41$ ...

L'idée, comme pour les nombres de Fermat ou de Mersenne, est celle d'une sorte d'équité de la répartition: au voisinage d'un nombre très composé comme a^2, les autres ont plus tendance être premiers[24].

La question est donc : quels sont les a tels que $a^2 + 1$ soit premier ? Hormis le cas de $a = 1$, qui donne 2, il faut évidemment que a soit pair. Ensuite, l'exercice est une occasion d'un premier contact avec les congruences, d'abord dans leur forme élémentaire : quel peut être le dernier chiffre de a ? Hormis $a = 2$, qui donne 5, on constate expérimentalement qu'il faut que a se termine par 0, 4, 6 (sinon $a^2 + 1$ est multiple de 5). On peut le montrer[25] en écrivant, par exemple : $(10k + 2)^2 + 1 = 100k^2 + 40k + 4 + 1$. On trouve des exemples avec les trois finales : $101 = 10^2 +1$, $17 = 4^2 + 1$ et $37 = 6^2 + 1$.

On constate ensuite qu'un nombre de la forme $a^2 + 1$ n'est jamais multiple de 3. Pour le prouver, on écrit $a = 3k + r$ avec $r = 0, 1, 2$ et on calcule le carré[26] $9k^2 + 6rk + r^2$ avec $r^2 = 0, 1, 4$, de sorte que $r^2 + 1$ n'est pas multiple de 3. Si l'on veut aller plus loin, on peut voir que $a^2 + 1$ n'est jamais non plus multiple de 7, ni de 11. Pour ceux-là on peut se contenter de l'expérience, mais si l'on veut, par exemple pour 7, on y arrive en énumérant les carrés modulo 7. (Quand on est savant on sait que -1 est un carré modulo un nombre premier impair p si et seulement si on a $p \equiv 1 \pmod 4$, voir ci-dessous **§III.6**.)
Avec 13, comme on a $-1 \equiv 5^2$, pour avoir des mauvais a (c'est-à-dire des a tels que a^2+1 soit multiple de 13) il suffit de prendre $a \equiv \pm 5 \pmod{13}$.
La question naturelle, qui émerge si l'on écrit un programme donnant les $a^2 + 1$ est celle de leur infinitude. C'est encore une question ouverte ! Si l'on note $P_1(N)$ le nombre d'entiers $1 \leq n \leq N$ tels que $n^2 + 1$ soit premier on ne sait donc pas si $P_1(N)$ tend vers l'infini, mais si c'est le cas, Shanks a montré qu'on a $P_1(N) \sim 0.6864 \int_2^N \frac{dt}{\ln t} \sim 0.6864 \frac{N}{\ln N}$. Si la conjecture est vraie, un petit calcul montre que la probabilité de trouver un nombre premier de la forme $a^2 + 1$ avec $a \leq 10^n$ en se limitant aux nombres se terminant par 0, 4, 6 est presque exactement $1/n$.
Pour l'exemple des nombres $n^2 + n + 41$ (qui donnent des nombres premiers pour tout n entre 0 et 39), voir https://www.imo.universite-paris-saclay.fr/~daniel.perrin/journeedu2311/redaction2311e.pdf

[24] Idée aussi naïve que celle des joueurs de Loto qui pensent qu'un nombre qui vient de sortir à moins de chances de revenir.

[25] Je sais, on ne voit plus la formule donnant $(a + b)^2$ au collège, mais c'est un scandale absolu et, par ailleurs, on la retrouve aisément en développant $(a + b)(a + b)$ et elle saute aux yeux si l'on décompose un carré de côté $a + b$ en deux carrés et deux rectangles.

[26] Cet exercice est une véritable publicité pour deux choses : pour le dialogue expérience, conjecture, preuve et aussi pour les identités remarquables.

3. Factorisation

Pierre Landin, mathématicien en retraite à Saint-Tricotin, plus connu sous son pseudonyme de Dernier Lapin, a quelques trucs pour factoriser[27] un entier n. Il utilise la technique élémentaire qui consiste à diviser n par les nombres premiers p jusque $\sqrt{n}$. *Mais il a quelques ruses supplémentaires ...*

3.1. Les critères de divisibilité

Ils sont évidents pour 2 et 5 et faciles pour 3 et 11 mais c'est l'occasion d'un travail algébrique pour montrer ces critères, disons avec des nombres de trois chiffres. On écrit $n = 100c + 10d + u$. Pour 3, on écrit $n = 99c + 9d + c + d + u$ et n est multiple de 3 si et seulement si $c + d + u$ l'est. Pour 11 on écrit $n = 99c + 11d + c - d + u$ et n est multiple de 11 si et seulement si $c - d + u$ l'est.

3.2. Ajuster en retranchant ou en ajoutant

Pour voir si le nombre de Fermat 257 est multiple de 7, on retranche 7, il reste $250 = 25 \times 10 = 5 \times 5 \times 2 \times 5$ qui n'est pas multiple de 7, donc 257 non plus. C'est le lemme suivant :

2.1 Lemme. *Si p divise a et b il divise a + b et a − b.*

Démonstration. On écrit $a = pa'$, $b = pb'$ et on a $a - b = p(a' - b')$ et $a + b = p(a' + b')$.
Pour appliquer cette méthode, on se souvient que les nombres premiers se terminent par deux types de finales 3, 7 d'une part et 1, 9 de l'autre. L'application est facile si n et p sont du même type par rapport à 3, 7 ou 1, 9 comme 257 avec 7 ou 13. Précisément, si le nombre n se termine par 3 ou 7 il est facile de tester $p = 7, 13, 17, 23$, etc. S'il se termine par 1 ou 9 c'est facile pour 19, 29, 31, etc. C'est plus difficile si n et p sont de types différents. Dans ce cas il faut connaître des multiples de l'autre type. Voici les plus commodes : $3 \times 7 = 21$, $7 \times 7 = 49$, $3 \times 13 = 39$, $7 \times 13 = 91$, $3 \times 17 = 51$, $3 \times 19 = 57$, $3 \times 23 = 69$, $3 \times 29 = 87$, etc.

Cette méthode pose une question : pourquoi est-on sûr qu'il y a toujours un multiple de p qui se termine par un « bon » chiffre ? C'est le lemme suivant :

2.2 Lemme. *Soit p premier (distinct de 2 et 5) et soit a un chiffre en base 10, premier à 10 (donc 1, 3, 7, 9). Il y a toujours un multiple de p qui se termine par a.*

*Démonstration***.** Savamment, c'est le fait que p engendre $(\mathbb{Z}/10\mathbb{Z})^*$, qui n'est autre que le théorème de Bézout. Mais il n'y a pas besoin de ça, il suffit de regarder les terminaisons : si p se termine par 1, on obtient a en multipliant p par a, s'il se termine par 3 on multiplie par 7, 1, 9, 3 pour attraper 1, 3, 7, 9, etc. Autrement dit on constate, en faisant tous les produits $a \times b$ avec $a, b \in \{1, 3, 7, 9\}$:

2.3 Lemme. *Dans la table des 1, 3, 7 ou 9 on trouve un et un seul nombre se terminant par chacun des chiffres 1, 3, 7 ou 9.*

3.3. Une autre ruse pour éliminer des indésirables

C'est encore le lemme précédent (ou presque) qui sert pour voir qu'un nombre n (disons de trois chiffres) n'est pas multiple d'un p (disons 41) grâce aux terminaisons et aux ordres de grandeur. Si par exemple n est < 410, il y a un seul multiple de 41 pour chaque terminaison possible et on conclut avec l'ordre de

[27] Je me livre à ce genre de calcul en permanence, avec le total de mon ticket de cantine, avec les numéros des voitures dans la rue, etc.

grandeur. Par exemple, à cause de la terminaison, si 237 était multiple de 41 ce ne pourrait être que 7 × 41, mais comme on a 7 × 4 = 28, il est clair que 7 × 41 est trop grand. On peut faire le même raisonnement avec 373 et 47 (ce serait 9 × 47 donc de l'ordre de 430). Voici le lemme :

***2.4 Lemme**. Soit p un nombre premier distinct de 2 et 5 et soient a, b des chiffres en base 10. Si ap et bp ont même chiffre des unités on a a = b.*

Comme on le voit, toutes ces ruses requièrent une bonne connaissance des tables de multiplication et sont une motivation pour les réviser.

3.3. Divisible c'est bien beau, mais encore faut-il diviser

Ceci s'applique notamment pour 9 et 11. Dans le cas où l'on a repéré, grâce au critère de divisibilité, que n est multiple de 9 ou de 11, il s'agit de calculer le quotient. Pour cela, on repère l'ordre de grandeur et le dernier chiffre. Par exemple, si l'on cherche $n = 3483/9$, il se termine par 7, il est dans les 300 et plus grand que 348. De plus on doit retrouver $n \times 10$ en ajoutant n à 3483. On voit que n est de l'ordre de 370 ou 380 et c'est précisément[28] 387.

3.4. Différence de deux carrés

C'est la méthode qu'utilisait Fermat (et qui reste à la base des méthodes actuelles de factorisation). Si n est de la forme $a^2 - b^2$ il se factorise en $(a - b)(a + b)$. Par exemple on a $221 = 225 - 4$ et si l'on sait que $225 = 15^2$, on voit que c'est $(15 - 2)(15 + 2)$, donc 13×17.

De même on a $323 = 324 - 1 = 17 \times 19$, $5893 = 5929 - 36 = 77^2 - 6^2 = 71 \times 83$.

3.5. Les copains d'abord

Enfin, il y a plein de nombres que je connais comme premiers ou non, tous ceux < 100 (il suffit de savoir que $91 = 7 \times 13$), en fait jusqu'à 130 et quelques-uns qui sont mes copains pour diverses raisons : 163, 257, 641, 1729, etc.

3.6. Un exemple pas tout à fait évident : 3763

Il n'est pas multiple de 3 ni de 11. Pour 7 on voit le 63, pour 13, on utilise, en retranchant, $375 = 25 \times 15$ ou $375 = 390 - 15$, pour 17, $378 = 340 + 38$, pour 19, $3763 = 3800 - 37$, pour 23, $374 = 11 \times 34$, pour 29, $3763 + 87 = 3850$ et $385 = 5 \times 77$ ou 11×35, pour 31, $3763 = 3100 + 620 + 43$, 37 est clair, pour 41, $3763 - 123 = 3640$ et 364 serait 4×41, qui est trop petit, pour 43, 372 serait 4×43, non, pour 47, 381 serait 3×47 non, pour 53, 371 serait 7×53. Ah, c'est ça ! et on a donc $3763 = 53 \times 71$.

4. D'autres problèmes de Saint-Tricotin : la crue de la Pelote

À la suite des inondations provoquées par la crue de la Pelote, tout le canton de Saint-Tricotin a été sinistré. Le préfet de Marne-et-Garonne, Henri Bambel, est chargé de répartir les secours. Malheureusement, le bordereau qui portait la somme à diviser en parts égales entre les 396 victimes a été endommagé par les eaux et certains chiffres de la somme sont invisibles. On lit seulement 38 ••2 *Le préfet est bien embêté car il se souvient seulement que la somme attribuée à chacun était un nombre entier d'euros. Combien doit-il donner à chaque sinistré ?*

[28] On notera que 387 est encore multiple de 9 : 9 x 43.

Voici quelques éléments de solution. L'énoncé indique que le nombre $N = 38\bullet\bullet2$ est multiple de 396. Mais, ce dernier nombre se décompose en produit de facteurs premiers (ou plutôt primaires) : $396 = 4 \times 9 \times 11$. Il en résulte que N doit être à la fois multiple de 4, de 9 et de 11. (En fait, c'est équivalent, mais il n'y a pas besoin de savoir ça.) Examinons donc ce que donne chaque facteur.

Pour la divisibilité par 9 on a le critère déjà vu : la somme des chiffres doit être divisible par 9. Ici, il y a un point essentiel qui est de donner[29] un nom aux deux chiffres manquants : $N = 38xy2$ avec x, y entre 0 et 9. Dire que le nombre est divisible par 9 c'est dire que $3 + 8 + x + y + 2 = 13 + x + y$ l'est. On se récite la table des 9 en n'oubliant pas que x et y sont ≤ 9. Il reste deux possibilités : $x + y + 13 = 18$ ($x + y = 5$) ou $x + y + 13 = 27$ (donc $x + y = 14$) (le suivant $x + y + 13 = 36$ donne $x + y = 23$ et c'est trop). On garde ça en réserve.

On fait la même chose avec 11, mais avec la somme alternée des chiffres : $3 - 8 + x - y + 2 = x - y - 3$ doit être multiple de 11. Attention, là, $x - y - 3$ peut être négatif, et c'est une grosse difficulté. On regarde donc les multiples de 11 et il y a une autre difficulté qui est de ne pas oublier 0. Si $x - y - 3 = 11$, on a $x - y = 14$ et c'est impossible avec $x \leq 9$. Bien sûr c'est encore pire avec 22, etc. Si $x - y - 3 = 0$ on a $x - y = 3$. Si $x - y - 3 = -11$, on a $x - y = -8$ ou encore $y - x = 8$, et c'est tout juste possible, avec $x = 0$, $y = 8$ ou $x = 1$, $y = 9$. On garde ça en réserve.

Pour la divisibilité par 4 il faut regarder la table des 4 et on voit que les multiples de 4 sont pairs (ça c'est clair !), ce qui est le cas ici, car le chiffre des unités est 2, mais attention, parmi les nombres se terminant par 2, seuls ceux dont le chiffre des dizaines est impair[30] sont multiples de 4 (12, 32, 52, 72 et 92 mais pas 22, 42, etc.) Les centaines et les chiffres d'ordre plus grand ne changent rien car 100 est multiple de 4. On retient donc une seule chose : le nombre y est impair.

On revient à ce qu'on a trouvé avec 11. On a soit $x - y = 3$, soit $y - x = 8$ et on a vu que cette dernière solution donne, avec y impair, $y = 9$ et $x = 1$. Mais la somme $x + y$ est alors égale à 10, donc ni à 5 ni à 14. Bref, il reste $x + y = 3$. Du côté de la somme on a soit $x + y = 5$, soit $x + y = 14$. Si l'on est malin, on note que $x - y$ et $x + y$ sont de même parité car on a $x + y = x - y + 2y$. Il reste donc $x + y = 5$. Là, avec $x - y = 3$, on voit aussitôt la solution qui est $x = 4$, $y = 1$. (Si l'on ne voit rien on peut calculer $(x + y) + (x - y) = 8 = 2x...$) et on trouve $N = 38412$ et $N/396 = 97$.

En fait, si l'on est astucieux, on peut trouver ce résultat très vite[31]. On voit que le quotient q de N (de l'ordre de 38000) par 396 doit être un peu en dessous de 100. On voit aussi que le chiffre des unités de q doit être 2 ou 7 (car il faut trouver 2 en multipliant par 6). On essaie 92, c'est trop petit, mais 97 convient !

Il est clair que cet exercice est difficile et qu'il demande de l'initiative. Le contenu mathématique proprement dit comporte la factorisation (de 396), l'introduction d'inconnues, les critères de divisibilité et l'exploitation des résultats. On peut adapter la difficulté, par exemple on a une variante facile avec 36 sinistrés et $N = 7x6$ à distribuer et une variante difficile avec 2772 sinistrés et $N = 71xyz4$ (seule solution 712404, parts de 257, avec là encore une variante plus rapide par division et essais.). Pour éviter l'usage de cette méthode par division et essais, il suffit d'effacer le premier chiffre de N. Par exemple on peut prendre,

[29] Pour un mathématicien c'est un réflexe évident, mais c'est un point dont les élèves ne sont pas toujours persuadés. Cet exemple est très convaincant de ce côté.

[30] Ici, on peut se convaincre du résultat en énumérant tous les possibles ou écrire une preuve algébrique.

[31] C'est un défaut de cette version de l'exercice !

toujours avec 396 sinistrés, N = •02•2 (solution 50292 = 396 × 127). Attention aussi à la position des inconnues, de manière à avoir la somme avec le critère par 9 et la différence avec celui par 11. Sans cela, il y a souvent plusieurs solutions (5 solutions pour 3*x*4*y*2 avec 396).

5. Les dimensions des champs

A la suite des inondations provoquées par la crue de la Pelote, les champs rectangulaires d'Elisabeth Rave ont été inondés, leurs bornes ont disparu et le cadastre a été endommagé. Elisabeth, qui a pris un coup de vieux, a oublié les dimensions de ses champs. Elle se souvient juste qu'elles étaient toutes entières et plus grandes que 20. Pour les deux premiers, elle se souvient que leurs aires étaient de 851 et 858 et que leurs périmètres n'étaient pas plus que 120. Pour le dernier que le périmètre était 360 et le pgcd des dimensions 18. Aidez-là à retrouver les dimensions de ses champs.
L'unité de longueur est le décamètre (1 dam = 10m) l'unité d'aire est l'are ou dam².

Si l'aire d'un champ rectangulaire est de 851, on décompose ce nombre en produit de facteurs premiers : 851 = 23 × 37. Les dimensions peuvent donc être seulement 23 et 37 (*a priori* il y a aussi 1 et 851, mais, outre le fait que c'est très improbable pour un champ, c'est contraire à l'hypothèse sur le périmètre). Dans ce cas facile la réponse est donc 23 et 37.

Pour le second on a 858 = 2 × 3 × 11 × 13 il y a beaucoup plus de solutions. Il faut énumérer les diviseurs de ce nombre. Je propose pour cela une méthode qui consiste à ordonner ces diviseurs selon le nombre de leurs facteurs premiers : 0 facteur : 1, puis 1 facteur, 2, 3, 11, 13 puis 2 facteurs : 6, 22, 26, 33, 39, 143, puis 3 facteurs (les « compléments » des 1 facteur) : 66, 78, 286 et 429 et enfin 858. Chacun de ces diviseurs vient avec son complément. La condition sur les périmètres permet d'écarter aussitôt nombre de solutions et il ne reste que 22, 39 ou 26, 33. Dans le premier cas le périmètre est 122, dans le second 118. La solution est donc 26, 33.

Il reste le champ de périmètre 360. Appelons a, b ses dimensions. On a donc $a + b = 180$ et $pgcd(a, b) = 18$. Ce qu'il faut connaître, là, c'est ce que j'appelle la comptine du *pgcd* : on a $a = 18a'$, $b = 18b'$ avec a' et b' premiers entre eux. On a donc $a' + b' = 10$ et, si l'on n'oublie pas la condition premiers entre eux, il reste seulement les solutions $a' = 1$, $b' = 9$, $a' = 3$, $b' = 7$ (ou les mêmes à l'envers). Cela donne $a = 18$, $b = 162$, que l'on rejette car l'une des dimensions est < 20, ou $a = 54$, $b = 126$ qui est la bonne solution.

Le thème général de ce type d'exercices est de déterminer deux entiers a, b à partir de certaines quantités qui leur sont liées. Sur ce dernier point, il y a une foule de possibilités et on peut laisser libre cours à son imagination. Il y a bien sûr la somme $a + b$ et le produit ab mais aussi $a^2 + b^2$, $a^2 - b^2$, le *pgcd*, le *ppcm*, etc. Ces variantes peuvent être plus ou moins difficiles selon les choix, voir de nombreux exemples dans [1]. Parfois une seule donnée suffit. L'intérêt majeur de l'exercice proposé est le travail sur la factorisation et l'énumération de diviseurs. Du point de vue technique, il y a aussi l'utilisation de la disjonction de cas et de la comptine du pgcd. Certains choix peuvent même mener à des problèmes ouverts, par exemple $a^3 - b^2$ (ou $a^3 + b^2$) qui correspond à l'équation de Bachet.

6. Le druide de Septimanie

Dans la Gaule antique, le village de Saint-Tricotin-sur-Pelote (Marne-et-Garonne) se trouvait au cœur d'une région appelée Septimanie, nommée ainsi parce que ses habitants avaient la manie de compter en base 7. On sait que les Gaulois ne craignaient qu'une chose, c'est que le ciel ne leur tombe sur la tête, ce qui est une façon de craindre la fin du monde. D'ailleurs, feu le druide Pacorabanix, fort versé en numérologie, avait prévu ce cataclysme pour l'an

$\overline{5555}$. *Les esprits forts savent que cette prévision est sujette à caution, puisqu'il n'y a aucune raison que ce nombre, remarquable en base 7, le soit encore dans une autre base et ils le vérifieront en calculant ce nombre en base 10.*

C'est juste une récréation : le nombre 5555 en base 7 n'est autre que 2000 en base 10 !

7. Les champs carrés

Elisabeth Rave, la fermière de Saint-Tricotin, aime les champs carrés et elle connaît bien les entiers qui sont des carrés parfaits (1, 4, 9, 16, ..., 2809, ...). À défaut elle essaie d'écrire les entiers $n \geq 0$ comme différence de carrés parfaits (donc sous la forme $n = x^2 - y^2$ avec x, y entiers ≥ 0). Elle y arrive souvent, mais pas toujours.
Peut-on le faire avec les entiers suivants (et, lorsque c'est possible, de combien de manières) : 5, 11, 14, 17, 18, 20, 44, 45, 56, 66, 162, 257, 391, 426, 432, 452 ?
Pouvez-vous préciser tous les entiers qui peuvent s'écrire sous cette forme ?

On commence par explorer l'exercice avec les premières valeurs données[32]. On a facilement $5 = 9 - 4 = 3^2 - 2^2$, $11 = 36 - 25 = 6^2 - 5^2$. Avec un peu de patience on trouve $17 = 81 - 64 = 8^2 - 7^2$, mais, même avec un peu d'obstination, 14 n'a pas l'air de marcher. Si l'on regarde bien, on voit que dans tous les cas positifs ci-dessus on a pris la différence de deux carrés consécutifs. Si l'on écrit cela algébriquement[33] $(n + 1)^2 - n^2 = 2n + 1$ (en développant $(n + 1)^2$ ou en utilisant la différence de deux carrés), on voit qu'on va attraper ainsi tous les impairs. Par exemple, $391 = 2 \times 195 + 1 = 196^2 - 195^2$.

Il reste les pairs. On commence par le commencement, c'est-à-dire le nombre 2. En consultant la liste des carrés et la taille des différences, on constate que 2 ne peut pas s'écrire comme différence de deux carrés. On le prouve facilement avec l'écriture algébrique, si l'on connaît les identités remarquables. En effet, si l'on a $2 = x^2 - y^2 = (x - y)(x + y)$, la seule façon de faire cela en entiers c'est de prendre $x - y = 1$ et $x + y = 2$, mais ça n'existe pas ! Il y a de multiples manières de le voir, la plus simple étant de noter que x et y sont compris entre 0 et 2 et d'essayer tous les cas. Mais on peut aussi résoudre le système et constater qu'il apparaît des demi-entiers, ou encore noter $x + y = (x - y) + 2y$ de sorte que $x - y$ et $x + y$ doivent être de même parité.

On peut alors revenir au cas de 14. Si $14 = (x - y)(x + y)$, avec x, y entiers, les seules solutions sont $x - y = 1$ et $x + y = 14$ ou $x - y = 2$ et $x + y = 7$ et, là encore, la parité contredit. Avec cette réflexion on obtient le résultat général. En effet, supposons qu'on ait $n = x^2 - y^2$ avec n pair. On a donc $n = (x - y)(x + y)$ donc l'un des nombres $(x - y)$ ou $(x + y)$ est pair. Mais alors ils le sont tous les deux et n est multiple de 4. On ne peut donc pas écrire sous cette forme les nombres pairs qui ne sont pas multiples de 4.

Il faut encore vérifier que les multiples de 4 marchent. L'expérience avec $4 = 2^2 - 0^2$, $8 = 3^2 - 1^2$, $12 = 4^2 - 2^2$ montre qu'il faut prendre des entiers écartés de 2 : $4p = (p + 1)^2 - (p-1)^2$, toujours les identités remarquables.

Il reste la question plus délicate du nombre de façons d'écrire n sous la forme $x^2 - y^2$ quand c'est possible. Supposons d'abord n impair. On décompose n en produit de facteurs premiers $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et on cherche à l'écrire $(x - y)(x + y)$. Pour cela, on prend pour $a = x - y$ et $b = x + y$ deux diviseurs de n, « complémentaires » (c'est-à-dire tels que leur produit soit égal à n) avec $a \leq b$. Il reste à montrer le lemme suivant :

[32] Il peut être utile d'établir la liste des carrés des nombres de 1 à 20.

[33] On voit ici, de manière éclatante, tout l'intérêt de l'écriture algébrique.

2.5 Lemme. *Si a, b sont des entiers impairs, avec* $a \leq b$, *le système* $a = x - y$, $b = x + y$ *a une solution unique dans les entiers* ≥ 0.

Démonstration. La solution est $x = \frac{b+a}{2}$ et $y = \frac{b-a}{2}$.
Le nombre *S* de solutions, dans le cas impair, est donc le nombre de diviseurs *a* de *n* tels que $a \leq b = n/a$. Comme le nombre total de diviseurs de *n* est (α_1+1) _ _ _ (α_r+1), *S* est la moitié de ce nombre (s'il est pair, ce qui est le cas sauf si n est un carré, cas que le lecteur examinera ...). Par exemple, pour $n = 391 = 17 \times 23$, on a $\alpha_1 = \alpha_2 = 1$, donc il y a deux solutions, $a = 1$, $b = 391$ qui donne $x = 196$ et $y = 195$, mais aussi $a = 17$, $b = 23$ qui donne $x = 20$ et $y = 3$. Pour $6615 = 3^3 \times 5 \times 7^2$ il y a 12 solutions.

Il reste le cas où *n* est multiple de 4 : on écrit $n = 4k = (x - y)(x + y)$ avec $x - y$ et $x + y$ de même parité donc pairs, $x - y = 2p$, $x + y = 2q$, donc $k = pq$ et on est ramené à chercher les décompositions de *k*. Par exemple, pour $464 = 4 \times 116$, les décompositions de 116 sont 1, 116 ; 2, 58 et 4, 29 qui donnent pour *x*, *y* : 117, 115 ; 60, 56 et 33, 25.

Il est facile d'écrire un programme qui donne toutes les décompositions : le seul point délicat est de borner *x*. Comme on a $x + y \leq n$ et $x > y$ on en déduit $y < n/2$, comme $x - y$ divise *n*, on a $x < 3n/2$. Voici un exemple écrit avec SAGE :

```
def rave(n):
    for y in [0..(n-1)/2] :
        for k in [0..sqrt(y^2+n)-y] :
            if k^2+2*k*y==n :
                print (y+k,y)
```

Cet exercice montre l'intérêt d'une approche expérimentale des mathématiques. En effet, pour le résoudre, on peut commencer par regarder quelques cas particuliers, avec des *n* petits, par tous les moyens, y compris très artisanaux. L'intérêt est de voir se dégager les phénomènes : le cas des impairs, la difficulté pour les nombres pairs non multiples de 4. Cette approche peut mener à des conjectures qui donneront le résultat final. Ensuite, pour écrire une preuve on aura besoin de l'écriture algébrique, particulièrement efficace dans ce cas, qui mettra aussi en évidence l'intérêt de factoriser en arithmétique. On verra aussi apparaître d'autres notions : les congruences modulo 4, les équations linéaires. Enfin, pour la question du nombre de solutions, c'est encore la décomposition en produit de facteurs premiers qui sera essentielle, avec l'énumération des diviseurs.

8. Non à l'euro ! ¶

Le maire de Saint-Tricotin-sur-Pelote (Marne-et-Garonne), Jacques Huse, très hostile à l'Europe, a décidé de quitter la zone euro et de faire utiliser aux habitants de Saint-Tricotin leur propre monnaie : la maille. Pour éviter de frapper trop de sortes de pièces, deux types de pièces seulement seront disponibles, l'une de 9 mailles, l'autre de 11 mailles.

1) Au début de l'opération, les commerçants n'ont pas de pièces pour rendre la monnaie et les acheteurs doivent faire l'appoint. Faire la liste des sommes ≤ 30 mailles que l'on peut payer. Peut-on payer les sommes suivantes (en mailles) : 41, 53, 71, 79 *?*

2) Montrer qu'on peut payer toutes les sommes de c mailles avec $80 \leq c \leq 88$, *puis toutes les sommes* $c \geq 80$, *par exemple 118 ou 417 (on suppose que l'acheteur a à sa disposition autant de pièces qu'il veut) (¶). Indiquer toutes les manières de le faire (¶¶).*

3) On suppose qu'au bout d'un certain temps les commerçants ont un stock de pièces suffisant pour rendre la monnaie. Montrer qu'on peut maintenant payer n'importe quelle somme entière (on pourra commencer par la somme de une maille). Comment payer les sommes suivantes : 13 mailles, 41 mailles, 79 mailles en manipulant le moins possible de pièces (¶¶) ?

Je détaille ci-dessous la solution et les divers arguments. Bien entendu, tout n'est pas faisable en classe, mais c'est un thème très riche.

8.1. Sans rendre la monnaie, 1)

Si l'on ne rend pas la monnaie, les seules sommes que l'on peut payer sont de la forme $9a + 11b$ avec a, b entiers ≥ 0. Pour avoir toutes les sommes possibles ≤ 30 et ne pas en oublier, une technique sûre consiste à ordonner les tentatives selon les valeurs de $s = a + b$. Ainsi, $a + b = 0$ donne $a = b = 0$, $a + b = 1$ donne (1, 0) ou (0, 1), etc. On obtient comme sommes possibles : 0 ($s = 0$) ; 9, 11 ($s = 1$) ; $18 = 2 \times 9$, $20 = 9 + 11$, $22 = 2 \times 11$ ($s = 2$) ; $27 = 3 \times 9$, $29 = 2 \times 9 + 11$ ($s = 3$) et c'est tout pour les sommes ≤ 30 car $9 + 2 \times 11 = 31$ et $4 \times 9 = 36$.

Pour décider lesquelles sont possibles parmi les quatre propositions 41, 53, 71, 79, on peut faire la liste des multiples de 9 et de 11 et essayer d'en ajuster deux qui font le total. On trouve ainsi, avec un peu de patience, $53 = 44 + 9$ et $71 = 44 + 27$.

En revanche, on ne peut pas payer 41 ni 79. Détaillons le raisonnement pour 41. On regarde les multiples de 11 plus petits que 41 et on ne gagne que si la différence avec 41 est multiple de 9. Or on a $41 = 33 + 8 = 22 + 19 = 11 + 30 = 0 + 41$ et aucun ne convient. On peut même aller un peu plus vite, par exemple pour 79 on part de 77, avec $79 = 77 + 2$ et chaque fois qu'on diminue de 11 le 77 on ajoute 11 à 2. On trouve successivement : 2, 13, 24, 35, 46, 57, 68, 79. Comme aucun n'est multiple[34] de 9 le paiement est impossible. On peut d'ailleurs utiliser cette méthode aussi pour traiter les cas positifs. Avec 53 on gagne tout de suite, $53 = 44 + 9$, avec 71 on a $71 = 66 + 5 = 55 + 16 = 44 + 27$, stop.

8.2. Sans rendre la monnaie, 2)

Pour les sommes entre 80 et 88 c'est un peu plus rusé. Il y a évidemment deux nombres faciles : $88 = 8 \times 11$ et $81 = 9 \times 9$. Si, dans le $88 = 8 \times 11$, on change un 11 pour un 9, on diminue la somme de 2, donc on obtient 86, 84, 82, 80 (et même 78, 76, 74, 72 mais on n'en a pas besoin ici). Si, dans $81 = 9 \times 9$, on change un 9 pour un 11 on augmente de 2, et on obtient donc 83, 85, 87 (et les suivants jusqu'à 99). On voit qu'on a bien obtenu toutes les sommes comprises entre 80 et 88.

En fait, cette procédure donne un moyen d'avoir toutes les sommes possibles. On part d'un seul 9, on peut le changer en 11, on a donc 9, 11. Avec deux 9 on trouve 18, 20, 22, on continue ainsi à partir du multiple $k \times 9$ en allant de deux en deux jusqu'au multiple $k \times 11$, par exemple 36, 38, 40, 42, 44, etc. (Ici on voit que 41 manque). Du côté de 79 la série est $72 = 8 \times 9$, 74, 76, 78, 80, …, $88 = 8 \times 11$.

Il reste à montrer qu'au-delà de 80, on peut payer toutes les sommes. L'idée est très simple : si l'on peut payer une somme s, on peut payer aussi[35] $s + 9$, $s + 18$, $s + 27$, etc. Mais, comme on a toutes les sommes entre 80 et 88, on a, pour le dire savamment, toutes les congruences modulo 9, donc on va pouvoir tout

[34] Mais on voit bien que si l'on en prenait un 11 de plus, on aurait un multiple de 9, à savoir 90.

[35] On peut aussi ajouter 11, 22, etc.

obtenir. De manière élémentaire, si l'on ajoute 9 à 80, on voit qu'on obtient 89 (donc on fait la jonction avec 88) et avec 81,…, 88 on obtient les 8 suivants jusqu'à 97. En recommençant avec 89, 90, …, 97 on obtient 98 et les 8 suivants, etc.

Quand on part d'une somme fixée, par exemple 118, on peut procéder par essais et erreurs, mais si l'on veut éviter cela, le raisonnement est le suivant. On divise 118 par 9 : $118 = 9 \times 13 + 1$, le reste est 1. Pour trouver le point de départ convenable entre 80 et 88 on prend le nombre dont le reste est 1, c'est 82 et on a $118 - 82 = 36 = 4 \times 9$. Comme on a $82 = 5 \times 11 + 3 \times 9$ on trouve $118 = 5 \times 11 + 7 \times 9 = 55 + 63$.

Dans le cas de 417, on a $417 = 9 \times 46 + 3$ et $84 = 9 \times 9 + 3$. Comme on a $84 = 6 \times 11 + 2 \times 9$, on ajoute $417 - 84 = 333 = 37 \times 9$. On obtient la solution $417 = 6 \times 11 + 39 \times 9$.

Bien sûr, quand on sait que la congruence modulo 9 d'un nombre est aussi celle de la somme de ses chiffres, par exemple qu'on a $417 \equiv 4 + 1 + 7 \equiv 3 \pmod 9$, on trouve le résultat bien plus vite.

On obtient ainsi une solution. Pour les avoir toutes il suffit de remplacer 11×9 par 9×11 jusqu'à plus soif et on trouve $417 = 15 \times 11 + 28 \times 9$ puis $417 = 24 \times 11 + 17 \times 9$ et enfin $417 = 33 \times 11 + 6 \times 9$. Ce qui est derrière est le résultat suivant :

2.6 Lemme. *Si l'on a $9a + 11b = 9c + 11d$, avec, par exemple, $a < c$, on a $c - a = 11k$ et $b - d = 9k$ avec $k > 0$.*

Démonstration. On a $9(c - a) = 11(b - d)$ et, comme 11 est premier avec 9, il divise $c - a$ par Gauss, donc on a $c - a = 11k$ et on en déduit $b - d = 9k$.

On peut aussi trouver ces solutions en écrivant quelques lignes de programme.

Pour déterminer le nombre de solutions dans le cas général le mieux est d'écrire une relation de Bézout avec 1, par exemple $1 = 5 \times 9 - 4 \times 11$. Cela donne $n = 5n \times 9 - 4n \times 11$ et le raisonnement ci-dessus montre que toutes les solutions de l'équation $n = 9a + 11b$ sont de la forme $n = (5n - 11k) \times 9 + (9k - 4n) \times 11$, avec $k \in \mathbb{Z}$. Pour avoir des coefficients $a, b \geq 0$, il suffit que $5n - 11k$ et $9k - 4n$ soient ≥ 0. Cela signifie $\frac{4n}{9} \leq k \leq \frac{5n}{11}$. Si l'écart est ≥ 1 on est sûr de trouver un entier. Comme l'encadrement s'écrit $\frac{44n}{99} \leq k \leq \frac{45n}{99}$, c'est évidemment vrai pour $n \geq 99$.

Traitons l'exemple de 417. On écrit $417 = (5 \times 417 - 11k) \times 9 - (9k - 4 \times 417) \times 11$ et il faut que les deux coefficients soient ≥ 0 ce qui donne $185.33 \leq k \leq 189.54$, donc $k = 186, 187, 188$ ou 189 et retrouve les quatre solutions ci-dessus.

Pour une discussion approfondie sur ce thème, voir :

https://www.imo.universite-paris-saclay.fr/~daniel.perrin/CAPES/arithmetique/diophantepositif.pdf

8.3. En rendant la monnaie

Pour traiter le cas général il suffit d'écrire une relation de Bézout avec 1 et les deux plus simples sont $1 = 55 - 54 = 5 \times 11 - 6 \times 9$ ou $1 = 45 - 44 = 5 \times 9 - 4 \times 11$. À partir de ces relations, on trouve tous les entiers n en multipliant ces relations par n.

Cela étant, la solution ainsi obtenue n'est pas toujours optimale (au sens où $|a| + |b|$ est minimal : manipuler le moins de pièces possible). Ainsi on trouve avec cette procédure $13 = 13 \times 5 \times 11 - 13 \times 6 \times 9$ alors qu'on peut faire $13 = 22 - 9$. Pour trouver la plus petite solution on peut partir d'une de celles dont

on dispose $n = 11a - 9b$ et prendre $11(a - 9k) - 9(b - 11k)$ en prenant pour k un entier tel que $|a - 9k|$ et $|b - 11k|$ soient les plus petits possibles.

Attention, si $n > 99$ il n'y a pas de raison que les quotients euclidiens de a par 9 et de b par 11 soient les mêmes. Par exemple, avec $417 = 2085 \times 11 - 2502 \times 9$ on a $2085 = 231 \times 9 + 6$ et $2502 = 227 \times 11 + 5$. En prenant au milieu 229 on trouve $417 = 24 \times 11 + 17 \times 9$, avec un coût $c = 24 + 17 = 41$, mais on peut faire mieux avec $33 \times 11 + 6 \times 9$, $c = 39$. Quelques lignes de programme montrent que c'est le meilleur résultat possible.

Voici les réponses optimales pour les sommes proposées : $13 = 22 - 9$, coût en nombre de pièces 3, $41 = 63 - 22$, coût 9, $79 = 88 - 9$, coût 9.

Le lecteur curieux et patient pourra établir le résultat général :

2.7 Proposition. *Soit n un entier positif. On écrit $5n = 11q + r$ avec $0 \leq r < 11$. La solution optimale de l'équation $9x+11y = n$ dans $\mathbb{Z}$ (c'est-à-dire celle pour laquelle $|x|+|y|$ est minimum) est donnée par $x = 5n + 11k$ et $y = -4n - 9k$ avec k défini comme suit :*

A) *Si $q \geq 4r$, on a $k = -q$ et le minimum vaut $n - 2q$.*

B1) *Si $q < 4r$ et $9r \leq q + 50$, on a $k = -q$ et le minimum vaut $9n - 20q$.*

B2) *Si $q < 4r$ et $9r > q + 50$, on a $k = -q - 1$ et le minimum vaut $-9n + 20q + 20$.*

2.8 *Remarque*. Le cas B1 se produit pour les n suivants : 1, 3, 5, 7, 10, 12, 14, 16, 21, 23, 25, 30, 32, 34, 41, 43, 50, 5, 61, 70. Le cas B2 pour les n suivants : 2, 4, 6, 8, 13, 15, 17, 19, 24, 26, 28, 35, 37, 39, 46, 48, 57, 59, 68, 79. Pour tous les autres n on est dans le cas A.

C'est une situation très riche et il me semble qu'il faut admettre, dans un premier temps, des solutions artisanales par approximations successives. Qui n'a jamais tâtonné pour trouver un résultat mathématique ne s'est sans doute jamais frotté à un résultat un peu difficile. Bien entendu, ensuite, il est important de donner aussi des méthodes fiables et certaines.

C'est enfin un thème où l'utilisation de l'ordinateur apporte beaucoup. Du point de vue mathématique, le ressort de l'exercice est le fait que 9 et 11 étant premiers entre eux ils vérifient une relation de Bézout. Le théorème de Gauss n'est pas très loin non plus.

III - ANNEXE 1 : QUELQUES COMPLÉMENTS

Je donne ici quelques démonstrations de résultats utilisés dans ce qui précède, avec des versions relativement élémentaires[36], renvoyant le lecteur qui voudrait en savoir plus à [1].

1. Deux axiomes

Les deux axiomes ci-dessous seront essentiels pour les démonstrations. On peut les considérer comme intuitivement évidents.

Il y a d'abord l'axiome de « bon ordre » sur les entiers :

[36] Mais rédigées pour des professeurs, pas pour des élèves.

3.1 Axiome. *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

Cet axiome, évoqué par René Cori dans sa conférence, est essentiellement équivalent au principe de récurrence, voir [1] chapitre 1. Il s'utilise en raisonnant par « absurde et minimalité » : pour montrer qu'une propriété (P) portant sur les entiers est vraie, on suppose qu'elle ne l'est pas, elle admet donc un contre-exemple et on choisit un tel contre-exemple minimal.

Il y a ensuite le caractère archimédien de $\mathbb{N}$:

3.2 Axiome. *Étant donnés deux entiers a et N de* $\mathbb{N}$*, avec* $a > 0$*, il existe un entier n tel que* $na \geq N$.

Cet axiome est la traduction d'un nombre incalculable de proverbes du genre : *les petits ruisseaux font les grandes rivières.*

2. La division euclidienne

3.3 Théorème. *Soient* $a, b \in \mathbb{N}$ *avec* $b > 0$*. Il existe des entiers q et r uniques tels que* $a = bq + r$ *et* $0 \leq r < b$.

Démonstration. Le cas $a = 0$ étant évident on peut supposer $a > 0$. En vertu de **3.2** il existe un entier $n > 0$ tel que $bn \geq a$. On considère alors le plus petit de ces entiers (il existe d'après **3.1**). On le note $q + 1$ et le couple q, $r = a - bq$ convient.

Pour l'unicité on suppose qu'on a $a = bq + r = bq' + r'$ avec, par exemple, $q < q'$. On écrit $b(q'-q) = r - r'$ et on a une contradiction avec les hypothèses sur r, r'.

3. Existence et unicité de la décomposition en produit de facteurs premiers

On suppose qu'on a défini les nombres premiers.

3.4 Théorème. *Soit a un entier positif. Alors a s'écrit, de manière unique, sous la forme* $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ *avec* $r \geq 0$*, les* p_i *premiers vérifiant* $p_1 < p_2 < \dots < p_r$ *et les* $\alpha_i > 0$.

3.5 *Remarques.* 1) Le cas $r = 0$ (produit vide) correspond à $a = 1$.
2) L'existence d'une décomposition en produit d'irréductibles est banale (elle est vraie dans tout anneau noetherien). En revanche l'unicité caractérise ce qu'on appelle les anneaux factoriels.

Démonstration. On utilise systématiquement le raisonnement par absurde et minimalité.
1) Existence. Sinon il y aurait un plus petit entier a ne s'écrivant pas sous la forme annoncée. En particulier, a n'est pas premier, donc s'écrit $a = bc$ avec $b, c < a$. Mais alors b et c ne sont plus des contre-exemples, donc sont produits de nombres premiers et a aussi, ce qui est absurde.
2) L'unicité est plus difficile. On commence par montrer le lemme d'Euclide[37]:

3.6 Lemme. *Soient a, b des entiers positifs. Si un nombre premier p divise le produit ab il divise a ou b.*

Démonstration. Le résultat est évident si a ou b est égal à 1. On peut donc supposer $a, b \geq 2$.
On raisonne par absurde et minimalité : on suppose que la propriété n'est pas vraie et on prend le plus petit ab qui soit un contre-exemple et, pour cet ab, le plus petit p qui mette en défaut le lemme. On a donc

[37] Pour une preuve via Bézout et Gauss, voir [1], pour une preuve plus proche de celle d'Euclide, voir le paragraphe suivant.

$ab = pc$. L'hypothèse de minimalité implique $a, b < p$ (sinon en les divisant par p on a un exemple plus petit) et on en déduit $c < a < p$, $c < b < p$ et $c > 1$ car p est premier. Mais, c admet un diviseur premier q (c'est l'existence de la décomposition), on a $c = qc'$ et, comme q est plus petit que p et divise ab, ce n'est plus un contre-exemple, donc il divise a par exemple. On a donc $a = qa'$ et $a'b = c'p$. Comme $a'b$ est plus petit que ab, ce n'est plus un contre-exemple, donc p divise a' ou b, donc a ou b.

3.7 Corollaire. *Si un nombre premier p divise un produit de nombres premiers $q_1 \dots q_r$ il est égal à l'un d'eux.*

Démonstration. Sinon, on prend un contre-exemple avec le nombre r de facteurs minimum et on applique le lemme d'Euclide pour avoir une contradiction.

Revenons à l'unicité. On prend encore un plus petit contre-exemple, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r} = q_1^{\beta_1} \dots q_s^{\beta_s}$. Le corollaire du lemme d'Euclide montre que p_1 est égal à l'un des q_i. En divisant les deux membres par ce nombre on a un contre-exemple plus petit et c'est absurde.

4. Retour sur le lemme d'Euclide

Lors du colloque est apparu plusieurs fois un théorème qui semble avoir été communément admis dans l'enseignement au XIXème siècle et au début du XXème et qui porte sur l'écriture d'un rationnel sous forme de fraction irréductible. Ce résultat est notamment à la racine de preuves de l'irrationalité de $\sqrt{2}$ et d'autres qui ont été abordées dans les ateliers animés par Nathalie Chevalarias, par Fréderic Laurent et dans la conférence de Véronique Battie. J'essaie de faire le point sur ce thème, en revenant pour l'essentiel à Euclide, mais dit en langage moderne.

4.1. L'énoncé

Le résultat évoqué ci-dessus est le suivant :

***3.8* Théorème**. *Soient a, b, c, d des entiers positifs. Si l'on a $\frac{a}{b} = \frac{c}{d}$ et si a et b sont premiers entre eux, alors il existe e tel que $c = ae$ et $d = be$. En particulier, l'écriture d'un rationnel sous forme de fraction irréductible est unique.*

Ce théorème est essentiellement la réunion des propositions 20 et 21 du Livre VII d'Euclide.

4.2. Conséquences

Le théorème **3.8** a deux corollaires essentiels : le lemme d'Euclide (voir **3.6** ci-dessus) et l'irrationalité de $\sqrt{n}$ où n est un entier qui n'est pas un carré parfait.

Traitons **3.6**. On suppose que p divise ab. S'il divise a on a fini. Sinon, on écrit $ab = pc$ et on a $\frac{a}{b} = \frac{c}{d}$.
Comme p ne divise pas a, il est premier avec a, donc, par **3.8**, il divise b.
Montrons maintenant l'irrationalité de $\sqrt{n}$. Si $\sqrt{n}$ est rationnel, on a $\sqrt{n} = \frac{a}{b}$ avec a, b positifs et premiers entre eux, donc $n = \frac{a^2}{b^2}$ et a^2 et b^2 sont encore premiers entre eux (c'est le lemme d'Euclide !). On a donc $\frac{n}{1} = \frac{a^2}{b^2}$ et par **3.8**, on a $1 = b^2e$ et $n = a^2e$. Mais la première égalité impose $b = e = 1$ et on a donc $n = a^2$, contrairement à l'hypothèse.

4.3. La preuve de 3.8

La preuve d'Euclide n'est pas très facile à suivre à cause notamment de l'emploi de la notion : être des parties de *dont la définition n'est pas très claire et qui est donc délicate à utiliser. J'en donne une variante dont le ressort est la division euclidienne, qui est aussi à la base de tout le Livre VII.*

Une remarque d'abord. Si l'on a $\frac{a}{b} = \frac{c}{d}$ avec des entiers positifs et si $a \leq c$, alors on a $b \leq d$. En effet, sinon on a $b > d$ et $ad = bc$. Mais $a \leq c$ et $d < b$ implique $ad < bc$ et c'est une contradiction.

Le théorème repose alors sur le lemme suivant (proposition 20 d'Euclide) :

3.9 Lemme. *Soit r un rationnel. On suppose qu'on a deux écritures sous forme de fractions : $r = \frac{a}{b} = \frac{c}{d}$ où a, b, c, d sont des entiers positifs et où a est le plus petit entier vérifiant cette propriété. Alors il existe e tel que $c = ae$ et $d = be$.*

Démonstration. On divise c par a et d par b (voir **3.3**) : $c = ae + r$ avec $0 \leq r < a$ et $d = bf + s$ avec $0 \leq s < b$. On en déduit $ad = bc = abf + as = abe + br$ (*). Si r est nul on a $c = ae$ mais aussi $abf + as = abe$. En simplifiant par a on voit que b divise s, ce qui impose $s = 0$, puis $f = e$ et on a le résultat.
Si r est > 0 on a $as < ab$ et $br < ab$, de sorte que les deux expressions de (*) sont des divisions euclidiennes de $ad = bc$ par ab. En vertu de **3.3** on a unicité du reste, donc $as = br$, soit encore $\frac{a}{b} = \frac{r}{s}$ et comme on a $r < a$, cela contredit l'hypothèse de minimalité.
On peut alors finir de prouver **3.8**. Il suffit de montrer que la fraction irréductible a/b avec a, b premiers entre eux est celle qui a le plus petit a possible. Sinon on écrit $\frac{a}{b} = \frac{u}{v}$ avec u le plus petit possible (qu'une telle écriture existe vient de l'axiome du bon ordre **3.1**) et on suppose $u < a$. Mais, par le lemme **3.9**, on a alors $a = ue$ et $b = ve$ avec $e > 1$ et cela contredit le fait que a et b sont premiers entre eux.

5. Le principe des congruences

Le résultat le plus utile concerne la multiplication :

3.10 Lemme. *Si l'on a $x \equiv a \pmod n$ et $y \equiv b \pmod n$, alors on a $xy \equiv ab \pmod n$.*

Démonstration. Il s'agit de montrer que n divise $xy - ab$. C'est une vieille ruse, on écrit $xy - ab = x(y - b) + b(x - a)$.

6. Les carrés modulo *p*

Il s'agit de montrer, de manière élémentaire, que -1 est un carré modulo p (premier impair) si et seulement si p est congru à 1 modulo 4. On a vu que ce résultat intervient dans la recherche des nombres premiers de la forme $a^2 + 1$. Même si l'on peut ne pas parler de congruences au collège et au lycée, je le fais par commodité. Avec des élèves on parlera des restes dans la division euclidienne.

Dans tout ce qui suit p désigne un nombre premier impair.

3.11 Lemme. *Soit a un reste non nul modulo p. Les restes des ab, pour b = 1, …, p − 1 sont tous distincts.*

Démonstration. En effet, si $ab \equiv ab' \pmod p$, p divise $a(b - b')$ donc $b - b'$ par Euclide, donc $b = b'$.

3.12 Corollaire. *Soit a un reste non nul modulo p. Il existe un unique reste b tel que $ab \equiv 1 \pmod p$. On parle de l'inverse de a modulo p.*

Démonstration. Comme les restes des ab, pour $b = 1 \ldots p-1$, parcourent les restes non nuls et sont tous distincts, ils les atteignent tous[38].

3.13 Corollaire. *Le reste $p-1$ (ou -1) modulo p est un carré si et seulement si $p \equiv 1 \pmod 4$.*

Démonstration. Posons $p-1 = 2k$. On regarde les $p-1$ restes de la division par p. On note d'abord que les restes de a^2 et de $(p-a)^2$ sont égaux (car $(p-a)^2 = p^2 - 2ap + a^2 \equiv a^2 \pmod p$). On a donc k restes des carrés parmi lesquels évidemment 1. On note ensuite que si $ab \equiv 1$ on a aussi $a^2b^2 \equiv 1$ par un calcul similaire. Si c est le carré de a et si d est l'inverse de c, soit b l'inverse de a. Comme on a $a^2 \equiv c$ et $a^2b^2 \equiv 1$ et comme d est unique, on a $d \equiv b^2$, autrement dit, d est aussi un carré. De plus, si $c \not\equiv 1$, c et d sont distincts. En effet, sinon on aurait $c^2 \equiv 1$, ce qui signifie que p divise $c^2 - 1 = (c-1)(c+1)$ et on conclut par le lemme d'Euclide. (Bien entendu, si p n'est pas premier c'est faux, par exemple, modulo 8 on a $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1$). Les carrés distincts de ± 1 se regroupent donc deux par deux (un carré et son inverse) et il y en donc un nombre pair $2m$. Pour faire k il ne reste que 1 et éventuellement -1 qui est un carré si et seulement si k est pair, donc $p \equiv 1 \pmod 4$.

7. Le petit théorème de Fermat

Il y a beaucoup de preuves de ce théorème (en utilisant la théorie des groupes, les coefficients binomiaux, etc.) En voici une très simple.

3.14 Théorème. *Soit p un nombre premier. On a les congruences $a^p \equiv a \pmod p$ pour tout a et $a^{p-1} \equiv 1 \pmod p$ si a n'est pas multiple de p.*

Démonstration. Il suffit de montrer le second point. Soit a un entier compris entre 1 et $p-1$. On considère le produit $N := \prod_{b=1}^{p-1} b$. On a $a^{p-1}N = \prod_{b=1}^{p-1} ab$. Mais on a vu que les congruences des ab sont toutes distinctes (cf. **3.11**), donc qu'elles parcourent les entiers de 1 à $p-1$, de sorte qu'on a $a^{p-1} N \equiv N \pmod p$. Comme p ne divise pas N (par le lemme d'Euclide), il divise $a^{p-1} - 1$ (par le même argument).

8. Solution d'un exercice

3.15 Proposition. *Soit n un entier > 2. Alors l'un des nombres $n! + 1$ et $n! + n + 1$ est composé.*

Démonstration. Si $n+1$ n'est pas premier il admet un diviseur premier $p \leq n$ et p divise $n!$ et $n+1$ donc $n! + n + 1$ qui est donc composé. Si $p := n+1$ est premier on sait qu'on a $(p-1)! \equiv -1 \pmod p$ (c'est le théorème de Wilson, que l'on prouve en regroupant les classes $\bar{a}$ et $\bar{a}^{-1}$ de $\mathbb{Z}/p\mathbb{Z}$). Autrement dit, $p = n+1$ divise $n!+1$ et, comme n est plus grand que 2, c'est un diviseur strict et on a gagné.

[38] Quand on est savant on dit qu'injectif implique surjectif, mais on n'a pas attendu d'avoir ces mots pour comprendre ça.

9. Quelques messages à décrypter

9.1. Deux messages par substitution

EYVOZMTVKGPPGLAGQGXOTAPQMBMPMBGZYGBPMPJSVGKMAL
TYEVGEYBCAFYGTGEZGOAPGEPOBPMPFGEMYTVGETOYGEFAQ
YBGAEGEXOTPYGEVGELMFGPEQOFRGTQGEBAOBKOYGBPGPOB
YQOYGBPFGEBMYTGEXTMRMBVGATEVGKGXOSEMTYCYBOF

NGWBLOINOAPMPOWBUWQMBBQDMQPOIIGWVVLOIWBA
OVMQPOAOPMQPHMTGBHWZOTLGWQIIOSOZPHOPGQPIH
OAJOSQZOOIHOBWOIHONLMAOIHOVLOAJOIHOALGAJOBI

9.2. Deux messages codés par Vigenère

Le code de Vigenère (1523-1596) permet de contrer l'analyse de fréquence. Le principe est le suivant : on choisit un mot clé, par exemple le mot CODE, qui correspond aux nombres 3, 15, 4, 5. On décale la première lettre du message de 3 crans, la deuxième de 15, la troisième de 4, la quatrième de 5, puis on recommence, la cinquième de 3, etc. Si on dépasse Z on continue avec A. Avantage : la même lettre n'est pas forcément codée par le même caractère, donc l'analyse de fréquence ne marche plus.

Un exemple, le message à coder :

RENDEZ-VOUS EN PRISON VOUS NE PASSEZ PAS PAR LA CASE DE DEPART VOUS NE TOUCHEZ PAS VINGT MILLE EUROS

Le message codé :

UTRIHOZTXHISSGMXRCZT XHRJSPW XHOTFVEEWOPG FVTHJGTTFUI ZTXHRJWDYH KTDUDHZNQVXRLAPJHJVTV

Pour décrypter Vigenère on repère des groupements fréquents :

UTRIHOZTXHISSGMXRCZTXHRJSPW XHOTFVEEWOPG FVTHJGTTFUI ZTXHRJWDYH KTDUDHZNQVXRLAPJHJVTV

et on en déduit la longueur du mot clé (ou au moins un multiple de cette longueur).

Voir http://www.dcode.fr/chiffre-vigenere

Un exemple facile codé par Vigenère :

npw fpgqoiwcw npw rwyu aitqstxepew, npw opmnwiwcw, ep wqyx npw tzfqew.
kww elpefpgyx vzyvpw npw ezqdtrctwqyw, kww pp wg qevtkwprv ueolmu.
dm xzyu lvttzgk e fpgtjtvpv ep qgdwcri, xzyu aswcvgk zqfw opwwcit lyz csdzxu.
dmpzr, xzyu oixpd gygqci vcexlmnwit fr rpy. ezytlkg.

Un exemple plus difficile :

zvtolgvfscgkdaavfkebidgnbscsmgslppyfksgcstsravruuldvfscsewtpsjabgsehosfmmqsstwu
vaveeoizkolhcwsnzlkdgtwacgzvkaacelelhvjelhfmtcollrcqygscbfftnczftaclluksuwnbsjarcfgd
uqelalqsegnrseiumwzdncgkhaqjisiqsdtlypcwqsskguqgvlrmagwnrarasnzllorqvdarsdgiebv
iuczrhuggjsnasuwbgsebuesiwtbwjlilulwrjsmjagrrneazvxaslhmicgkhrmdiwmcbkueoiffnm
adwlcpffscbjgujoisiqcewsrbrlupscdekseleeocwelhfmsjsjzokavkerozfsgelwlyrznepgzleb
segsmdzfimbjfetwvftnojveashmejsjmnqgfftnzlkrywjgnlosdeqelwlcgrmtpsjeaggjwujsdwn
rrvueoivfosgtgnbizkolgegsnsekecggsrbwmwrqsjnogsjwtlstgnqwuwrmbjhaqzvkmcavkcfc
jwsaoiuelsjlpygrkscnusvmwideqdiatzceeaggcwppweuinocwsrrvdandcaqssiticbcwsnzlkg
poeveqodwsqcelcydrtlcguwsnzlkgpoevstwtwsyijkizwvfqssuwsnzlkgpoeveqjvjtsgvlccioiu
gbveapqywnrelwfmfkdelhveelhgwutselatoeueppvsuaclhdyjrftyuvkijgjmitseltmiagupgcwd
pczlcfsdanoivfedcelccioiugqfmrcbkwtoizkelscgiebvft

9.3. *Un exemple de codage RSA*

Ma signature encodée en ASCII et cryptée c avec pq et e :

$$pq = 3182025935200771015207983046670052747435834209343862515620620481366 83$$
$$e = 94321654323578865325687908765434567779 99$$
$$c = 16710022994275830171960951435588588665707246512802868028703054827 8619$$

Pour des précisions sur le code ASCII on peut consulter :
https://fr.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

IV - RÉFÉRENCES

[1] Perrin D. *Mathématiques d'école*, Cassini, 2011.

[2] Perrin D. *Arithmétique et cryptographie*

https://www.imo.universite-paris-saclay.fr/~daniel.perrin/interdisciplines/Cours6cryptographie.pdf

email : *daniel.perrin@universite-paris-saclay.fr*

QUELS APPORTS DIDACTIQUES DE L'ARITHMÉTIQUE POUR LE RAISONNEMENT MATHÉMATIQUE ?

Véronique BATTIE
Université Claude Bernard Lyon 1
S2HEP (UR 4148)
veronique.battie@univ-lyon1.fr

Résumé
Dans les programmes actuels du Lycée, des pistes sont nouvellement mentionnées quant au raisonnement (e.g. envisager différentes preuves d'un même résultat, prouver sur un exemple générique) et nous proposons de les explorer dans le domaine de l'arithmétique à la lumière de travaux en didactique des mathématiques. Plus largement, nous tâchons d'apporter des éléments de réponse à la question des potentialités de l'arithmétique pour l'enseignement et l'apprentissage du raisonnement dans le Secondaire et à la transition Lycée-Université.

I - INTRODUCTION

Raisonner en arithmétique est-ce incongru ? Cette question rejoint ce qui est au cœur de nos recherches en didactique en mathématiques depuis le retour de l'arithmétique en 1998 dans les programmes du Secondaire après des années d'absence. De façon dialectique avec notre pratique enseignante en première année de Licence de mathématiques, nos recherches sont centrées sur l'étude des spécificités et potentialités de l'arithmétique, théorie des nombres élémentaire, pour l'apprentissage et l'enseignement du raisonnement mathématique à la transition Lycée-Université.

L'objet de la première partie de cette contribution est l'outil épistémologique dont nous avons eu besoin pour étudier les spécificités du raisonnement en arithmétique. Dans une seconde partie, nous tentons d'illustrer comment cet outil permet d'apporter des éléments de réponse à la question des apports didactiques de l'arithmétique pour le raisonnement mathématique. Nous concluons en abordant la question des ressources bibliographiques relatives à la didactique de l'arithmétique.

II - DIMENSIONS ORGANISATRICE ET OPÉRATOIRE DU RAISONNEMENT EN ARITHMÉTIQUE

Au sein du raisonnement en arithmétique, nous distinguons deux dimensions complémentaires, la dimension organisatrice et la dimension opératoire, en appui sur l'étude de textes historiques (Battie, 2003). La première s'identifie au raisonnement global qui traduit la mise en acte d'une visée : elle organise et structure les différentes étapes du raisonnement. La dimension opératoire quant à elle est relative à tout ce qui relève des manipulations de calcul opérées sur les objets en jeu et qui permettent la mise en œuvre des différentes étapes du raisonnement global suivi (dimension organisatrice). Sous quelles formes identifie-t-on spécifiquement en arithmétique chacune de ces dimensions ? Nous apportons dans ce qui suit des éléments de réponse à cette question et les exemples présentés éclairent ce que recouvre chacune

des deux dimensions. Nous mettons ensuite à jour comment ces dimensions sont susceptibles d'interagir dans le raisonnement en arithmétique.

1. Dimensions organisatrices en arithmétique

Au titre de premier exemple, la dimension organisatrice prend forme avec la visée de réduire la résolution d un problème à l'étude d un nombre fini de cas : la disjonction de cas qui exploite le concept de partition d un ensemble et la recherche exhaustive où l on teste une à une les solutions potentielles (avec préalablement ou non une phase de limitation de cette recherche).

Un deuxième pôle d exemples, appelé le jeu d extension-réduction et propre aux anneaux factoriels, apparaît avec la visée d'établir une propriété pour tout élément d un anneau factoriel : dans $\mathbb{Z}$, en appui sur le théorème fondamental de l'arithmétique, on montre que la propriété est multiplicative et qu elle est vraie pour tout nombre premier.

En arithmétique, « plonger » modulo un entier naturel n une égalité ou une équation relève de la dimension organisatrice. La visée associée peut être d'obtenir des critères de divisibilité. Et, articulée avec un raisonnement par l'absurde, la dimension organisatrice « plonger modulo n » permet aussi de montrer qu'une équation diophantienne n'a pas de solution. Le lecteur pourra se reporter à (Perrin, 2011, pp.24-26) pour illustrer ces deux exemples.

Enfin, la dimension organisatrice peut prendre formes à travers l exploitation de la propriété de bon ordre de l ensemble $\mathbb{N}$: raisonnement par récurrence, descente infinie, raisonnement par l absurde et minimalité. Nous avons l'équivalence logique entre raisonnement par récurrence, descente infinie, et raisonnement par l absurde et minimalité. Néanmoins, il ne serait pas raisonnable de supposer une équivalence didactique. Un sondage auprès d'étudiants en première année de Licence de mathématiques en 2022-2023 vient appuyer cette position. Nous nous centrons sur la question suivante extraite du sondage :

> *Voici une démonstration de l'irrationalité de $\sqrt{2}$:*
> *Supposons par l'absurde que $\sqrt{2}$ soit rationnel, alors il existe a et b entiers naturels non nuls tels que $\sqrt{2} = \frac{a}{b}$. Montrons que a et b sont pairs : avec l'égalité précédente on a $2b^2 = a^2$ donc a^2 est pair et a aussi. Il existe un entier a' non nul tel que $a = 2a'$; d'où $2b^2 = 4(a')^2$ ou encore $b^2 = 2(a')^2$. Comme précédemment, on en conclut que b est pair. Ainsi, à partir des entiers a et b on obtient des entiers naturels a' et b' tels que $\sqrt{2} = \frac{a'}{b'}$, a'<a et b'<b. On a construit une suite infinie d'entiers naturels strictement décroissante et ainsi aboutit à une contradiction.*
> *Y a-t-il un lien entre cette démonstration et le principe de récurrence ? Expliquer votre réponse.*

D'un point de vue qualitatif, quatre types de réponses apparaissent : pas de réponse (type 0), réponse négative (type 1), réponse positive avec une explication que nous qualifions de hors-sujet (type 2) et réponse positive avec une explication qui serait à préciser (type 3). Chacun de ces types de réponses, à l'exception du type 0, est illustré en annexe : le lecteur trouvera une réponse de type 1 puis une réponse de type 2 et ensuite deux réponses de type 3. Les résultats de ce sondage font écho à d'autres travaux en didactique des mathématiques :

> *Des études didactiques (Gardes et al., 2016 ; Grenier, 2003, 2012 ; Grenier et Payan, 1998) ont montré que*

> *le concept de récurrence et le raisonnement associé sont très mal compris par la grande majorité des élèves et des étudiants de licence scientifique. Le « sens » de la récurrence et son intérêt comme outil de démonstration sont absents. De plus, l'idée qu'un raisonnement par l'absurde est incompatible avec un raisonnement par récurrence est très répandue […]. (Bernard et al., 2018)*

La dimension organisatrice « exploitations de la propriété de bon ordre de $\mathbb{N}$ » offre une piste didactique pour faire rencontrer principe de récurrence et raisonnement par l'absurde.

2. Dimensions opératoires en arithmétique

Pour la dimension opératoire nous identifions en arithmétique plusieurs pôles. Un premier pôle apparaît avec le choix de représentation des objets en jeu dans le raisonnement. Deux choix essentiels sont les suivants : la structuration autour des nombres premiers (en appui sur le théorème fondamental de l arithmétique), les réseaux réguliers liés à l ordre partiel de la relation divisibilité (congruences) et l'écriture des nombres dans différentes bases de numération.

Un deuxième pôle opératoire renvoie à l utilisation de théorèmes et de résultats admis au cours du raisonnement. Nous parlerons dans ce cas-là d'encapsulation de la dimension opératoire par analogie avec l'informatique[1].

Les manipulations algébriques opérées dans le raisonnement définissent un troisième pôle opératoire en incluant l utilisation des combinaisons linéaires d entiers.

Nous pointons enfin un quatrième pôle avec l ensemble des traitements relatifs à l articulation entre l ordre (partiel) divisibilité noté $|$ et l ordre (total) naturel noté $\leq$ au sein des entiers naturels. Ces traitements sont développés en appui sur :

- $\forall(m,n) \in \mathbb{N}^2, m|n \Longrightarrow m \leqslant n$
- $\forall(m,n) \in \mathbb{N}^2, m|n$ et $n|m \Leftrightarrow m = n \Leftrightarrow m \leqslant n$ et $n \leqslant m$
- Le plus grand commun diviseur coïncide pour les deux ordres

Nous illustrons cette articulation via une extraction de la dimension opératoire d'un processus de preuve arithmétique de l'irrationalité de $\sqrt{2}$. Soient a et b deux entiers premiers entre eux tels que $a^2 = 2b^2$. L'égalité précédente peut être lue en termes de divisibilité des deux façons suivantes :

- $2|a^2, 2 \leqslant a^2$
- $a^2|2b^2$ et d'après le théorème de Gauss, a^2 et b^2 étant premiers entre eux, on a $a^2|2, a^2 \leqslant 2$

Ainsi $a^2 = 2$.

[1] En programmation informatique, l'encapsulation de données est l'idée de cacher l'information de façon intentionnelle. Dans l'analogie que nous faisons, ce caractère intentionnel n'entre pas en jeu.

Ce qui permet de formuler la preuve suivante avec un raisonnement par l'absurde pour la dimension organisatrice.

> **Preuve A.** *Supposons par l'absurde que $\sqrt{2}$ soit rationnel, il existe a et b entiers naturels non nuls tels que $\sqrt{2} = \frac{a}{b}$. On suppose que a et b sont premiers entre eux. Avec l'égalité précédente, on a $a^2 = 2b^2$:*
> - $2|a^2$, $2 \leqslant a^2$
> - $a^2|2b^2$ *et d'après le théorème de Gauss, a^2 et b^2 étant premiers entre eux, on a* $a^2|2$, $a^2 \leqslant 2$
>
> *Ainsi $a^2 = 2$.*
> *On obtient une contradiction car 2 n'est pas un carré dans $\mathbb{N}$. En conclusion, $\sqrt{2}$ est irrationnel.*

L'analyse de la dimension opératoire du raisonnement en termes d articulation entre l ordre divisibilité et l ordre naturel nécessite une attention ciblée sur le sens de lecture des égalités en termes de divisibilité.

3. Interactions entre dimensions organisatrice et opératoire

Ces dimensions organisatrice et opératoire sont introduites avec l idée qu elles interagissent dans le raisonnement mathématique. Nous avons mis à jour quatre principales voies d interactions (Battie, 2003).

Il est tout d abord possible d identifier de façon privilégiée une dimension organisatrice donnée à un certain pôle opératoire. Le jeu d extension-réduction et la structuration autour des nombre premiers vont de pair. Une disjonction de cas ou une phase de limitation de recherche exhaustive est susceptible d'être définie en lien étroit avec l articulation entre l ordre divisibilité et l ordre naturel ; par exemple, au sein d une disjonction de cas définie à partir de l ordre naturel, les propriétés « être pair » et « être impair » peuvent être chacune associée spécifiquement à un des cas (ce qui peut être illustré à partir du problème « Déterminer les entiers naturels m et n tels que $19^m - 2^n$ soit un carré » (Battie, 2003)).

Un deuxième type d interactions se situe dans la façon dont les objets sur lesquels porte le travail opératoire influent sur la nature de la dimension organisatrice. Le lecteur pourra se reporter à (Battie, 2003) pour une illustration de ce type d'interactions à partir de preuves historiques du problème « Il n'existe pas de triangle rectangle en nombres dont l'aire soit un carré » (Goldstein, 1995).

Une troisième voie d interactions concerne l apparition de sous-dimensions organisatrices dans la dimension opératoire : le raisonnement prend forme via l imbrication de plusieurs dimensions organisatrices. En guise d'exemple, reprenons la preuve de l'irrationalité de $\sqrt{2}$ mentionnée dans le sondage présenté précédemment. Dans cette preuve, l'implication « $\forall a \in \mathbb{N}, 2|a^2 \Longrightarrow 2|a$ » est admise. Si on choisit de la démontrer, une preuve possible serait :

> **Preuve B.** *Supposons par l'absurde que $\sqrt{2}$ soit rationnel, il existe a et b entiers naturels non nuls tels que $\sqrt{2} = \frac{a}{b}$. Montrons que a et b sont pairs. Avec l'égalité précédente, on a $2b^2 = a^2$ donc a^2 est pair et a aussi : en raisonnant par contraposée, s'il existe k entier tel que $a = 2k + 1$, on aurait $a^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$ avec $2k^2 + 2k$ entier. Ainsi, il existe un entier a' non nul tel que $a = 2a'$, d'où $2b^2 = 4(a')^2$ ou encore $b^2 = 2(a')^2$. Comme précédemment, on en conclut que b est pair. Ainsi, à partir des entiers a et b on obtient des entiers naturels a' et b' tels que $\sqrt{2} = \frac{a'}{b'}$, a'<a et b'<b. On a construit une suite infinie d'entiers naturels strictement décroissante et on aboutit à une contradiction. En conclusion, $\sqrt{2}$ est irrationnel.*

Un raisonnement par contraposée complexifie la dimension organisatrice de la preuve initiale en s'imbriquant dans le raisonnement par l'absurde. Dans un sens de complexification inverse, cet exemple illustre aussi qu'en admettant un résultat prouvé dans le jeu opératoire (processus d encapsulation) une ou plusieurs dimensions organisatrices sont susceptibles de disparaître dans le raisonnement.

Enfin, on peut mentionner qu en spécifiant un objet de la dimension opératoire on peut éviter de spécifier la dimension organisatrice. Dans la preuve précédente, la dimension organisatrice principale est un raisonnement par l'absurde spécifié en descente infinie et l'objet fraction $\frac{a}{b}$ n'est quant à lui pas spécifié. Dans la preuve donnée ci-dessous, le raisonnement par l'absurde n'est pas spécifié, c'est l'objet fraction qui l'est via son représentant irréductible avec l'hypothèse que les entiers a et b sont premiers entre eux :

> **Preuve C.** *Supposons par l'absurde que* $\sqrt{2}$ *soit rationnel, il existe a et b entiers naturels non nuls tels que* $\sqrt{2} = \frac{a}{b}$ *avec a et b premiers entre eux. Montrons que a et b sont pairs. Avec l'égalité précédente, on a* $2b^2 = a^2$ *donc* a^2 *est pair et a aussi : en raisonnant par contraposée, s'il existe k entier tel que* $a = 2k + 1$*, on aurait* $a^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1$ *avec* $2k^2 + 2k$ *entier. Ainsi, il existe un entier a' non nul tel que* $a = 2a'$*, d'où* $2b^2 = 4(a')^2$ *ou encore* $b^2 = 2(a')^2$*. Comme précédemment, on en conclut que b est pair. Ainsi, on aboutit à une contradiction : à la fois a et b sont premiers entre eux et a et b sont pairs. En conclusion,* $\sqrt{2}$ *est irrationnel.*

Mise à part la spécification de l'objet fraction, les deux preuves précédentes ne différent pas du point de vue de la dimension opératoire. Elles diffèrent en termes de dimension organisatrice principale : un raisonnement par l'absurde spécifié en descente infinie est remplacé par un raisonnement par l'absurde non spécifié. Dans la descente infinie, on aboutit à une contradiction extrinsèque à la preuve (une suite infinie d'entiers naturels strictement décroissante est construite) et, dans le raisonnement par l'absurde non spécifié, on aboutit à une contradiction intrinsèque à la preuve (les entiers a et b sont à la fois premiers entre eux et non premiers entre eux).

III - TRAVAILLER LES INTERACTIONS ENTRE DIMENSIONS ORGANISATRICE ET OPÉRATOIRE A LA TRANSITION LYCÉE-UNIVERSITÉ

Pourquoi envisager de travailler avec les élèves et les étudiants les interactions entre dimensions organisatrice et opératoire du raisonnement ? Il s'agit tout d'abord de se référer à la pratique experte : dans ses raisonnements, dans le processus de preuve, un.e mathématicien.ne est en contrôle de ses interactions, c'est donc selon nous un enjeu de formation à la pratique des mathématiques. De plus, nous nous appuyons sur des travaux didactiques relatifs au raisonnement. Travailler ces interactions est susceptible de contribuer à l articulation des aspects syntaxique (lieu des opérations grammaticales indemnes de tout contenu, dépourvues de sens) et sémantique (lieu de la signification) et cela est d'autant plus important à la transition Lycée-Université où on observe un déséquilibre dans les pratiques à l Université (Deloustal-Jorrand et *al*., 2020 ; Alcock, 2010). Et, en appui sur les travaux de Durand-Guerrier (2005), travailler les interactions entre dimensions organisatrice et opératoire est aussi susceptible de contribuer au travail simultané sur les aspects logiques et mathématiques des concepts en jeu, les difficultés logiques étant très dépendantes des contenus mathématiques.

Aborder la question du comment travailler les interactions entre dimensions organisatrice et opératoire nécessite d'introduire des éléments de didactique de la preuve en mathématiques. C'est ce que nous faisons dans un premier temps avant de donner des pistes didactiques pour mettre en oeuvre ce travail à la transition Lycée-Université.

1. Preuves pragmatiques et preuves intellectuelles

Suivant le statut des connaissances engagées et la nature de la rationalité sous-jacente, Balacheff (1987) distingue les preuves pragmatiques qui sont intimement liées à l action et à l expérience, des preuves intellectuelles qui montrent que leur auteur a pris du recul par rapport à l action (la démonstration est une preuve intellectuelle particulière). L'évolution du rapport à la preuve en termes de passage de preuves pragmatiques à des preuves intellectuelles est un enjeu majeur des programmes du Cycle 4 (notamment à travers l'enseignement de la géométrie) et il reste d actualité à l entrée à l Université. Pour en témoigner, nous reproduisons ci-dessous une preuve produite par un étudiant en L1 mathématiques.

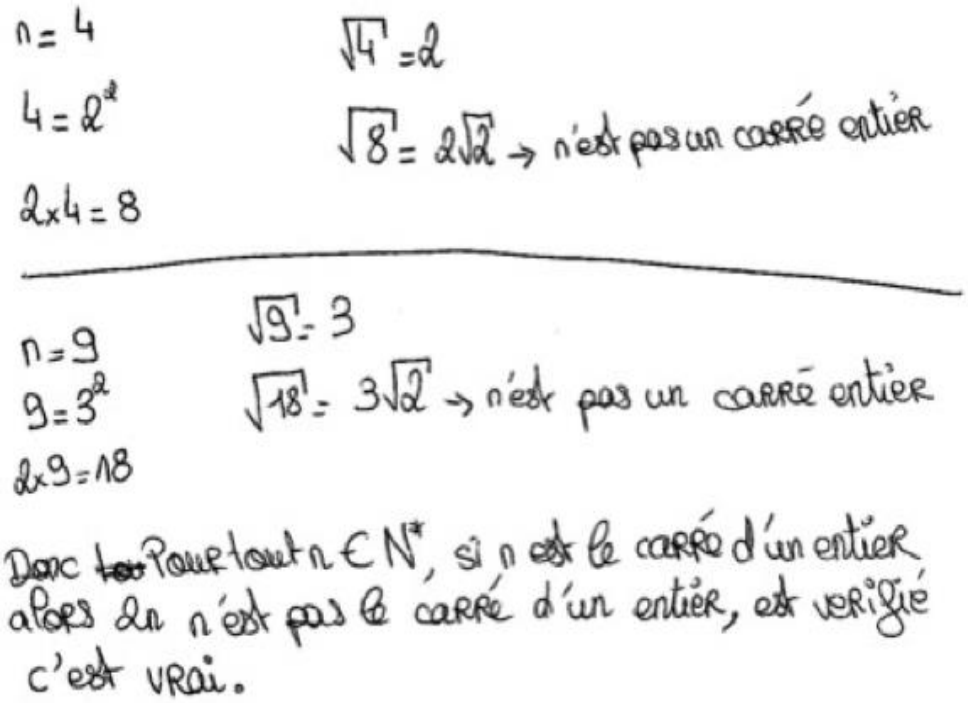


Figure 1. Empirisme naïf en L1 mathématiques

En arithmétique, l'empirisme naïf tel qu'il est défini par Balacheff est une preuve pragmatique où l'auteur mobilise un ou des exemples ayant le statut de preuve d'un énoncé avec quantification universelle.

En L1 mathématiques, l'empirisme naïf peut aussi apparaître au sein de la dimension opératoire d'une preuve. La production reproduite ci-après en témoigne.

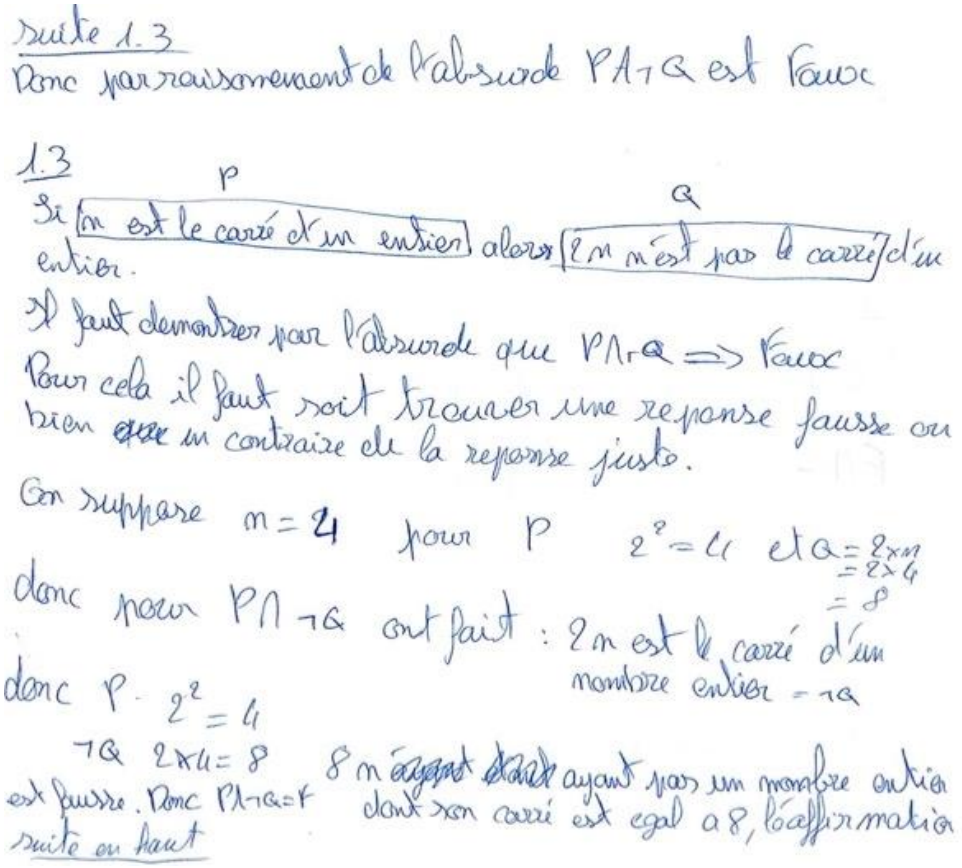


Figure 2. Empirisme naïf au sein de la dimension opératoire en L1 mathématiques

Dans cette preuve, on observe comment l'empirisme naïf parasite la dimension opératoire relative à la mise en œuvre de la dimension organisatrice principale (raisonnement par l'absurde nécessitant de nier une implication avec quantification universelle).

Parmi les preuves pragmatiques, Balacheff identifie aussi l'exemple générique nouvellement mentionné dans les documents d'accompagnement intitulés « Raisonnement et démonstration » des programmes de Seconde et Première de la voie générale (respectivement parus en août 2019 et novembre 2019) :

> *Une autre piste [de différenciation] consiste à démontrer un résultat sur un exemple générique. Il s'agit d'un exemple numérique ou d'un cas particulier dont le traitement n'entache pas une démonstration générale, en ce sens que les outils mobilisés et les modes de raisonnement sont assez facilement transférables au cas général. Dans certains cas, on peut s'en tenir à cet exemple en précisant qu'on admet le cas général.*

On retrouve bien la définition de l'exemple générique tel qu'il a été défini dans les travaux de Balacheff :

> *L'exemple générique consiste en l'explicitation des raisons de la validité d'une assertion par la réalisation d'opérations ou de transformations sur un objet présent non pour lui-même, mais en tant que représentant caractéristique d'une classe d'individus. La formulation dégage les propriétés caractéristiques et les structures d'une famille en restant attachée au nom propre et à l'exhibition de l'un de ses représentants. (Balacheff, 1987, p.20).*

Dans la partie qui suit, nous présentons l'idée d'activités multi-preuves spécifiquement en écho à cette définition et en guise de piste didactique pour travailler les interactions entre dimensions organisatrice et opératoire à la transition Lycée-Université.

2. Activités multipreuves de type generic proving

En référence à Leron et Zaslavsky (2013, p.24),

> *A generic proof is, roughly, a proof carried out on a generic example. We introduce the term generic proving to denote any mathematical or educational activity surrounding a generic proof.*

Et en écho à Dreyfus et *al*. (2012, p.198),

> *[…] a multiple proof tasks which explicitly require different types of proofs for the same mathematical statement*,

nous dénommons « activité multi-preuves de type generic proving » (generic proving multiple proofs tasks) toute activité où plusieurs preuves d'un même résultat mathématique sont fournies (et non demandées) dans une perspective de généralisation de ce résultat.

Pour concevoir ce type d'activités, l'enseignant.e a besoin d'être outillé.e pour mener une analyse comparative de preuves du résultat général en jeu. Une analyse en termes de dimensions organisatrice et opératoire répond à ce besoin et permet de sélectionner judicieusement un échantillon de preuves. Nous en donnons un exemple associé à la problématique d'accéder et de prouver le résultat suivant « Soit n un entier naturel, une condition nécessaire et suffisante pour que $\sqrt{n}$ soit rationnel est que n soit un carré d'entier » à partir de preuves arithmétiques de l'irrationalité de $\sqrt{2}$. Aux quatre preuves A, B et C rencontrées précédemment, nous ajoutons la preuve suivante :

> **Preuve D.** *Supposons par l'absurde que* $\sqrt{2}$ *soit rationnel, il existe a et b entiers naturels non nuls tels que* $\sqrt{2} = \frac{a}{b}$ *d'où* $2b^2 = a^2$. *On appelle* α *l'exposant de 2 dans la décomposition en facteurs premiers de a et* β *celui de b. D'après l'égalité précédente on a* $1 + 2\beta = 2\alpha$, *ce qui est en contraction avec « un nombre impair ne peut être égal à un nombre pair ». En conclusion,*$\sqrt{2}$ *est irrationnel.*

Les preuves A et D ont un pouvoir générique supérieur à celui des preuves B et C et cette hétérogénéité est recherchée dans la conception de ce type d'activités. Autrement dit, à partir des preuves A et D, nous pouvons aisément aboutir à une preuve du résultat général. Avec les preuves B et C, les preuves sont de plus en plus complexes du point de vue de la dimension organisatrice (de nouveaux cas apparaissent dans le raisonnement par contraposée) et aller vers une généralisation est problématique. Le ressort fondamental ici est identifié dans la dimension opératoire et plus précisément dans le choix de travailler sur les entiers via leur décomposition en produit de nombres premiers. Ce choix est explicite et directement utilisé dans la preuve D que nous qualifions de fondamentale. Dans la preuve A, c'est à travers l'utilisation du théorème de Gauss qu'il apparaît. Le lecteur pourra se reporter à Battie (2021) pour plus de détail.

Les preuves A à D constituent un ensemble hétérogène en termes de pouvoir générique et peuvent être exploitées à la transition Lycée-Université dans l'activité que nous présentons à présent.

Dans un premier temps, les consignes suivantes sont données à des groupes de 3 à 4 élèves/étudiants :

> *On rappelle qu'un nombre est rationnel si et seulement s'il peut s'écrire sous la forme d'une fraction $\frac{a}{b}$ avec a entier et b entier naturel non nul.*
>
> *1. Selon votre groupe, le nombre $\sqrt{2}$ est-il rationnel ou non rationnel ? Justifier votre réponse.*
> *2. Selon votre groupe, le nombre $\sqrt{3}$ est-il rationnel ou non rationnel ? Justifier votre réponse.*
> *3. A votre avis, pour quelles valeurs de n le nombre $\sqrt{n}$ est-il rationnel ? Tenter de démontrer votre conjecture.*

Dans un second temps, les preuves A à D sont fournies et accompagnées des consignes suivantes :

4. *De quelle preuve vos idées du ... sont-elles les plus proches ?*
5. *Choisir la preuve qui vous permet le plus facilement de démontrer l'irrationalité de $\sqrt{3}$ et écrivez la preuve associée.*
6. *On peut se demander pour quelles valeurs de n le nombre $\sqrt{n}$ est rationnel ; complétez la phrase suivante : « $\sqrt{n}$ est rationnel si et seulement si n est .....». Tenter de démontrer cette équivalence en vous inspirant de la preuve qui vous semble la plus facile à adapter.*

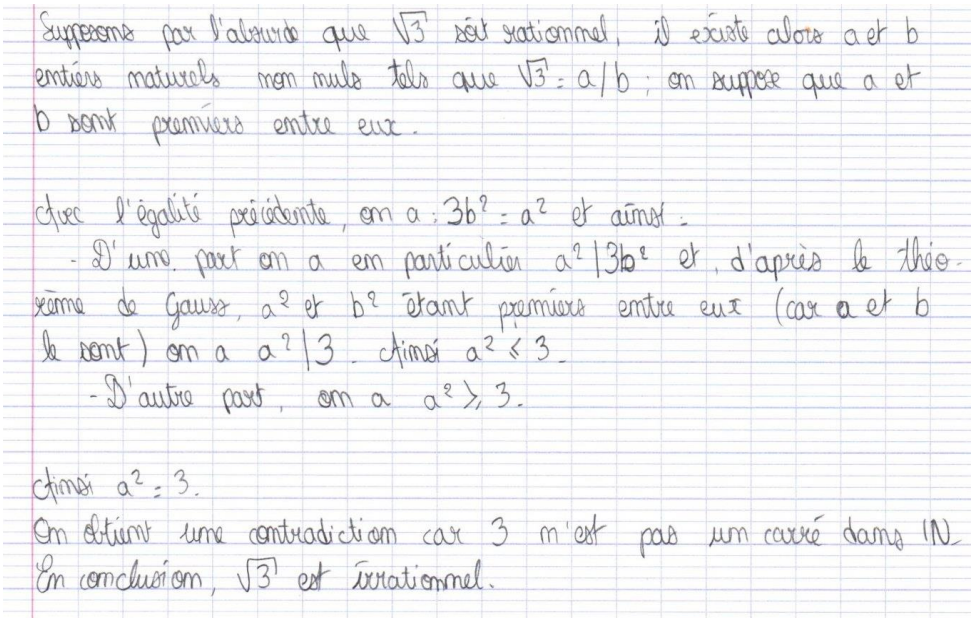
Dans cette activité, les élèves/étudiants sont amenés à analyser et produire des preuves de façon dialectique, plus précisément dans un jeu d'allers-retours entre lecture-analyse des preuves fournies et production de preuves. L'intérêt didactique de ce type d'activités est double en termes de travail sur les interactions entre dimensions organisatrice et opératoire : il permet à la fois d'exploiter le potentiel didactique des preuves génériques pour travailler sur la preuve en mathématiques et de prendre en charge le passage de preuve(s) générique(s) à une preuve générale. Cette caractéristique va dans le sens du conseil donné par le mathématicien Beardon à Rowland didacticien de l'arithmétique :

> *There is a sense in which you are reversing a familiar step. If a student dot not understand a proof one often suggests that he/she « works it through in a particular case ». What you are suggesting, I think, is that you reverse the order here with the added benefit that the student is confident before the formal proof rather than been depressed after it...I think that if you want to have a good chance of success you must not only develop the idea of the generic example, but also show how it really lead on to a formal proof. (Rowland, 2002, p.179)*

Les résultats des expérimentations menées (Battie, 2015, 2021) sont encourageants avec une préférence spontanée des élèves/étudiants pour les preuves génériques (preuves A et D). Ce constat est d'autant plus remarquable que la preuve communément rencontrée dans le Secondaire est la preuve C.

Néanmoins, dans la mise en œuvre de ce type d'activités, il faut rester vigilant sur deux points en particulier. Tout d'abord, il faut développer une vigilance quant au rapport des élèves/étudiants à la preuve. En effet, proposer plusieurs preuves d'un même résultat mathématique pourrait prêter à confusion quant à la suffisance d'une preuve pour établir la validité de ce résultat. De plus, il faut rester prudent quant à l'interprétation de ce que donne à voir une production écrite d'un élève/étudiant,

particulièrement dans le cas de l'exploitation des preuves génériques où les adaptations à faire sont minimes. Dans l'activité présentée précédemment, un élève/étudiant peut par exemple réécrire la preuve A uniquement en changeant « 2 » en « 3 ».


Supposons par l'absurde que $\sqrt{3}$ soit rationnel, il existe alors a et b entiers naturels non nuls tels que $\sqrt{3} = a/b$; on suppose que a et b sont premiers entre eux.

Avec l'égalité précédente, on a : $3b^2 = a^2$ et ainsi :
- D'une part on a en particulier $a^2 | 3b^2$ et, d'après le théorème de Gauss, a^2 et b^2 étant premiers entre eux (car a et b le sont) on a $a^2 | 3$. Ainsi $a^2 \leq 3$.
- D'autre part, on a $a^2 \geq 3$.

Ainsi $a^2 = 3$.
On obtient une contradiction car 3 n'est pas un carré dans $\mathbb{N}$.
En conclusion, $\sqrt{3}$ est irrationnel.

Figure 3. Preuve produite par un étudiant L1 mathématiques à partir de la preuve A de l'irrationalité de $\sqrt{2}$

Uniquement à partir de cette production, on ne peut être certain de l'authenticité de la compréhension des preuves en jeu et nous rejoignons Rowland avec cette citation :

> *I believe that the accounts given here of my work with undergraduates offer grounds for considerable optimism regarding the possibility of students "seeing" the generality we intend them to see in arguments based on particular cases. At the same time, it warns us against naïve complacency : we cannot be sure what they will see, and they may see considerably less than we might hope. (Rowland, 2002)*

En termes de limite didactique, nous n'avons pas avec cette activité la rencontre heureuse mentionnée par Hanna (2018, p.5) :

> *[...] it its often possible to find the happy concurrence in which a proof enlightens both the process of proving and the broader mathematical context with which it deals.*

En effet, cette activité ne donne pas accès aux propriétés permettant de manipuler les réels (Durand-Guerrier, 2019). En ce sens, et contre l'avis de Hanna (2018) et Steiner (1978), les preuves arithmétiques sont limitées selon nous en termes d explication mathématique de l irrationalité de $\sqrt{2}$. Cela renvoie à la traduction du problème dans le domaine de l'arithmétique :

> *[...] de nombreux problèmes d'irrationalité peuvent être étudiés au sein de l'arithmétique. [...] Ainsi (P) « $\sqrt{2}$ est irrationnel » signifie (Q) « $a^2 = 2b^2$ n'a pas de solution entière » et apparaît donc comme un théorème*

> *réellement arithmétique. Nous pouvons poser la question « $\sqrt{2}$ est-il irrationnel ? » sans sortir du champ de l'arithmétique […] (Hardy et Wright, 2007, p.47)*

On peut étudier le problème arithmétique en jeu (résolution dans Z de l'équation $a^2 = 2b^2$) sans disposer des nombres réels.

3. Conclusion

Lors des dernières rencontres du réseau INDRUM (International Network for Didactic Research in University Mathematics[2]), un élément de conclusion du groupe de travail centré sur la preuve et auquel nous participions a été formulé ainsi :

> *Finally, we consider that introducing specific work on proof and proving in University teacher training would be valuable, to initiate a change in the way proof is taught in general at university: moving from proof made in front of students, to students' proof elaboration and analysis. (Durand-Guerrier et Turgut, 2022, p.242).*

Les activités multi-preuves présentées précédemment, via un travail sur les interactions entre dimensions organisatrice et opératoire, nous semblent constituer une piste didactique allant dans le sens de cette recommandation. D'autres pistes existent et, en guise de conclusion, nous les mentionnons brièvement en indiquant les références de ressources bibliographiques correspondantes.

Nous pouvons tout d'abord mentionner les activités proposant aux élèves/étudiants une lecture critique de preuves erronées. Il peut s'agir par exemple de mettre à l'épreuve l'authenticité de la compréhension par les élèves/étudiants du principe de récurrence (Gardes et *al*., 2016).

Les activités proposant une analyse de preuves en fournissant une grille de lecture sont aussi une piste à explorer. Dans la Littérature, on parle de « tests de compréhension de preuves » (Conradie et Frith, 2000 ; Mejia-Ramos et *al.* 2012 ; Trouvé, 2022).

Au-delà de ces activités spécifiques, il nous semble important dans le travail sur le raisonnement de favoriser auprès des élèves et étudiants une mise en relief de ce qui relève spécifiquement de chacune des dimensions organisatrice et opératoire et de leurs interactions.

IV - REMARQUES CONCLUSIVES EN TERMES DE RESSOURCES BIBLIOGRAPHIQUES

Lors d'un entretien avec Jean-Louis Nicolas, théoricien des nombres, nous posions la question de la différence entre arithmétique et théorie des nombres et de leurs définitions respectives si différence il y avait. La référence donnée fut la *MSC* (*Mathematics Subject Classification)* où on identifie une rubrique à part entière *Number theory* et au sein de laquelle apparaît la sous-rubrique *Elementary number theory*.

Dans la littérature en didactique des mathématiques, l'arithmétique en tant que théorie des nombres élémentaire est identifiée au sein des mathématiques discrètes dans les publications de synthèse telle

[2] https://hal.science/INDRUM/

l'*Encyclopedia of Mathematics Education* ou tel un récent numéro du volume 54 de la revue *ZDM* (Volume 54, issue 4, August 2022). Il est regrettable que les travaux didactiques mentionnés dans ces publications soient essentiellement propres aux mathématiques discrètes hors arithmétique. Pour cette raison, les ouvrages dédiés spécifiquement à la didactique de l'arithmétique tels les ouvrages édités par Zazkis et Campbell (2002, 2006) sont à prendre en compte de façon complémentaire.

Depuis le retour de l'arithmétique en 1988 dans les programmes scolaires, les IREM ont publié de nombreuses brochures dédiées à son enseignement et ses potentialités didactiques. Bon nombre de ces revues n'ont pas été numérisées jusqu'à présent et restent peu visibles et difficilement accessibles pour les lecteurs intéressés. C'est ainsi que nous terminons en lançant un appel à recenser ces brochures au sein de l'ensemble des IREM, à communiquer l'inventaire via le portail des IREM pour plus de visibilité et à envisager leur numérisation pour une meilleure diffusion.

V - BIBLIOGRAPHIE

Alcock, L. (2010). Mathematicians perspectives on the teaching and learning of proof. In F. Hitt, D. Holton, P. Thompson (Eds.), *Research in Collegiate Mathematics Education*. VII (p. 63-91). American Mathematical Society.

Balacheff, N. (1987). Processus de preuve et situations de validation. *Educational Studies in Mathematics*. 18(2) 147-176.

Battie, V. (2003). *Spécificités et potentialités de l'arithmétique élémentaire pour l'apprentissage du raisonnement mathématique*, Thèse de Doctorat, Université Paris7, Paris.

Battie, V. (2015). Arithmétique et raisonnement mathématique en classe de terminale C&E au Gabon. *Revue africaine de didactique des sciences et des mathématiques*, 12.

Battie, V. (2021). Pouvoir générique d une preuve. *XXVIIème colloque CORFEM*, Strasbourg, France.

Bernard, D., Gardes D., Gardes M.-L., Grenier D. (2018). Une étude didactique du raisonnement par l absurde pour le Lycée. *Petit x*, 108, 5-40.

Campbell, S. R., Zazkis, R. (Eds.). (2002). LE*Learning and teaching number theory: Research in cognition and instruction*. Ablex Publishing.

Conradie, J., Frith, J. (2000). Comprehension tests in mathematics. *Educational Studies in Mathematics*, 42(3), 225-235.

Deloustal-Jorrand, V., Gandit, M., Mesnil, Z., da Ronch, M. (2020). Utilisation de l articulation entre les points de vue syntaxique et se´mantique dans l analyse d un cours sur le raisonnement. In T. Hausberger, M. Bosch, & F. Chellougui (E´ds.), *INDRUM2020 proceedings : Third conference of the International Network for Didactic Research in University Mathematics* (p. 378-387). University of Carthage and INDRUM.

Dreyfus, T., Nardi, E., Leikin, R. (2012). Cognitive development of proof. *In Proof and proving in mathematics education: the 19th ICMI Study*. Hanna, G. & de Villiers, M. (Eds), New York : Springer.

Durand-Guerrier, V. (2005). Questions de logique dans l'enseignement supérieur. *IIIe Colloque Questions de pédagogie dans l'enseignement supérieur*, Lille, France.

Durand-Guerrier, V. (2019). Travailler avec les preuves pour favoriser l'appropriation des concepts mathématiques. XXVIe *Colloque CORFEM*, Juin 2019, Strasbourg, France.

Durand-Guerrier, V., Turgut, M. (2022). TWG3: Teaching and learning of linear and abstract algebra, logic, reasoning and proof. In Trigueros, M., Barquero, B., Hochmuth, R. & Peters, J. (Eds) *INDRUM2022 Proceedings,* Hannover.

Gardes D., Gardes M.-L., Grenier D. (2016). Etat des connaissances des élèves de Terminale S sur le raisonnement par récurrence. *Petit x*, 67-98.

Goldstein, C. (1995). *Un théorème de Fermat et ses lecteurs* ; Presses Universitaires de Vincennes, Saint-Denis.

Hanna, G. (2018). Reflections on proof as explanation. In Stylianides, A. J. & Harel, G. (Eds.) *Advances in mathematics education research on proof and proving. An international perspective*. Springer.

Hardy, G.-H., Wright, E.-M. (2007). *Introduction à la théorie des nombres*. Vuibert.

Leron, U., Zaslavsky, O. (2013). Generic proving : Reflections on scope and method. *For the learning of Mathematics*, 33(3), 24-30.

Mejia-Ramos, J. P., Fuller, E., Weber, K., Rhoads, K., Samkoff, A. (2012). An assessment model for proof comprehension in undergraduate mathematics. *Educational Studies in Mathematics*, 79(1), 3-18.

Perrin, D. (2011). *Mathématiques d'école*. Cassini.

Rowland, T. (2002). Generic proofs in number theory. In Campbell, S. R., Zazkis, R. (Eds.), *Learning and teaching number theory: Research in cognition and instruction* (pp.157-183). Ablex Publishing.

Steiner, M. (1978). Mathematical explanation. *Philosophical Studies*, 34, 135–151.

Trouvé, T. (2022). *Apports des preuves génériques pour sonder la compréhension d'une preuve formelle à la transition secondaire–supérieur.* [Mémoire de master, Université Claude Bernard Lyon1]. https://dumas.ccsd.cnrs.fr/dumas-04071091v1

Zazkis, R., Campbell R.S. (Eds). (2006). *Number theory in mathematics education*. LEA Publishers.

VI - ANNEXE : ILLUSTRATION DES TYPES DE RÉPONSES AU SONDAGE AUPRES D'ÉTUDIANTS EN L1 MATHÉMATIQUES

Y a-t-il un lien entre cette démonstration et le principe de récurrence ? Expliquer votre réponse.

Non : la récurrence n'aboutit jamais à une contradiction, mais à une affirmation que la propriété P est bien vraie $\forall n \in$ à un ensemble. Il n'y a pas non plus d'initialisation ni même d'hypothèse pour un rang n, qui semble la base de la récurrence et de son raisonnement

Y a-t-il un lien entre cette démonstration et le principe de récurrence ? Expliquer votre réponse.

Oui il y a un lien entre cette démonstration et le principe de récurrence. Cette démonstration commence par une supposition et enchaine avec un "Montrons que", ce qui ressemble fort à l'hérédité dans le principe de la récurrence.

Y a-t-il un lien entre cette démonstration et le principe de récurrence ? Expliquer votre réponse.

Cette démonstration utilise un principe de récurrence car on construit une suite infinie de termes en utilisant les termes précédents.

Y a-t-il un lien entre cette démonstration et le principe de récurrence ? Expliquer votre réponse.

Il y a un lien entre cette démonstration et le principe de récurrence. En définissant a' en fonction de a on fait une récurrence avec des termes de plus en plus petit.
On peut donc voir l'utilisation du principe de récurrence bien que ce soit avec des termes de plus en plus petit et non pas de plus en plus grand comme habituellement.

ARITHMÉTIQUE ET LOGIQUE

René CORI
MCF retraité, Université Paris Cité
IMJ-PRG / IREM
cori@math.univ-paris-diderot.fr

Résumé
La logique, c'est l'étude du langage et du raisonnement, base de toute activité mathématique. Elle est donc omniprésente dans notre enseignement.
Nous suivons ici sa trace en arithmétique où, comme ailleurs, elle est parfois bien visible mais souvent soigneusement cachée, comme on le constate dans tous les manuels scolaires. Le raisonnement par récurrence est un exemple emblématique. Nous nous intéressons aussi à l'énoncé du théorème de Bézout et aux questions de langage qu'il soulève. Mais la logique est avant tout présente dans les fondements de l'arithmétique, sujet dont les élèves (voire les professeurs !) n'entendent pratiquement jamais parler. Nous présentons donc ici les axiomes de Peano et nous évoquons les modèles de l'arithmétique. Nous terminons par un résultat très troublant qui mêle inextricablement arithmétique et logique : le théorème de Goodstein.

DÉDICACE

Je dédie cet exposé à la mémoire de Pierre Audin, décédé le 28 mai dernier, et à celle de ses parents, Josette et Maurice Audin. Pierre était un formidable promoteur des mathématiques. Il les a fait découvrir sous leur meilleur jour à des milliers de jeunes au Palais de la Découverte, où il a été pendant plus de vingt ans responsable de la médiation pour notre discipline.

Pierre Audin sous un portrait de son père Maurice

Mais Pierre a aussi agi sans relâche pour perpétuer la mémoire de Maurice Audin, enlevé, torturé et tué à Alger par l'armée française en 1957 alors que Pierre avait à peine plus d'un mois. Maurice Audin était un jeune mathématicien qui luttait pour l'indépendance de l'Algérie aux côtés de Josette, également professeure de mathématiques, disparue en 2019. Pierre a été avec sa mère au premier rang d'un long combat pour que soit dite toute la vérité sur le sort réservé à Maurice Audin. Le 18 septembre 2018, le président de la République s'est déplacé au domicile de Josette Audin pour reconnaître officiellement la responsabilité de l'État dans la disparition de Maurice Audin et dans l'instauration d'un système de torture pendant la guerre d'Algérie. Ce geste solennel d'Emmanuel Macron a été une étape décisive dans cette lutte pour la vérité, mais de nombreuses interrogations demeurent.

[https://www.association-audin.fr/6]

I - PROLOGUE : QU'EST-CE QU'UN NOMBRE PAIR ?

À cette question, une amie professeure des écoles a répondu : « C'est un nombre qui se termine par 0, 2, 4, 6 ou 8 », en s'étonnant de cette question, à laquelle elle n'imaginait pas d'autre réponse. J'ai voulu en savoir plus. J'ai obtenu la même réponse auprès de plusieurs autres professeures des écoles. Des collègues de l'IREM spécialisées dans l'enseignement primaire m'ont confirmé que c'était généralement cette définition qui était utilisée. Je suis alors allé consulter les textes officiels et les manuels scolaires. Le résultat est édifiant.

Dans l'ensemble des documents publiés par le ministère de l'Éducation nationale [voir l'annexe I] (programmes, attendus, outils d'évaluation, documents d'accompagnement), on trouve au total 55 occurrences de la chaîne de caractères « p a i r ». Mais pour 41 d'entre elles (soit 74,5%), le mot dans lequel elles figurent est pris dans un sens non mathématique (« présentation des travaux à ses pairs », « une paire de chaussettes » …). Je note incidemment que j'ai eu l'idée de dénombrer les occurrences des mots « compétences » et « connaissances » dans le programme du socle commun. Résultats respectifs : 46 et 58.

Dans les 14 manuels de l'enseignement primaire que j'ai consultés, la situation est radicalement différente. « pair » pris dans le sens « alter-ego » apparaît très peu, alors que les textes officiels en font un usage immodéré. Ici, sur 77 occurrences de « pair », 60 correspondent à la signification mathématique de ce mot. MAIS je n'ai RIEN trouvé qui puisse être considéré comme une définition de la notion de nombre pair !

Comment interpréter cela ?

Les enseignantes, et notamment les autrices de manuels scolaires, ont évidemment besoin de parler de la notion de nombre pair. Or elles ne trouvent rien dans les textes officiels qui puisse les guider, et rien dans les manuels qui soit une définition de cette notion. Elles se disent qu'un nombre pair, tout le monde finit par savoir ce que c'est ! Elles en parlent donc sans ambages, convaincues que, de même qu'Alphonse Allais n'avait pas besoin de caractères pour reconnaître un chou-fleur [voir l'annexe II], nous n'avons pas besoin de définition pour reconnaître un nombre pair.

Mais en maths, on aimerait bien quand même disposer d'une définition… Et heureusement, il y en a une !

« n est pair »

est synonyme de

« il existe au moins un entier k tel que $n = 2k$ »

ou encore (n'ayons pas peur !) de

$$(\exists k \in \mathbb{N}) \quad n = 2k.$$

Comment passer d'une connaissance intuitive, installée très tôt, à la possibilité de formuler une telle définition ? C'est une question qui me semble fondamentale, mais à laquelle je ne prétends pas apporter de réponse.

II - RÉCURRENCE

1. Un théorème bien connu : ($\forall n \in \mathbb{N}$) ($n = 0$ ou $n = 1$)

J'appelle $P[n]$ la propriété ($n = 0$ ou $n = 1$), définie pour chaque entier naturel n, et je vais démontrer par récurrence la propriété ($\forall n \in \mathbb{N}$) $P[n]$.

Pour ce faire, consultons la notice :

Propriété **Principe de récurrence**
Si une propriété est vraie pour l'entier naturel n_0 et s'il est prouvé que lorsqu'elle est vraie pour un entier naturel p supérieur ou égal à n_0, elle est vraie aussi pour l'entier naturel $p + 1$, alors elle est vraie pour tous les entiers naturels supérieurs ou égaux à n_0.

Une démonstration utilisant ce principe comporte **deux étapes**.
P (n) désigne une propriété qui dépend d'un entier naturel n et n_0 désigne un entier naturel. Pour démontrer que pour tout entier naturel $n \geqslant n_0$, P (n) est vraie, on procède comme ci-dessous.

- **Première étape :** on vérifie que P (n_0) est vraie, c'est l'**initialisation** de la récurrence.
- **Deuxième étape : l'hérédité.** On suppose ensuite qu'il existe un entier p tel que P (p) soit vraie, c'est l'hypothèse de récurrence et on démontre alors que P ($p + 1$) est vraie.

Éditions Bordas, collection Indice, TS programme 2012

Et suivons-la pas à pas :

Première étape (initialisation) : ici, $n_0 = 0$, et $P[n_0]$ est donc la propriété : ($0 = 0$ ou $0 = 1$). On doit pouvoir démontrer qu'elle est vraie… La première manche est gagnée !

Deuxième étape (hérédité) : La notice dit : « On suppose qu'il existe un entier p tel que $P[p]$ soit vraie ». Est-ce le cas ? On dirait que oui : il suffit de prendre $p = 0$. Mais alors $p + 1 = 1$ et on dirait bien que $P[1]$ est également vraie : ($1 = 0$ ou $1 = 1$).

Il en résulte que ($\forall n \in \mathbb{N}$) ($n = 0$ ou $n = 1$).

Victoire en deux manches !

2. Digression

On considère un polynôme Q à coefficients réels. Essayons de traduire dans un langage symbolique la propriété qui s'énonce de façon informelle comme suit :

« Si le polynôme Q a une racine réelle, alors elle est positive ou nulle. »

La tentation est grande d'écrire :

$$(\exists x \in \mathbb{R})\ Q[x] = 0 \quad \Rightarrow \quad x \geq 0.$$

Mais on voit bien que cela ne va pas : la variable x est muette dans l'expression à gauche du symbole d'implication (elle est liée par le quantificateur existentiel), tandis qu'elle est libre à droite. La proposition ainsi écrite équivaut à $(\exists y \in \mathbb{R})\ Q[y] = 0 \quad \Rightarrow \quad x \geq 0$. Contrairement à ce qu'on pourrait croire, la propriété que l'on voulait traduire formellement est une proposition universelle :

$$(\forall x \in \mathbb{R})\ (Q[x] = 0 \Rightarrow x \geq 0).$$

La situation est tout à fait analogue à ce que nous venons de voir pour la récurrence. En effet la formulation adoptée pour l'hérédité dans le manuel cité conduit tout naturellement à écrire :

$$(\exists p \in \mathbb{N})\ P[p] \quad \Rightarrow \quad P[p+1],$$

alors que la formulation correcte est :

$$(\forall p \in \mathbb{N})\ (P[p] \Rightarrow P[p+1]).$$

Nous pouvons ainsi pointer ce qui ne va pas dans notre manuel :

Propriété **Principe de récurrence**
Si une propriété est vraie pour l'entier naturel n_0 et s'il est prouvé que lorsqu'elle est vraie pour un entier naturel p supérieur ou égal à n_0, elle est vraie aussi pour l'entier naturel $p+1$, alors elle est vraie pour tous les entiers naturels supérieurs ou égaux à n_0.

Une démonstration utilisant ce principe comporte **deux étapes**.
P(n) désigne une propriété qui dépend d'un entier naturel n et n_0 désigne un entier naturel. Pour démontrer que pour tout entier naturel $n \geqslant n_0$, P(n) est vraie, on procède comme ci-dessous.

- **Première étape :** on vérifie que P(n_0) est vraie, c'est l'**initialisation** de la récurrence.
- **Deuxième étape : l'hérédité.** On suppose ensuite qu'il existe un entier p tel que P(p) soit vraie, c'est l'hypothèse de récurrence et on démontre alors que P($p+1$) est vraie.

3. Le principe de récurrence

Il s'exprime par la proposition suivante, qui est vraie :

$$(P[0] \quad \text{et} \quad (\forall k \in \mathbb{N})\ (P[k] \Rightarrow P[k+1])) \quad \Rightarrow \quad (\forall n \in \mathbb{N})\ P[n]$$

Bien entendu, il n'est pas question d'asséner cette formule à nos élèves[1] ! Nous voulons simplement faire observer qu'elle comporte deux quantificateurs universels et deux implications, ce qui explique peut-être les difficultés rencontrées par plusieurs élèves pour rédiger une preuve par récurrence...

[1]On peut par exemple leur dire que, pour démontrer qu'une propriété $P[n]$ est vraie pour tout entier n, il suffit, d'une part (initialisation) de démontrer que $P[0]$ est vraie, et d'autre part (hérédité) de démontrer que, **pour tout entier *k***, si $P[k]$ est vraie, alors $P[k+1]$ est également vraie.

III - À PROPOS DU THÉORÈME DE BÉZOUT

L'expression suivante nous est familière :

« n peut s'écrire sous la forme $au + bv$, avec u et v dans $\mathbb{Z}$. »

Les variables qui ont au moins une occurrence dans cette proposition sont n, a, u, b et v.

Mais de quels objets la proposition « parle »-t-elle ? De n, de a et de b. Mais ni de u, ni de v.

n, a et b y sont *libres* (ou *parlantes*). u et v y sont *liées* (ou *muettes*).

Pourquoi u et v sont-elles muettes ? Qui leur « coupe la parole » ? Il n'y a pas de symbole de quantificateur, ni de sommation ou d'intégration (ni d'autres signes qui ont pour effet de rendre des variables muettes).

Mais il y a une quantification existentielle implicite, et c'est le mot « avec » qui en témoigne. Pour expliciter la quantification, il conviendrait de formuler la proposition de la manière suivante :

« Il existe des entiers relatifs u et v tels que $n = au + bv$. »

Le discours mathématique fait un usage intensif du mot « avec ». Il cache la plupart du temps une quantification existentielle. Mais il peut y avoir des exceptions. Ainsi on peut rencontrer la phrase suivante : « On a $\ln(x^2) = 2\ln x$, avec $x \in \mathbb{R}$ et $x > 0$ », où il s'agit manifestement d'une quantification universelle implicite. Mais je ne recommande vraiment pas ce genre de formulation.

La proposition considérée nous parle donc des objets n, a et b. Lorsque des variables apparaissent dans une proposition, cette proposition exprime une propriété des objets désignés par celles des variables qui y sont LIBRES.

Le théorème de Bézout peut être énoncé de la manière suivante :

> Pour tout entier n, n est un multiple du pgcd de a et b si et seulement si n peut s'écrire sous la forme $au + bv$ avec u et v dans $\mathbb{Z}$.

Cette proposition nous parle uniquement des objets a et b. Qu'est-il arrivé à la variable n ? Elle a été rendue muette par la quantification universelle (« pour tout entier n »). On dit qu'elle a été *mutifiée*.

Voici une autre manière de dire la même chose (en précisant que la variable n est *astreinte*[2] à $\mathbb{N}$ et que les variables a, b, k, u et v sont astreintes à $\mathbb{Z}$) :

[2]On dit qu'une variable x est *astreinte* à un ensemble E lorsqu'elle est appelée à *prendre ses valeurs* dans E. Il y a une différence majeure entre « $x \in E$ » et « x est astreinte à E ». La première phrase nous parle d'un objet mathématique, nommé x (et nous dit que cet objet appartient à l'ensemble E), la deuxième nous parle d'un symbole du langage appelé à désigner des objets mathématiques. Il est important de faire la distinction entre un objet et le nom de cet objet. On retrouve ici la dualité classique signifié / signifiant. Le *signifié* est l'objet dont on parle, le *signifiant* est le nom qu'on lui donne. Le nom de l'objet relève de la syntaxe. L'objet lui-même relève de la sémantique. On connaît la devinette : *SANS MOI, PARIS SERAIT PRIS. QUI SUIS-JE* ?

$$\forall n \quad \left[\exists k \quad n = k\ \mathrm{pgcd}(a,b) \iff \exists u\ \exists v \quad n = au + bv\right]$$

Là aussi apparaît nettement la complexité de la structure de cette proposition, où il y a six variables et quatre quantificateurs (sur l'emplacement desquels il ne faut pas se tromper !), mais qui ne parle en fait que de deux objets (a et b). Mettons-nous à la place d'un élève de Terminale ! On me dira que justement, comme c'est compliqué, il vaut mieux ne pas expliciter tous les quantificateurs et dire les choses « avec les mots de tous les jours ». Je m'inscris évidemment en faux contre ce point de vue : cacher une difficulté ne peut pas faciliter la compréhension, bien au contraire. Attention ! Je ne dis pas qu'il faille donner la formule ci-dessus aux élèves ! Mais qu'une enseignante ait conscience de sa structure me semble vraiment utile.

Pour clore cette section, je reproduis un extrait d'un manuel du début des années 2010. Je n'en ai pas retrouvé la référence mais j'en garantis l'authenticité.

Propriétés

(1) a et b **sont** deux entiers naturels. **Si** a divise b, **alors** $\mathrm{PGCD}(a;b) = a$.

(2) **Propriété fondamentale** : **Soit** a non nul tel que $a = bk + r$ **où** k est un entier. Alors $D(a) \cap D(b) = D(b) \cap D(r)$ et $\mathrm{PGCD}(a;b) = \mathrm{PGCD}(b; a - bk)$.

Les mots en bleu ont été soulignés par mes soins. Ils vous invitent à méditer sur le statuts des 4 variables qui apparaissent dans ce texte, sur les sorts respectifs réservés à k et à r, et à deviner où se nichent des quantifications. Le « Si …, alors ... » de la propriété (1) suggère évidemment une quantification universelle sur a et b. Hélas, la phrase précédente (on admirera qu'elle soit présentée par le titre comme une *propriété* !) indiquerait plutôt que a et b sont deux objets particuliers. Dans (2), le mot « Soit » est censé faire comprendre aux lectrices que ce qui va suivre vaut pour tout élément a. Mais l'autrice ne juge pas utile de nous renseigner sur b ! Si le mot « où » témoigne d'une quantification existentielle implicite sur la variable k, en revanche rien n'est dit, ni même suggéré, à propos de r.

IV - LES AXIOMES DE PEANO

Avec les axiomes de Peano et les deux sections suivantes, respectivement consacrées aux ensembles bien ordonnés et aux ordinaux, nous quittons les mathématiques de l'enseignement secondaire pour aborder des notions plus abstraites, qui ne font pas partie de la formation de base des enseignantes et enseignants de mathématiques. Nous nous permettons de le faire pour deux raisons. La première est que ces notions interviennent dans la septième et dernière section, où est présenté le théorème de Goodstein. Cet énoncé et les objets qui y interviennent sont plutôt élémentaires, puisqu'il s'agit de définir et d'étudier une suite de nombres entiers. Le résultat est très spectaculaire et est accessible à des élèves de Terminale. C'est la démonstration du théorème qui nécessite de faire un détour par la théorie des ordinaux. Et il faut avoir une idée de ce qu'est une théorie axiomatique pour comprendre le statut très spécial du théorème de Goodstein. La deuxième raison pour laquelle nous avons voulu présenter ces notions plus avancées, c'est qu'elles nous semblent dignes de figurer dans le bagage culturel de toute personne qui enseigne les mathématiques ou réfléchit à leur enseignement. Quoi de plus basique en effet que les nombres entiers et les

Pour trouver la bonne réponse (la lettre « A »), il faut renoncer à l'interprétation spontanée (*Sans moi, la ville de Paris serait prise*) et considérer que PARIS est ici le nom de la ville (le signifiant) et non la ville elle-même (le signifié).

fondements des mathématiques ? Si vous avez des réticences à aborder directement les considérations abstraites qui suivent, vous pouvez commencer par aller découvrir à la section VII le théorème de Goodstein. Il est probable qu'il vous fascinera et vous donnera envie de revenir en arrière pour en savoir plus.

Pour un exposé des notions abordées ici, on peut consulter [2] *et* [3].

1. Le langage de l'arithmétique et les axiomes de Peano

Les axiomes de Peano sont des propositions, écrites dans un langage en respectant des règles syntaxiques simples (ce n'est pas le lieu de les expliciter ici), et qui sont vérifiées dans l'ensemble $\mathbb{N}$ des entiers naturels qui nous est familier, celui dont nous avons une connaissance intuitive, sans laquelle il n'est pas possible de faire des mathématiques. L'idée serait d'avoir un ensemble d'axiomes duquel on puisse déduire *toutes* les propriétés vraies dans $\mathbb{N}$. Hélas il faudra renoncer à cet objectif. Nous reviendrons sur ce point.

Le *langage de l'arithmétique* est constitué, d'une part de symboles dits *logiques* (variables, connecteurs, quantificateurs, parenthèses), et d'autre part des symboles spécifiques suivants :

- le symbole d'égalité : $=$
- un **symbole de fonction unaire** : S (pour la fonction successeur)
- deux **symboles de fonction binaires** : $+$ et $\times$ (pour l'addition et la multiplication)
- un symbole de constante : 0 (pour le nombre 0)

L'*arithmétique du premier ordre* est la théorie constituée des axiomes suivants (de Peano) :

- $\forall x\ \forall y\ \ (Sx = Sy \Longrightarrow x = y)$
- $\forall x\ \ (x \neq 0 \Longleftrightarrow \exists y\ x = Sy)$
- $\forall x\ \ x + 0 = x$
- $\forall x\ \forall y\ \ x + Sy = S(x + y)$
- $\forall x\ \ x \times 0 = 0$
- $\forall x\ \forall y\ \ x \times Sy = (x \times y) + x$
- $\left\{ \left(F[0] \text{ et } \forall x\ (F[x] \Longrightarrow F[Sx])\right) \Longrightarrow \forall x\ F[x] \ \middle|\ F \text{ est une proposition} \right\}$

Remarquez que le dernier item n'est pas un axiome unique mais un ensemble (infini) d'axiomes : il y en a un pour chaque proposition F écrite dans le langage. On appelle cet ensemble le *schéma de récurrence*.

2. Les modèles de l'arithmétique

Un modèle de l'arithmétique, c'est un ensemble M muni d'une fonction unaire S, de deux fonctions binaires + et × et d'un élément distingué 0 qui vérifie les axiomes de Peano.

Notre ensemble $\mathbb{N}$ avec sa structure habituelle est un modèle de ces axiomes, mais ce n'est sûrement pas le seul. Il y a en effet des théorèmes de logique qui garantissent l'existence de bien d'autres modèles de l'arithmétique de Peano, non isomorphes à $\mathbb{N}$, y compris des modèles non dénombrables !

L'existence d'un modèle fait que l'arithmétique de Peano est une *théorie cohérente*. (Le mot « théorie » désigne simplement un ensemble de propositions sans variables libres.)

De plus, l'arithmétique de Peano est une théorie incomplète. Cela signifie qu'il existe des propositions (du langage) qui ne peuvent être ni démontrées ni réfutées à partir de ces axiomes. De telles propositions sont vraies dans certains des modèles et fausses dans les autres. Il y a en particulier des propositions qui sont vraies dans $\mathbb{N}$ mais qui ne peuvent pas être démontrées à partir des axiomes de Peano. C'est en exhibant une telle proposition que Kurt Gödel a démontré vers 1930 que l'arithmétique est incomplète. Mais la proposition qui a servi à Gödel a un défaut majeur : même si elle est relative aux nombres entiers, elle est très éloignée de l'intuition qui nous guide lorsque nous faisons de l'arithmétique et il est vraiment difficile de l'appréhender. À tel point que certaines personnes y voient un objet pathologique, étranger au « vrai monde » des mathématiques. Cette objection tombe avec le théorème de Goodstein : il s'agit d'une proposition arithmétique qui parle en des termes usuels d'objets familiers. Elle n'est pas prouvable à partir des axiomes de Peano mais elle est vraie dans $\mathbb{N}$. Nous reviendrons à la section VII sur cette affirmation, mais pour en mieux comprendre la signification, il faut renoncer à l'idée qu'il n'y aurait qu'un unique modèle de la théorie de Peano et faire connaissance avec les modèles non-standard, que nous présentons maintenant.

Dans tout modèle de l'arithmétique de Peano, il y a des éléments (des entiers, donc) qui représentent nos entiers à nous, ceux avec lesquels nous faisons des mathématiques, appelons-les entiers intuitifs. Il s'agit de l'élément 0, de son image par la fonction successeur (c'est-à-dire par la fonction qui est l'interprétation du symbole S), du successeur de 0, etc. :

$$0,\ S(0) \text{ (noté 1)},\ S(S(0)) = S^2(0) \text{ (noté 2)},\ S^3(0) \text{ (noté 3)},\ \ldots,\ S^n(0) \text{ (noté } n\text{)},\ \ldots$$

[*La notation* $S^n(0)$ *est définie par récurrence :* $S^0(0) = 0$ *et, pour tout entier (intuitif !)* k, $S^{k+1}(0) = S(S^k(0))$.]

Mais attention à ce « etc. » et à ces points de suspension : les entiers utilisés ici (comme exposants de la fonction S) sont nos entiers intuitifs, et rien ne nous garantit que les images itérées de 0 par la fonction successeur vont constituer tous les éléments du modèle. Il y a même un théorème qui affirme qu'il existe des modèles contenant des éléments autres que ces successeurs itérés de 0. Les successeurs itérés de 0, nous les appelons *entiers standard*. L'itération, nous la faisons avec nos entiers intuitifs. Si elle ne suffit pas à épuiser le modèle, c'est qu'il contient d'autres éléments : les entiers non-standard.

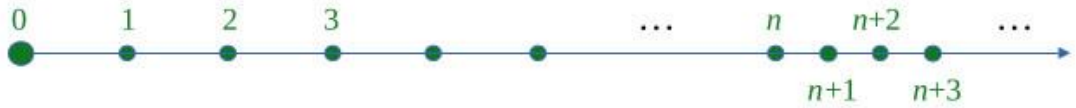
Les modèles où il y a des entiers non-standard sont appelés modèles non-standard. Notre ensemble $\mathbb{N}$ des entiers intuitifs, muni des opérations usuelles S, +, x, 0, est un modèle standard, et même LE modèle standard, car il est unique à isomorphisme près. (Deux modèles sont isomorphes s'il existe entre eux une bijection compatible avec les interprétations respectives des symboles S, +, x, 0.) En revanche, il y a beaucoup de modèles non-standard, et il y en a dans toutes les cardinalités infinies.

V - ENSEMBLES BIEN ORDONNÉS

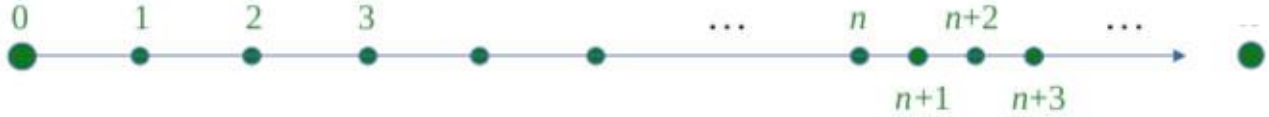
Pour cette section et la suivante (ordinaux), on peut se référer à [2], [3] et [7].

Un ensemble E muni d'une relation d'ordre $\leqslant$ est bien ordonné si toute partie non vide de E admet un plus petit élément pour l'ordre $\leqslant$.

L'exemple emblématique de bon ordre est fourni par l'ensemble $\mathbb{N}$ des entiers naturels avec son ordre usuel :



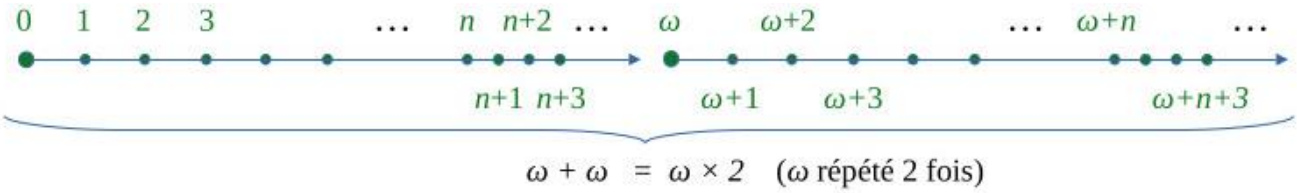
On a encore un ensemble bien ordonné en adjoignant aux entiers un élément qui soit plus grand que tous les autres :



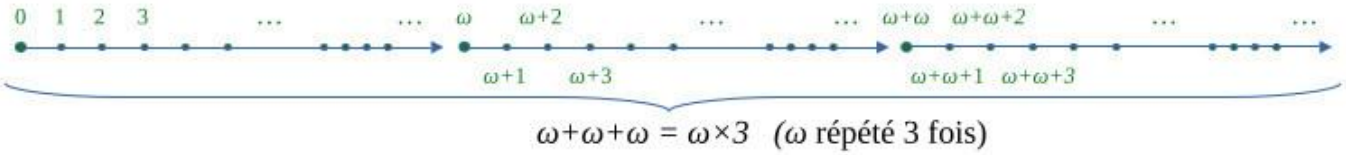
… ou plusieurs :

Donnons des noms à ces nouveaux éléments :

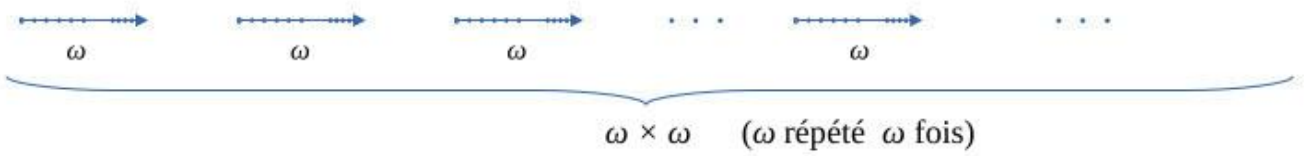
On peut aussi mettre bout à bout deux exemplaires de l'ensemble des entiers :



… ou trois :



… ou un grand nombre :



Propriété fondamentale des ensembles bien ordonnés :

> *Étant donné deux ensembles bien ordonnés quelconques, il y en a toujours au moins un des deux qui est isomorphe à un segment initial de l'autre.*

On peut esquisser une démonstration. Soit A et B deux ensembles bien ordonnés. Si l'un d'eux est vide, il est lui-même un segment initial de l'autre. S'ils sont tous les deux non vides, chacun est une partie non vide de lui-même et a donc à ce titre un plus petit élément, disons a_0 pou A et b_0 pour B. Si A n'a pas d'autre élément que a_0, l'application qui envoie a_0 sur b_0 est un isomorphisme de A sur un segment initial de B. Situation symétrique si c'est B qui a un seul élément. Si ni A ni B ne sont réduits à un élément, leurs sous-ensembles obtenus en ôtant a_0 de A et b_0 de B sont non vides, et ont donc chacun un plus petit élément, disons a_1 pou A et b_1 pour B. Si A n'a pas d'autre élément que a_0 et a_1, l'application qui envoie a_0 sur b_0 et a_1 sur b_1 est un isomorphisme de A sur un segment initial de B. Situation symétrique si c'est B qui n'a que deux éléments. On continue ainsi tant qu'il reste à la fois des éléments dans A et dans B, et on finira bien par épuiser les éléments de l'un ou de l'autre de ces ensembles. Cette dernière phrase est évidemment une escroquerie : rien ne permet d'affirmer que l'on arrivera à passer en revue tous les éléments de l'un des deux ensembles. Déjà, si on parvenait à le faire, cela signifierait que l'ensemble en question (disons que ce soit A) est dénombrable (on aurait énuméré ses éléments sous la forme d'une suite a_0, a_1 , …, a_k, …). Le raisonnement ne tient donc pas si A et B sont tous les deux infinis et non dénombrables. Mais il ne tient pas non plus lorsque l'un des deux est dénombrable : supposons en effet que A soit l'ensemble $\omega + \omega$ (obtenu en mettant bout à bout deux exemplaires de l'ensemble des entiers naturels) ; on ne pourra jamais atteindre avec notre procédé les éléments du deuxième exemplaire. La démonstration n'est donc pas aussi simple que ça, mais le résultat est bien vrai (à condition d'admettre l'axiome du choix ; mais nous n'en dirons pas plus à ce sujet).

Il en résulte que les *classes d'isomorphisme* des ensembles bien ordonnés sont deux à deux comparables. Il y a un ordre total sur ces classes. Et cet ordre est même un bon ordre !

VI - LES ORDINAUX

1. Présentation et premières propriétés

Nous ne donnerons pas de définition des ordinaux : cela relève de la théorie des ensembles et sortirait du cadre de cet exposé. Contentons-nous de dire que les ordinaux sont des représentants particuliers des classes d'isomorphisme d'ensembles bien ordonnés dont nous venons de parler.

Il y a d'abord les ordinaux finis, que l'on identifie aux entiers naturels. Certains d'entre eux (mais pas forcément tous ! il y peut y avoir des ordinaux finis non-standard) s'obtiennent de la façon suivante :

$$\begin{aligned}
\varnothing &= 0\\
\{\varnothing\} &= 1\\
\{\varnothing, \{\varnothing\}\} &= \{0,1\} = 2\\
\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} &= \{0,1,2\} = 3\\
&\vdots
\end{aligned}$$

Le premier ordinal est donc l'ensemble vide (identifié à l'entier 0).

Chaque ordinal est égal à l'ensemble de ceux qui le précèdent.

Pour tout ordinal a, l'ensemble $a \cup \{a\}$ est aussi un ordinal, appelé successeur de α et noté $S(a)$ ou $a + 1$.

Voici quelques propriétés des ordinaux :

Tous les éléments d'un ordinal sont des ordinaux.

Quels que soient les ordinaux α et β, si $\beta \in \alpha$, alors tous les éléments de β appartiennent aussi à α.

Il y a trois sortes d'ordinaux :

- 0 (l'ensemble vide) ;
- les ordinaux successeurs (un ordinal α est successeur s'il existe un ordinal β tel que $\alpha = \beta \cup \{\beta\}$) ;
- les ordinaux limites (ce sont tous les autres).

L'ordre sur les ordinaux est très simple :

Quels que soient les ordinaux α et β, on a

- $\alpha < \beta$ si et seulement si $\alpha \in \beta$ (l'ordre strict est l'appartenance) ;
- $\alpha \leqslant \beta$ si et seulement si $\alpha \subseteq \beta$ (l'ordre large est l'inclusion).

L'ordinal ω est le premier ordinal non fini.

ω est l'ensemble des ordinaux finis.
C'est aussi le premier ordinal limite.

- Chaque ordinal est un ensemble bien ordonné.
- La classe de tous les ordinaux est bien ordonnée.
- Toute classe non vide d'ordinaux a un plus petit élément.

► Il n'existe pas de suite d'ordinaux strictement décroissante.

Cette dernière propriété est cruciale. Nous y reviendrons.

2. Arithmétique ordinale

On définit trois opérations binaires sur les ordinaux : l'*addition*, la *multiplication* et l'*exponentiation*. Elles correspondent à des opérations sur les ensembles bien ordonnés, qui « passent au quotient », c'est-à-dire sont compatibles avec la relation d'isomorphisme entre ensembles bien ordonnés.

Étant donné deux ordinaux α et β, nous allons définir la somme $\alpha + \beta$, le produit $\alpha \times \beta$ et l'exponentielle α^β.

2.1. Addition

$\alpha + \beta$ est l'ordinal représentant l'ensemble bien ordonné obtenu en mettant « bout à bout » l'ensemble bien ordonné α suivi de l'ensemble bien ordonné β.

Formellement, on prend l'ensemble $(\{0\} \times \alpha) \cup (\{1\} \times \beta)$, avec l'ordre lexicographique.

On constate immédiatement que cette addition n'est pas commutative. Par exemple, $\omega + 1$ est l'ordinal successeur de ω, tandis que $1 + \omega$ est égal à ω.

En revanche, l'addition des ordinaux est associative.

2.2. Multiplication

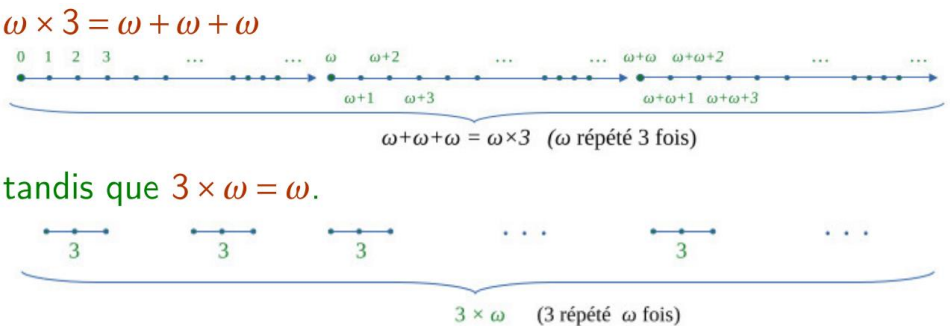
$\alpha \times \beta$ est l'ordinal représentant l'ensemble bien ordonné obtenu en munissant le produit cartésien $\alpha \times \beta$ de l'ordre anti-lexicographique :

$$(\gamma, \delta) \leqslant (\mu, \nu) \text{ si et seulement si } [\delta < \nu \text{ ou } (\delta = \nu \text{ et } \gamma \leqslant \mu)].$$

(On peut aussi prendre le produit cartésien $\beta \times \alpha$ avec l'ordre lexicographique.)

Intuitivement, $\alpha \times \beta$, c'est l'ordinal α « répété β fois ».

Là encore, il n'y a clairement pas commutativité :



Mais, comme l'addition, la multiplication des ordinaux est associative.

Nous nous permettrons, comme cela se fait toujours pour les multiplications usuelles, de noter indifféremment « $a \times \beta$ » ou « $a.\beta$ ».

2.3. Exponentiation

Pour définir l'ordinal a^β, on considère l'ensemble $a^{(\beta)}$ des applications de β dans a dont le *support* est fini. Le support d'une application f de β dans a est l'ensemble des éléments de β en lesquels f ne prend pas la valeur 0. Sur cet ensemble $a^{(\beta)}$, on définit l'ordre suivant :

> f est strictement inférieure à g s'il existe un ordinal $\gamma \in \beta$ tel que $f(\gamma) < g(\gamma)$ et, pour tout ordinal $\delta > \gamma$ dans β, $f(\delta) = g(\delta)$.

On obtient ainsi un ensemble bien ordonné dont l'ordinal est, par définition, a^β.

Pour tout ordinal $\alpha \neq 0$, il existe un nombre fini d'entiers non nuls $k_1, k_2, \ldots, k_n$, et un même nombre d'ordinaux $\alpha_1, \alpha_2, \ldots, \alpha_n$ vérifiant

Attention : l'exponentiation des ordinaux n'a rien à voir avec celle des cardinaux. Ainsi, l'ordinal 2^ω est dénombrable. Et il est tellement dénombrable qu'il est égal à ω…

2.4. Fort heureusement...

Appliquées aux seuls ordinaux finis, les trois opérations que nous venons de définir ne produisent que des ordinaux finis, et elles coïncident parfaitement avec celles de l'arithmétique de notre enfance : addition, multiplication et exponentiation des entiers.

3. Théorème de la forme normale de Cantor

Pour tout ordinal $\alpha \neq 0$, il existe un nombre fini d'entiers non nuls $k_1, k_2, \ldots, k_n$, et un même nombre d'ordinaux $\alpha_1, \alpha_2, \ldots, \alpha_n$ vérifiant

$$\alpha_1 > \alpha_2 > \ldots > \alpha_n,$$

tels que

$$\alpha = \omega^{\alpha_1}.k_1 + \omega^{\alpha_2}.k_2 + \ldots + \omega^{\alpha_n}.k_n.$$

Cette décomposition est unique et s'appelle la forme normale de Cantor de l'ordinal α.

Nous ne démontrons pas ce résultat. Voir [3] *pour plus de détails.*

On pourrait appeler cette décomposition l'*écriture de l'ordinal a en base ω*, par analogie avec l'écriture des entiers non nuls dans une base donnée.

VII - LE THÉORÈME DE GOODSTEIN

1. Écritures d'un entier naturel non nul en base 2 et en base 2 étendue

Partons de votre entier préféré : 89. Comme tous ses confrères, il s'écrit comme somme de puissances de 2 :

$$89 = 64 + 16 + 8 + 1 = 2^6 \cdot 1 + 2^5 \cdot 0 + 2^4 \cdot 1 + 2^3 \cdot 1 + 2^2 \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1$$

Cette décomposition est unique et on le représente donc ainsi dans cette base : $89 = \overline{1011001}_{[2]}$.

Mais les exposants, eux, sont écrits en base 10.

Écrivons-les à leur tour en base 2 puis itérons ce procédé tant que c'est nécessaire, pour ne plus avoir que des puissances de 2.

On obtient ainsi l'écriture de l'entier 89 **en base 2 étendue** :

$$89 = 2^{2^1+2^{2^1}} \cdot 1 + 2^{2^0+2^{2^1}} \cdot 0 + 2^{2^{2^1}} \cdot 1 + 2^{2^0+2^1} \cdot 1 + 2^{2^1} \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1$$

[*Remplacer les* 1 *par* 2^0 *ne changerait rien pour ce qu'on va faire ensuite.*]

2. Écriture d'un entier non nul en base *k* étendue et changement de base

On définit évidemment de la même manière, pour tout entier $n \geq 1$ et tout entier $k \geq 2$, le développement de n en base k étendue.

Soit p et q deux entiers naturels strictement supérieurs à 1. Pour tout entier naturel n, on appelle $T_{p,q}(n)$ l'entier obtenu en remplaçant toutes les occurrences de p par q dans l'écriture de n en base p étendue.

Ainsi, de l'écriture de 89 en base 2 étendue, on déduit que :

$$T_{2,3}(89) = 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 1$$

(*base* 3 *étendue*)

Le calcul donne :

$$T_{2,3}(89) = 213\,516\,729\,579\,718$$

3. Définition des suites de Goodstein

L'algorithme suivant définit la suite de Goodstein associée à un entier $n \geq 1$:

Voici l'algorithme qui définit la **suite de Goodstein associée à un entier** n :

- Le premier terme est $G_0 = n$. Dans notre exemple, $G_0 = 89$.
- On écrit le développement de G_0 en base 2 étendue.

$$89 = 2^{2^1+2^{2^1}} \cdot 1 + 2^{2^0+2^{2^1}} \cdot 0 + 2^{2^{2^1}} \cdot 1 + 2^{2^0+2^1} \cdot 1 + 2^{2^1} \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1$$

- On lui applique la fonction $T_{2,3}$.

$$T_{2,3}(G_0) = 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 1$$

- **On soustrait 1 au résultat obtenu**, ce qui fournit le deuxième terme de la suite : $G_1 = T_{2,3}(G_0) - 1 = 213\,516\,729\,579\,717$.
- On écrit le développement de G_1 en base 3 étendue.

$$G_1 = 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 0$$

- On lui applique la fonction $T_{3,4}$.

$$T_{3,4}(G_1) = 4^{4^1+4^{4^1}} \cdot 1 + 4^{4^0+4^{4^1}} \cdot 0 + 4^{4^{4^1}} \cdot 1 + 4^{4^0+4^1} \cdot 1 + 4^{4^1} \cdot 0 + 4^1 \cdot 0 + 4^0 \cdot 0$$

- **On soustrait 1 au résultat obtenu**, ce qui fournit le terme suivant de la suite : $G_2 = T_{3,4}(G_1) - 1$.
- On écrit le développement de G_2 en base 4 étendue.
- $G_2 = 4^{4^1+4^{4^1}} \cdot 1 + 4^{4^0+4^{4^1}} \cdot 0 + 4^{4^{4^1}} \cdot 1 + 4^{4^1} \cdot 3 + 4^3 \cdot 3 + 4^2 \cdot 3 + 4^1 \cdot 3 + 4^0 \cdot 3$
- *et on continue* ***tant que*** G_k ***n'est pas nul***.

Voici donc les tout premiers termes de la suite de Goodstein partant de 89 :

$$G_0 = \boxed{89}$$

$$= 2^{2^1+2^{2^1}} \cdot 1 + 2^{2^0+2^{2^1}} \cdot 0 + 2^{2^{2^1}} \cdot 1 + 2^{2^0+2^1} \cdot 1 + 2^{2^1} \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1$$

$$T_{2,3}(89) = 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 1$$

$$= 213\,516\,729\,579\,718$$

$$G_1 = T_{2,3}(89) - 1 = \boxed{213\,516\,729\,579\,717}$$

$$T_{3,4}(G_1) = 4^{4^1+4^{4^1}} \cdot 1 + 4^{4^0+4^{4^1}} \cdot 0 + 4^{4^{4^1}} \cdot 1 + 4^{4^0+4^1} \cdot 1 + 4^{4^1} \cdot 0 + 4^1 \cdot 0 + 4^0 \cdot 0$$

$$G_2 = T_{3,4}(G_1) - 1$$

$$= 3445806637995247454590524424538902454762197015892245098074955291036493355728901573038081694628894180916338187553926915069414747882670268476233447794563613695$$

C'est un nombre à 157 chiffres : $10^{156} \leqslant G_2 < 10^{157}$

Donnons la définition générale, par récurrence, de la suite de Goodstein $(G_k)_{k\in\mathbb{N}}$ associée à un entier n ≥ 1

$$G_0 = n,$$
$$G_1 = T_{2,3}(n) - 1,$$
et pour tout $k \in \mathbb{N}$,
$$G_{k+1} = \begin{cases} T_{k+2,k+3}(G_k) - 1 & \text{si } G_k \neq 0 \\ 0 & \text{si } G_k = 0 \end{cases}$$

Et donc, pour $n = 89$, on obtient :

$$G_0 = 89,$$
$$G_1 = T_{2,3}(89) - 1 = 205\,891\,132\,094\,757,$$
$$G_2 = T_{3,4}(205\,891\,132\,094\,757) - 1,$$
$$\bullet\bullet\bullet$$

On s'attend à ce que ces suites aient une croissance vertigineuse et tendent vers l'infini. Et pourtant...

4. Théorème de Goodstein

Toute suite de Goodstein stationne à la valeur 0.

Le logicien britannique *Reuben Louis Goodstein* a démontré cet étonnant résultat en 1944. Comment lui est venue l'idée d'étudier une suite aussi étrange ? Mystère ! [5]

La démonstration (voir [3]) utilise la théorie des ordinaux, et se fait donc dans le cadre de la théorie des ensembles, qui est strictement plus forte que l'arithmétique de Peano[3]. Or l'énoncé du théorème se ramène à une proposition du langage de l'arithmétique. En 1982, les logiciens *Jeff Paris* et *Laurence Kirby* ont prouvé ([6]) que cette proposition arithmétique n'est pas démontrable avec les seuls axiomes de Peano. On a ainsi un exemple de proposition « ordinaire » qui est vraie dans certains modèles de l'arithmétique (notamment dans notre modèle standard des entiers naturels) et fausse dans d'autres modèles[4]. C'est dans ce type de situation qu'on parle de propositions « vraies mais non démontrables ».

Nous allons donner pour terminer une idée de la preuve du théorème.

[3]Ce qui signifie que toute proposition arithmétique prouvable dans Peano l'est aussi dans la théorie des ensembles, mais qu'il existe des propositions arithmétiques prouvables dans la théorie des ensembles mais pas dans Peano.

[4]Mais décrire des modèles où elle est fausse est une tout autre histoire !

Soit p un entier strictement supérieur à 1. Pour tout entier naturel $n \geq 1$, on appelle $T_{p,\omega}(n)$ l'ordinal obtenu en remplaçant toutes les occurrences de p par ω dans l'écriture de n en base p étendue. La fonction $T_{p,\omega}$ est donc une application de $\mathbb{N}$ dans la classe des ordinaux.

Ainsi,

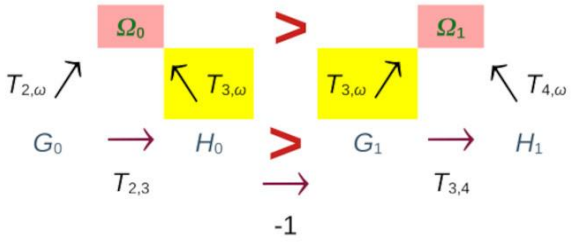
$$T_{2,\omega}(89) = \omega^{\omega^1+\omega^{\omega^1}} \cdot 1 + \omega^{\omega^0+\omega^{\omega^1}} \cdot 0 + \omega^{\omega^{\omega^1}} \cdot 1 + \omega^{\omega^0+\omega^1} \cdot 1 + \omega^{\omega^1} \cdot 0 + \omega^1 \cdot 0 + \omega^0 \cdot 1$$

Remarque importante : Quels que soient les entiers $p > 1$ et $q > 1$, $T_{p,\omega} = T_{q,\omega} \circ T_{p,q}$, c'est-à-dire que, pour tout entier $n \geq 1$, $T_{p,\omega}(n) = T_{q,\omega}(T_{p,q}(n))$. Autrement dit, il revient au même de remplacer toutes les occurrences de p par q, puis toutes celles de q par ω, que de remplacer directement toutes les occurrences de p par ω.

Nous admettons le résultat suivant (voir [3], 4.2.5, page 81) :

Lemme : Pour tout entier $p > 1$, la fonction $T_{p,\omega}$ est strictement croissante.

Posons, pour chaque entier naturel k, $H_k = T_{k+2,k+3}(G_k)$ et $\Omega_k = T_{k+2,\omega}(G_k)$.



Comme la fonction $T_{3,\omega}$ est strictement croissante, on a

$$\Omega_0 = T_{2,\omega}(G_0) = T_{3,\omega}(T_{2,3}(G_0)) = T_{3,\omega}(H_0) > T_{3,\omega}(H_0 - 1) = T_{3,\omega}(G_1) = \Omega_1$$

De même,

$$\Omega_1 = T_{4,\omega}(T_{3,4}(G_1)) = T_{4,\omega}(H_1) > T_{4,\omega}(H_1 - 1) = T_{4,\omega}(G_2) =$$
$$\Omega_2 = T_{5,\omega}(T_{4,5}(G_2)) = T_{5,\omega}(H_2) > T_{5,\omega}(H_2 - 1) = T_{5,\omega}(G_3) = \Omega_3 \ \ldots$$

Tant que l'entier G_k n'est pas nul, on peut définir l'**ordinal** Ω_k.

Si aucun des G_k n'était nul, on aurait une suite infinie strictement décroissante d'ordinaux : $(\Omega_k)_{k\in\mathbb{N}}$. Cela est impossible.

La suite de Goodstein finira donc nécessairement par s'annuler.

(*Sur le théorème de Goodstein, on trouve d'excellents exposés destinés à un large public dans l'article* [1], *et la vidéo* [4].)

VIII - BIBLIOGRAPHIE

[1] Artigue, M., Arzarello, F. et Epp, S. *Les suites de Goodstein ou la puissance du détour par l'infini*, Projet Klein, 2012.
http://blog.kleinproject.org/?p=722&lang=fr

[2] Cori, R. et Lascar, D. *Logique mathématique, cours et exercices* (2 tomes). Masson, collection Axiomes, 1992, Dunod, 2004.

[3] Dehornoy, P. *La théorie des ensembles*. Calvage et Mounet, collection Tableau noir, 2017, 2e éd. 2018.

[4] Dehornoy, P. *Georg Cantor et les infinis*. Société mathématique de France, Cycle de conférences « *Un texte un mathématicien* », 2009.
https://www.youtube.com/watch?v=cf15qYStKbA

[5] Goodstein, R. L. On the restricted ordinal theorem. *The Journal of Symbolic Logic*, 9, 33-41, 1944.

[6] Kirby, L.A.S. et Paris, J. B. Accessible Independant Results for Peano's Arithmetic. *Bulletin of the London Mathematical Society*, 14, 285–293, 1982.

[7] Krivine, J.-L. *Théorie des ensembles*, Cassini, 1998/2007.

ANNEXE 1 : DANS LES TEXTES OFFICIELS

La chaîne de caractères pair dans les documents du ministère de l'Éducation nationale.

Document	Nb occ	Math	Autre
Programme du cycle 2	19	**0**	19
Pour enseigner les nombres, le calcul et la résolution de problèmes au CP	4	2	2
Le calcul aux cycles 2 et 3	0	0	0
Le calcul en ligne au cycle 2	0	0	0
Doubles et moitiés	0	0	0
Programme du cycle 3	0	**0**	0
Résolution de problèmes - Cours moyen	6	1	5
Résolution de problèmes - Collège	15	6	9
Programme du cycle 4	6	**0**	6
Attendus de fin d'année 5ème	3	3	0
Attendus de fin d'année 4ème	2	2	0
Attendus de fin d'année 3ème	0	0	0
Socle commun	0	**0**	0
Évaluation des niveaux de maîtrise du socle (21 fiches pour Nombres et calculs)	0	0	0
	55	14	41

ANNEXE 2 : UN TEXTE D'ALPHONSE ALLAIS (1854-1905)

Extrait du conte Pour se donner une contenance (*Littoralement*, Éditions Arcanes, 1952)

Un jour, j'arrive à l'école – rara avis – pour passer un examen.

Parmi les examinateurs, j'aperçois qui ? Vous avez deviné : le vieux petit monsieur grincheux, chargé de sonder mes connaissances botaniques.

Oh ! combien rudimentaires, mes notions.

Le vieux petit monsieur grincheux m'offrit une plante médicinale, me demandant sur un ton d'où était bannie toute urbanité :

- Qu'est-ce que c'est que ça ?

– C'est du chou-fleur, monsieur.

– Le nom latin ?

– Je ne me rappelle pas, monsieur, mais je puis vous dire le nom anglais : cauliflower.

– Gardez votre anglais pour vous…
Et à quels caractères avez-vous reconnu cette plante ?

– Mais, monsieur, je n'ai pas besoin de caractères pour reconnaître du chou-fleur.

– Ça suffit... merci, monsieur.

Le vieux petit monsieur grincheux se vengea spirituellement de mes plaisanteries en me priant de repasser à une autre session.

ARITHMÉTIQUE DES ORDINATEURS

Jean-Michel MULLER
Directeur de Recherche au CNRS
Laboratoire LIP, ENS Lyon
jean-michel.muller@ens-lyon.fr

Résumé
L'arithmétique des ordinateurs s'intéresse à tous les aspects liés à l'implantation du calcul arithmétique sur ordinateur : systèmes de numération, algorithmes, circuits et programmes de calcul, erreurs d'arrondis, fiabilité. . . J'essaie dans cet article de donner un petit aperçu des diverses questions qui se posent actuellement dans ce domaine.

I - INTRODUCTION

Concevoir un système arithmétique pour calculer sur ordinateur n'est pas une tâche aisée car les diverses propriétés souhaitables d'un tel système ne sont pas toujours compatibles. On voudrait tout d'abord calculer *vite :* la simulation de certains phénomènes en dynamique des fluides fait appel à des systèmes capables de faire plusieurs milliers de milliards d'opérations arithmétiques par seconde.[1] Bien entendu, calculer vite ne sert pas à grand-chose si le résultat obtenu est complètement faux : la *précision* des calculs est, elle aussi, importante. Sans parler de certains "records" tels que le calcul du plus grand nombre de décimales[2] de π, certains domaines de la physique demandent une grande précision : les interféromètres LIRGO et VIRGO, qui ont été les premiers à détecter des ondes gravitationnelles, ont été capables de détecter des compressions relatives de l'espace-temps[3] de l'ordre de 10^{-22}. Nous devons donc être capables pour traiter certains problèmes de physique d'effectuer des suites de calculs, quelques fois longues, dont l'erreur relative finale n'est pas supérieure à 10^{-22}. Certains algorithmes de cryptanalyse demandent la manipulation de nombres de quelques centaines à quelques milliers de chiffres (Boudot *et al.*, 2020). La vitesse et la précision ne sont pas tout, d'autres contraintes plus technologiques sont elles aussi importantes. Il faut que les opérations arithmétiques *consomment peu d'énergie* pour des raisons environnementales, pour que les petits dispositifs tels que les téléphones ou les calculatrices aient une grande autonomie, mais également pour que les supercalculateurs ne brûlent pas, et que les circuits de calcul ne soient pas énormes. Finalement, pour des calculs mettant en jeu la sécurité de personnes ou de biens précieux, par exemple ceux effectués par le calculateur embarqué d'un avion ou ceux d'une ligne de métro automatique, il est important de pouvoir *prouver* le bon comportement du système. Un autre souhait

[1] Voir par exemple https://irfu.cea.fr/Projets/coast_documents/communication/Simulation.pdf ainsi que https://cerfacs.fr/gallery-of-images/

[2] Aux dernières nouvelles, on en serait à 10^{14} décimales.

[3] Voir https://www.nature.com/articles/nature.2016.19361

qui émerge actuellement est celui de la *reproductibilité* des calculs : une personne effectuant exactement les mêmes calculs que vous mais dans un contexte différent (une autre machine, une autre version du système d'exploitation, voire les mêmes mais à un autre moment) doit obtenir exactement les mêmes résultats. Les principales raisons de ce souhait sont scientifiques et techniques (vérification d'un résultat affirmé par une autre équipe) mais aussi légales (pouvoir expliquer devant une commission d'enquête ou un tribunal le processus qui a conduit à une décision). Toutes ces propriétés ne peuvent pas être satisfaites en même temps et les solutions ne seront donc pas les mêmes à l'intérieur d'un téléphone portable, d'un ordinateur de bureau, d'un supercalculateur ou d'une automobile.

II - LA FIABILITÉ N'A PAS TOUJOURS ÉTÉ DE MISE

Nous avons tous pesté devant un ordinateur « planté », un téléphone qu'il faut redémarrer, une imprimante qui n'imprime que les fichiers des autres ou un GPS qui nous ramène encore et encore devant la même route barrée. Il est très difficile de garantir qu'un programme ou un processeur sont exempts de « bugs » et les programmes et circuits arithmétiques n'échappent pas à cette fatalité. Il faut se méfier de l'intuition selon laquelle les algorithmes arithmétiques seraient « simples » et donc faciles à implanter sans erreur. Certes, les algorithmes d'addition, multiplication, division que nous avons appris à l'école sont simples mais, si on veut de la performance, il faut souvent utiliser des algorithmes nettement plus complexes, ce qui inévitablement augmente la probabilité de laisser une erreur. Voici quelques exemples de «bugs» arithmétiques célèbres :

— le processeur Pentium d'Intel, sorti en 1994, avait un algorithme de division faux. Dans les pires cas on n'avait que trois chiffres significatifs : le calcul de 8391667/12582905 par exemple donnait 0.666869… au lieu de 0.666910… . L'analyse de ce « bug » est assez amusante (Muller, 1995). La compagnie Intel a dû changer les processeurs défectueux. . . qu'elle a utilisé au Noël suivant pour offrir des porte-clés à ses cadres (Figure 1) ;

— sur certains ordinateurs des années 1970 (par exemple des Cray) on pouvait déclencher un overflow[4], c'est-à-dire un message nous informant que le plus grand nombre représentable était dépassé, en multipliant par 1 ;

— avec la version 6.0 de Maple (2000), en entrant 214748364810, vous obteniez 10. Si on remarque que 2147483648 est égal à 2^{32} on peut intuiter qu'une mauvaise conversion base 10/base 2 se cache derrière ce problème. Avec la version 7.0 du même logiciel (2001), le calcul de $\frac{5001!}{5000!}$ donnait 1 au lieu de 5001 ;

— avec les toutes premières versions d'Excel2007 (le bug a été vite corrigé), le calcul de $65535\text{-}2^{-37}$ donnait 100000 (là encore, une mauvaise conversion base 10/base 2 semble être à l'origine du problème);

— plus près de nous, avec une calculette Casio FX 83-GT ou FX-92, calculez $11^6/13$ et vous obtiendrez

$$\frac{156158413}{3600}\pi$$

[4] https ://people.eecs.berkeley.edu/˜wkahan/ieee754status/754story.html

qui est certes un résultat précis (la valeur affichée est effectivement très proche de $11^6/13$), mais très trompeur : la calculatrice nous fait croire qu'elle fait du calcul symbolique (comme le ferait par exemple le système de calcul formel Maple), et que le résultat affiché est exact.[5]

FIGURE 1 – Les porte-clés contenant des Pentium défectueux.

Parfois les bugs coûtent très cher. Nous avons déjà cité le cas du bug du Pentium, mais on peut aussi citer les cas suivants :

— en novembre 1998, à bord du navire de guerre américain *USS Yorktown*, un membre de l'équipage a par erreur tapé un « zéro » sur un clavier. Cela a entraîné une division par 0. Ce problème n'était pas prévu : il s'en est suivi une cascade d'erreurs qui a conduit à l'arrêt du système de propulsion;

— le premier tir, en 1996, de la fusée Ariane 5 a été un échec à la suite d'une mauvaise interprétation d'un « overflow ». Il aurait suffi à ce stade du vol de tout bonnement l'ignorer[6].

Mais, même en l'absence de « bugs », certains problèmes sont intrinsèquement difficiles et conduisent inévitablement à de larges erreurs. Laissez-moi vous conter une de mes mésaventures. Désirant sécuriser ma retraite, j'ai décidé il y a déjà longtemps de placer

$$e - 1 = 1.71828182845904523536028747135266249775724709 3 \ldots \text{ euros,}$$

où e est la base des logarithmes népériens. Je m'étais rendu à la *Société chaotique de banque* où le banquier m'a présenté leur toute nouvelle formule :

— la première année mon capital est multiplié par 1 et on me retire 1 euro pour frais de gestion. . . pas terrible ;

— la deuxième année mon capital est multiplié par 2 et on me retire 1 euro pour frais de gestion. . . c'est mieux;

— la troisième année mon capital est multiplié par 3 et on me retire 1 euro pour frais de gestion. . .

[5] Cette calculatrice est très répandue, beaucoup d'élèves de lycée en possèdent une. Cela peut-être l'occasion de glisser un mot sur l'irrationalité de π.

[6] https ://www-users.cse.umn.edu/~arnold/disasters/ariane5rep.html

c'est encore mieux;

— . . .

— la 25ème année mon capital est multiplié par 25 et on me retire 1 euro pour frais de gestion. . . c'est vraiment bien;

— et je peux retirer mon argent au bout de 25 ans.

Est-ce intéressant? En sortant de la banque, pour en avoir le cœur net, j'ai fait un rapide calcul sur ma calculette qui m'a annoncé que je disposerai de – 747895876335 € (gloups. . . environ 20 fois la dette des USA). Le même calcul fait sur mon ordinateur de bureau était plus rassurant et me prédisait +1201807247€. J'ai donc accepté l'offre. Ma déconvenue fut forte 25 ans après de constater que mon avoir n'était que d'environ 4 centimes! L'explication du problème est assez simple : on calcule des termes successifs de la suite

$$\begin{cases} u_0 &= e-1 \\ u_n &= n\cdot u_{n-1}-1 \end{cases} \tag{1}$$

pour laquelle il est assez facile de vérifier par récurrence que

$$u_n = \frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\cdots$$

Quelle que soit la précision de l'arithmétique utilisée u_0 est forcément représenté avec une petite erreur d'arrondi. Lors des itérations successives, cette erreur va être multipliée par 1, puis par 2, puis par 3, etc., de sorte que l'erreur sur u_n est de l'ordre de $n!$ fois l'erreur initiale. Il est donc normal d'obtenir n'importe quoi lorsqu'on calcule u_{25}. Il peut être amusant de constater que pour la même raison u_{25} peut se calculer très précisément en effectuant la récurrence (1) « à l'envers ». Si on prend comme valeur (complètement fantaisiste !) de u_{50} le nombre 42 et si on calcule successivement des approximations de u_{49}, u_{48}, etc. en utilisant

$$u_{n-1} = \frac{u_n+1}{n} \tag{2}$$

on obtient alors une excellente approximation de u_{25}.

Cet exemple est bien entendu un peu artificiel mais on en construit un tout-à-fait similaire en essayant de calculer, pour n grand, des valeurs de

$$I_n = \int_0^1 x^n e^{-x}dx,$$

en utilisant la relation (obtenue en intégrant par parties) $I_n = nI_{n-1} - 1/e$ et en partant de

$I_0 = 1 - 1/e$. On trouve facilement que $u_n = eI_n$.

Une autre cause fréquente d'erreurs informatiques est la mauvaise qualité des spécifications. La sonde *Mars Climate Orbiter* était censée orbiter autour de Mars pour analyser son climat. Elle s'est écrasée sur la planète dès son arrivée, en 1999. Une partie de l'équipe qui a conçu les logiciels pensait que les unités de mesure utilisées étaient celles du système métrique et l'autre partie croyait que c'était celles du système anglo-saxon.

III - L'ARITHMÉTIQUE VIRGULE FLOTTANTE

L'arithmétique à « virgule flottante » (VF) est de loin le système le plus utilisé pour représenter des nombres réels sur ordinateur. C'est le seul qui permette d'avoir des performances suffisantes pour effectuer en temps raisonnable les énormes calculs requis par la météo ou le calcul d'un profil d'avion, pour simuler un écoulement dans une turbine, etc. L'arithmétique VF est souvent perçue comme étant juste une « approximation floue » de l'arithmétique réelle et pourtant, comme nous allons le voir, elle est aussi une structure (au sens mathématique) parfaitement définie, sur laquelle on peut construire des algorithmes et prouver des théorèmes.

Si on se donne une *base* β ($\beta \in \mathbb{N}$, $\beta \geq 2$), une *précision* p ($p \in \mathbb{N}$, $p \geq 2$) et des *exposants extrémaux* $e_{\min}$ et $e_{\max}$ ($(e_{\min}, e_{\max}) \in \mathbb{Z}^2$, $e_{\min} < 0 < e_{\max}$), un nombre VF est un nombre de la forme

$$x = M \cdot \beta^{e-p+1}, \tag{3}$$

où $(M, e) \in \mathbb{Z}^2$, $|M| \leq \beta^p - 1$ (ce qui signifie que M s'écrit en base β sur au plus p chiffres) et $e_{\min} \leq e \leq e_{\max}$. Comme certains nombres peuvent avoir plusieurs représentations de la forme (3) satisfaisant les contraintes sur M et e, on demande que $|M|$ soit le plus grand possible. Ceci implique $|M| \geq \beta^{p-1}$, sauf dans le cas $e = e_{\min}$. Le nombre M est appelé *mantisse entière* de x et le nombre e est *l'exposant* de x.

La base choisie en pratique est presque toujours 2. Les calculatrices de poche et le système Maple utilisent la base 10. Une machine Russe, le Setun [7], construite à la fin des années 1950, utilisait la base 3.

Cette représentation découle de la *notation scientifique* utilisée massivement depuis le 19e siècle par les physiciens et les ingénieurs. On peut faire remonter cette dernière notation à très loin puisque le système babylonien « savant » (de base 60) représentait les nombres par leur mantisse entière (de sorte que 5 et 5×60^2 avaient la même représentation) et puisque une notation exponentielle des grands nombres avait déjà été mise au point par Archimède dans son traité *l'Arénaire* (Hirshfeld, 2009) pour compter le nombre de grains de sable que l'on pourrait disposer dans une sphère de diamètre la taille de l'Univers. Nicolas Chuquet semble être le premier à avoir considéré des exposants pouvant être négatifs ou nuls (Flegg *et al.*, 1985). Descartes semble être à l'origine de notre notation exponentielle moderne (a^3 pour $a \times a \times a$) et c'est

[7] Voir https://link.springer.com/content/pdf/10.1007/978-3-642-22816-2_10.pdf

probablement pour cela qu'on pouvait il y a quelques années lire sur un site américain visiblement très informé que *la notation scientifique a été inventée par Descartes puis améliorée par Archimède!* La représentation virgule flottante « moderne » semble avoir été inventée par Leonardo Torres y Quevedo et Konrad Zuse (Ceruzzi, 1981).

La somme, le produit, le quotient de deux nombres virgule flottante ne sont en général pas exactement représentables en virgule flottante. Il faut donc les arrondir. Jusqu'aux années 1980, la seule chose qu'on savait était que le résultat fourni par la machine était « proche » du résultat exact et des machines distinctes pouvaient avoir des comportements très différents, ce qui rendait la mise au point des programmes très difficile. Un effort important de standardisation, sous l'impulsion de Kahan (1981), professeur à UC Berkeley, a permis de mettre un peu d'ordre dans cela. Le Standard IEEE 754, publié en 1985 et révisé en 2008 et 2019, impose la base 2, spécifie plusieurs formats et, surtout, définit l'exigence *d'arrondi correct*. Des *fonctions d'arrondi* $\circ$ (qui sont des fonctions de $\mathbb{R}$ vers l'ensemble des nombres VF augmenté de $-\infty$ et $+\infty$) sont définies et, une fois que l'utilisateur a choisi une fonction d'arrondi , chaque fois que l'on effectue une opération de la forme $a \mathsf{T} b$ (où a et b sont des nombres VF et $\mathsf{T} \in \{+, -, \times, \div\}$ +, , ,), le résultat calculé par l'ordinateur doit être $\circ(a \mathsf{T} b)$. La même exigence est formulée pour la racine carrée. La fonction d'arrondi par défaut (celle que l'on obtient si on ne fait aucun choix) est *l'arrondi au plus près à arbitrage pair* (*round to nearest ties to even*), RN , défini comme suit : si t est le milieu exact de deux nombres VF consécutifs alors RN (t) est celui de ces deux nombres dont la mantisse entière est paire, sinon RN(t) est le nombre VF le plus proche de t. Cette exigence d'arrondi correct, ainsi que la spécification de ce que doit faire l'ordinateur quand on demande à calculer $1/0$, $\sqrt{-5}$, etc., rend l'arithmétique complètement déterministe, tout au moins tant qu'on se contente d'utiliser les opérations arithmétiques et la racine carrée. On peut alors élaborer des algorithmes et des preuves qui utilisent cette propriété. Un exemple simple (et très utile en pratique!) est l'algorithme Fast2Sum, présenté par le théorème suivant.

Théorème 1 (Fast2Sum (Dekker)). *Supposons $\beta \leq 3$. Soient a et b des nombres VF vérifiant $|a| \geq |b|$. L'algorithme suivant calcule deux nombres VF s et r tels que*

- $s + r = a + b$ *exactement;*
- s *est « le » nombre VF le plus proche de* $a + b$.

Algorithme 1 (FastTwoSum).

$s \leftarrow RN(a + b)$

$z \leftarrow RN(s - a)$

$r \leftarrow RN(b - z)$

L'algorithme FastTwoSum est implanté par le programme C suivant :

```
s = a+b;
z = s-a;
r = b-z;
```

On peut ainsi en trois opérations calculer l'erreur (le terme r de l'algorithme FastTwoSum) d'une addition virgule flottante. Il est possible également de calculer l'erreur d'une multiplication virgule flottante. Pour

ceci, nous devons utiliser l'opérateur arithmétique FMA, spécifié depuis la version 2008 du standard IEEE 754 et implanté sur tous les processeurs courants :

$$\mathrm{FMA}(a, b, c) = \mathrm{RN}(ab + c).$$

L'erreur commise en effectuant la multiplication virgule flottante $t = \mathrm{RN}(ab)$ est tout simplement $\mathrm{FMA}(a, b, -t)$. Ces petits algorithmes de calcul de l'erreur des opérations arithmétiques élémentaires permettent de mettre au point des programmes numériques précis où l'on parvient à compenser (partiellement) les erreurs d'arrondis. De nombreux algorithmes de calcul de sommes, de produits scalaires, de normes, etc. font appel à ces techniques, comme le décrit Rump (2012). L'arithmétique complexe utilise également fréquemment ces techniques, voir par exemple Brent *et al.* (2007); Jeannerod *et al.* (2017).

On peut ainsi, par exemple, représenter des nombres avec une grande précision comme somme de deux nombres VF (une « partie haute » et une « partie basse ») et mettre au point des algorithmes de manipulation de telles sommes. Une des principales difficultés que l'on rencontre est que les preuves de ces algorithmes deviennent très longues et donc sujettes à doutes (peu de gens les lisent). Il faut souvent faire appel à des techniques de « preuve formelle » pour les valider (Boldo et Melquiond, 2017; Muller et Rideau, 2022).

L'implantation très précise des fonctions mathématiques de base (sinus, cosinus, exponentielle) n'est pas un problème simple et fait toujours l'objet de nombreux travaux. On souhaiterait garantir l'arrondi correct de ces fonctions, ce qui demande la résolution d'un problème appelé *dilemme du fabricant de tables* (Boldo *et al.*, 2023a) qui très grossièrement consiste, si on s'intéresse à la fonction f, à déterminer quel est le nombre VF x tel que $f(x)$ est le plus proche du milieu exact de deux nombres VF consécutifs. Les mathématiques sous-jacentes à ce problème ne sont pas simples (Brisebarre *et al.*, 2017). La meilleure bibliothèque de fonctions mathématiques, actuellement, est construite dans le cadre du projet CORE-MATH, porté par Paul Zimmermann au Loria [8](Sibidanov *et al.*, 2022).

Terminons cette partie avec un exemple classique mais amusant, dérivé d'une idée de Malcolm (1972). Sur une arithmétique VF avec arrondi correct, l'algorithme suivant calcule la base β utilisée par votre processeur pour représenter les nombres VF (soit en général 2 mais le même algorithme transposé sur une calculatrice pourra donner 10). Saurez-vous trouver pourquoi?

Algorithme 2.

$A \leftarrow 1.0$
$B \leftarrow 1.0$
while $RN(RN(A + 1.0) - A) = 1.0$ ***do***
  $A \leftarrow RN(2 \times A)$
end while
while $RN(RN(A + B) - A) \neq B$ ***do***
  $B \leftarrow RN(B + 1.0)$
end while
return B

[8] https ://core-math.gitlabpages.inria.fr

Petit rappel : pour implanter cet algorithme sur votre machine il suffit d'omettre les « RN » puisque lorsque vous écrivez par exemple a+b dans un programme, ce qui est effectivement calculé est RN ($a + b$).

IV - RÉAPPRENONS L'ADDITION

Terminons ce petit tour en retournant à l'école : *comment faire une addition?* Supposons que l'on veuille additionner deux entiers x et y de n chiffres, écrits en base 2

$$(x_{n-1}\, x_{n-2}\, x_{n-3} \cdots x_0) \quad \text{et} \quad (y_{n-1}y_{n-2}y_{n-3} \cdots y_0),$$

ce qui signifie que les x_i et les y_i valent 0 ou 1, et que

$$x = \sum_{i=0}^{n-1} x_i 2^i \quad \text{et} \quad y = \sum_{i=0}^{n-1} y_i 2^i.$$

Comment fait-on une addition? L'algorithme élémentaire n'est pas très différent de celui de base 10 que nous avons appris à l'école. Nous partons d'une « retenue initiale » $c_0 = 0$ (nous verrons bientôt pourquoi j'introduis une retenue dès le premier chiffre). Nous calculons tout d'abord $x_0+y_0+c_0$. Si cette somme vaut 0 ou 1, elle sera le chiffre de droite s_0 de $x+y$, et nous propagerons vers l'étape suivante une retenue nulle c_1. Sinon, nous choisissons $s_0 = x_0 + y_0 + c_0 - 2$ et nous propagerons une retenue $c_1 = 1$. À l'étape suivante, nous calculons $x_1 + y_1 + c_1$ et nous prenons une décision similaire à la précédente selon que cette somme est inférieure ou égale à 1 ou pas. Bref, nous calculons itérativement la somme $s = s_n s_{n-1} s_{n-2} \cdots s_0$ comme suit :

$$\begin{aligned} &c_0 = 0, \\ &\text{pour } i = 0, \ldots, n-1 \\ &\qquad c_{i+1} = \begin{cases} 0 & \text{si } x_i + y_i + c_i \in \{0,1\} \\ 1 & \text{sinon} \end{cases} \\ &\qquad s_i = x_i + y_i + c_i - 2c_{i+1} \\ &s_n = c_n. \end{aligned} \tag{4}$$

Lorsqu'on effectue l'addition en utilisant (4), pour calculer s_n nous avons besoin de c_{n-1}. Mais le calcul de c_{n-1} requiert de connaître c_{n-2}. Et on peut calculer c_{n-2} uniquement si on connait c_{n-3} et ainsi de suite. Le processus d'addition décrit par (4) est *intrinsèquement séquentiel* et conduit à un temps de calcul qui *croît linéairement avec n*. On doit effectuer l'addition « de la droite vers la gauche ». Lorsqu'on effectue une addition « à la main » cela ne me pose pas de problème car on ne sait de toute façon calculer que séquentiellement. Il en va tout autrement d'un circuit intégré dont tous les transistors peuvent fonctionner en même temps et qui en principe serait capable d'effectuer simultanément des calculs portant sur tous les chiffres de x et y. Une des solutions pour accélérer le calcul est la suivante. Supposons pour simplifier que n est une puissance de 2 et que nous savons déjà additionner rapidement des nombres de $n/2$ chiffres. Pour effectuer l'addition

```
  10010110010110111100010111100011010100101101001 01
+ 01101001001110011010010111100101010010111101101 10
```

la première solution qui vient à l'esprit est de couper chacun des nombres x et y en deux paquets de $n/2$ bits :

```
100101100101101111000101 1   1100011010100101101001 01
011010010011100110100101     1110010101001011110110110
```

et d'additionner les paquets de droite, puis lorsqu'on connait la retenue sortante de cette addition, de l'utiliser comme retenue entrante pour additionner les paquets de gauche. En faisant ainsi, si on appelle T_n le temps de l'addition de nombres de n chiffres, on a $T_n = 2T_{n/2}$. Le temps de calcul reste proportionnel à n et on n'a rien gagné. Mais puisque la retenue sortante de l'addition des paquets de droite ne peut rendre que deux valeurs possibles (0 ou 1), on peut travailler sur les deux hypothèses en parallèle. Dupliquons les paquets de gauche et décidons, *dès le début du calcul, sans attendre, de faire en parallèle trois additions de nombres de n/2 bits* : celle des paquets de droite, celle des paquets de gauche en supposant une retenue entrante nulle et celle des paquets de gauche en supposant une retenue entrante égale à 1 :

```
                                0
 100101100101101111000101      1100011010100101101001 01
+ 011010010011100110100101   + 1110010101001011110110110

                                1
 100101100101101111000101
+ 011010010011100110100101
```

Au bout d'un temps $T_{n/2}$, ces trois additions sont terminées et, au vu de la retenue sortante de l'addition des paquets de droite, on peut choisir lequel des deux résultats des additions des paquets de gauche est le bon :

```
                                0
 100101100101101111000101      1100011010100101101001 01
+ 011010010011100110100101   + 1110010101001011110110110
   yyyyyyyyyyyyyyyyyyyyyyy      1xxxxxxxxxxxxxxxxxxxxxxxxx
                                ↙
                                1
 100101100101101111000101
+ 011010010011100110100101
   zzzzzzzzzzzzzzzzzzzzzzz
```

Le temps de calcul T_n devient alors égal à $T_{n/2} + C$ où C est un terme constant qui est le temps, tout petit, requis par les circuits logiques utilisés pour choisir entre les deux paquets de gauche. On en déduit facilement que T_n devient proportionnel à $\log(n)$. En pratique le gain est considérable dès que n est un peu grand et, dans les processeurs, des solutions semblables à celle-ci, ou d'autres solutions elles-aussi à temps logarithmique (Knowles, 2001) sont utilisées pour additionner des nombres de 32 bits ou plus.

En utilisant un théorème de Winograd, on peut montrer que dans nos systèmes usuels de numération (par exemple base 2 et chiffres 0 ou 1, ou base 10 et chiffres compris entre 0 et 9), sous des hypothèses raisonnables (le nombre d'entrées d'une « porte logique » est borné), un circuit ne peut pas additionner ou multiplier des nombres de n chiffres en un temps meilleur que logarithmique en n. Mais on peut tout de même aller plus vite en changeant notre manière de représenter les nombres. Cela nécessite cependant de renoncer à l'*unicité* de la représentation, ce qui ne va pas sans poser d'autres problèmes (les comparaisons par exemple deviennent nettement plus difficiles, la consommation de mémoire sera supérieure). Par exemple Avizienis (1961) a proposé de représenter les nombres en base 10 avec des chiffres allant de -6 à +6. Dans ce système de numération, certains nombres ont plusieurs représentations possibles : ce système est dit *redondant*. Le lecteur constatera aisément que l'algorithme ci-dessous permet à un circuit de calculer en « temps constant » (i.e. indépendant de la taille n des entrées) la somme de deux nombres x et y écrits dans ce système (le chiffre s_i se choisit au vu d'une « fenêtre » de deux chiffres seulement de x et de y).

Algorithme 3 (Addition d'Avizienis)**.**

1. *Calculer pour* $i = 0 \dots n-1$:

$$t_{i+1} = \begin{cases} -1 & si \quad x_i + y_i \leq -6 \\ 0 & si \quad -5 \leq x_i + y_i \leq 5 \\ 1 & si \quad x_i + y_i \geq 6 \end{cases}$$
$$w_i = x_i + y_i - 10t_{i+1}$$

2. *Calculer pour* $i = 0 \dots n$: $s_i = w_i + t_i$, *avec* $w_n = t_0 = 0$.

Des systèmes de numération redondants un peu analogues (en base 2) sont utilisés à l'intérieur de certains circuits de multiplication et division pour accélérer les nombreuses additions que ces opérations nécessitent. Le résultat final est converti dans un système usuel de sorte que cette utilisation d'un système redondant en interne est complètement transparente pour l'utilisateur.

V - POUR EN SAVOIR PLUS

J'espère vous avoir persuadé que même l'addition et la multiplication sont encore (un peu) du domaine de la recherche. Le lecteur qui souhaite en savoir plus sur l'arithmétique virgule flottante pourra consulter Boldo *et al.* (2023b). Les algorithmes utilisés en matériel (c'est-à-dire dans des circuits intégrés) pour effectuer des opérations arithmétiques sont décrits dans plusieurs ouvrages (il suffit de taper « computer arithmetic » ou « digital arithmetic » sur Google), mais j'ai un petit faible pour celui de Ercegovac et Lang (2004). Sur l'utilisation de techniques de preuve formelle pour valider des algorithmes critiques, le livre de Boldo et Melquiond (2017) est un incontournable. La personne désirant suivre les travaux de la communauté française d'arithmétique des ordinateurs peut s'inscrire au groupe de travail « Arith » du GDR IFM sur le site `https://mygdr.hosted.lip6.fr/`.

VI - BIBLIOGRAPHIE

AVIZIENIS, A. (1961). Signed-digit number representations for fast parallel arithmetic. *IRE Transactions on Electronic Computers*, 10:389–400.

BOLDO, S., BRISEBARRE, N. et MULLER, J.-M. (2023a). Le dilemme du fabricant de tables. *La Recherche*, (572).

BOLDO, S., JEANNEROD, C.-P., MELQUIOND, G. et MULLER, J.-M. (2023b). Floating-point arithmetic. *Acta Numerica*, 32:203–290.

BOLDO, S. et MELQUIOND, G. (2017). *Computer Arithmetic and Formal Proofs*. ISTE Press - Elsevier.

BOUDOT, F., GAUDRY, P., GUILLEVIC, A., HENINGER, N., THOMÉ, E. et ZIMMERMANN, P. (2020). Nouveaux records de factorisation et de calcul de logarithme discret. *Techniques de l'Ingénieur*, 12-2020:1–10.

BRENT, R., PERCIVAL, C. et ZIMMERMANN, P. (2007). Error bounds on complex floating-point multiplication. *Mathematics of Computation*, 76:1469–1481.

BRISEBARRE, N., HANROT, G. et ROBERT, O. (2017). Exponential sums and correctly-rounded functions. *IEEE Transactions on Computers*, 66(12):2044–2057.

CERUZZI, P. E. (1981). The early computers of Konrad Zuse, 1935 to 1945. *Annals of the History of Computing*, 3(3):241–262.

ERCEGOVAC, M. D. et LANG, T. (2004). *Digital Arithmetic*. Morgan Kaufmann Publishers, San Francisco, CA.

FLEGG, G., HAY, C. et MOSS, B. (1985). *Nicolas Chuquet, Renaissance Mathematician, A study with extensive translation of Chuquet's mathematical manuscript completed in 1484*. Springer Dordrecht.

HIRSHFELD, A. (2009). *Eureka Man, The life and legacy of Archimedes*. Walker & Company.

JEANNEROD, C.-P., KORNERUP, P., LOUVET, N. et MULLER, J.-M. (2017). Error bounds on complex floating-point multiplication with an FMA. *Mathematics of Computation*, 86:881–898.

KAHAN, W. (1981). Why do we need a floating-point arithmetic standard? Rapport technique, Computer Science, UC Berkeley. `http://www.cs.berkeley.edu/~wkahan/ieee754status/why-ieee.pdf`.

KNOWLES, S. (2001). A family of adders. *In Proceedings 15th IEEE Symposium on Computer Arithmetic. ARITH-15 2001*, pages 277–281.

MALCOLM, M. A. (1972). Algorithms to reveal properties of floating-point arithmetic. *Communications of the ACM*, 15(11):949–951.

MULLER, J.-M. (1995). Algorithmes de division pour microprocesseurs : illustration à l'aide du " Bug " du Pentium. *Technique et Science Informatiques*, 14(8):1031–1049. https ://hal.science/hal-04143937/file/MullerPentiumBug95.pdf.

MULLER, J.-M. et RIDEAU, L. (2022). Formalization of double-word arithmetic, and comments on "Tight and rigorous error bounds for basic building blocks of double-word arithmetic". *ACM Transactions on Mathematical Software*, 48(2):1–24.

RUMP, S. M. (2012). Error estimation of floating-point summation and dot product. *BIT Numerical Mathematics*, 52(1):201–220.

SIBIDANOV, A., ZIMMERMANN, P. et GLONDU, S. (2022). The CORE-MATH project. *In 29th IEEE Symposium on Computer Arithmetic*. https://hal.inria.fr/hal-03721525.

NOMBRES, OPÉRATIONS ET PROBLÈMES RÉCRÉATIFS : HISTOIRE(S) PARFAITE(S) ET FIGURÉE(S) POUR ENSEIGNER L'ARITHMÉTIQUE EN CYCLE 3

Marc MOYON
INSPÉ DE L'ACADÉMIE DE LIMOGES, UNIV. LIMOGES, CNRS
XLIM, UMR 7252
marc.moyon@unilim.fr

Résumé
Cette contribution a pour objectif d'afficher quelques exemples de ce qui pourrait, dans l'histoire et l'épistémologie des mathématiques, être introduit pour travailler l'arithmétique dès la fin de l'école primaire et tout au long du collège (voire du lycée). L'histoire des mathématiques, quelle que soit l'époque, quelle que soit la culture, quelle que soit la langue, nourrit les enseignants et permet en particulier de construire des ressources pédagogiques originales à tous les niveaux de l'enseignement des mathématiques, comme le montrent les nombreux travaux des IREM, de la commission inter-IREM « histoire et épistémologie » et ceux du groupe international HPM (history and pedagogy of mathematics). Même si les sources historiques peuvent paraître difficiles d'accès pour un élève de cycle 3, elles offrent néanmoins de nombreuses opportunités pour travailler le concept de nombres, les opérations élémentaires et le raisonnement arithmétique. Il s'agit ici de le démontrer à partir de trois exemples principaux : les nombres figurés et polygonaux, les abaques à jetons à partir de comptabilités médiévales, la duplication égyptienne et le code binaire.

I - INTRODUCTION

Si l'on s'intéresse aux documents officiels disponibles pour le cycle 3 afin de comprendre comment l'arithmétique et ses raisonnements peuvent être entendus et définis dans le champs scolaire[1], il est difficile de trouver une définition précise de l'arithmétique, en tant que chapitre des mathématiques de l'école. Le terme est néanmoins très souvent employé pour caractériser des problèmes faisant intervenir les quatre opérations élémentaires : addition, soustraction, multiplication et division. Une étude des principaux dictionnaires (mathématiques) disponibles s'est montrée nécessaire[2]. Le Lionnais fournit une longue description dans son dictionnaire dont les passages suivants sont extraits :

D'abord limitée [..] *à des procédés de calcul combinant des entiers naturels par des opérations élémentaires,*

[1] L'ensemble des ressources sont disponibles sur https://eduscol.education.fr/251/mathematiques-cycle-3.

[2] Deledicq et Launay (2021) n'ont aucune entrée pour « arithmétique » dans leur *Dictionnaire amoureux des mathématiques*. Le *Dictionnaire des mathématiques* de la collection "Encyclopaedia Universalis" (coordonné par J.-L. Verley) n'a pas plus d'entrée « arithmétique » et sa lecture ne m'a pas permis de dégager une caractérisation simple de la discipline.

> *l'arithmétique s'est ensuite donnée pour but l'étude des relations des nombres rationnels entre eux et avec des opérations.* […] *L'arithmétique a le privilège d'avoir passionné les mathématiciens les plus éminents en même temps qu'elle n'a cessé d'attirer les amateurs. Cette séduction tient, pour beaucoup, dans ce dernier cas, au fait que des problèmes très difficiles, parfois non résolus, ont souvent des énoncés simples qui peuvent être compris à partir d'une formation mathématique presque inexistante. (Bouvier, Georges et Le Lionnais, 1993, p. 63)*

Enfin, Busser et Hauchecorne (2021) rédigent une notice dans leur *Dictionnaire décalé des mathématiques* :

> *Quel joli mot, un tantinet désuet, et dont la racine grecque nous rappelle ses débuts dans l'Antiquité. Les Grecs se posaient déjà de nombreux problèmes de son ressort.* […] *De nos jours, on préfère parler de théorie des nombres.* […] *Dans le sens commun, l'arithmétique concerne les opérations sur les nombres entiers positifs et leurs propriétés. (Busser et Hauchecorne, 2021, pp. 13-14)*

Le CNRTL (Centre National de Ressources Textuelles et Lexicales) définit l'arithmétique comme « la science qui a pour objet l'étude de la formation des nombres, de leurs propriétés et des rapports qui existent entre eux[3] ». Si le terme 'arithmétique' est « un tantinet désuet », la discipline qu'il représente a une longue histoire, depuis l'Antiquité jusqu'à nos jours où les mathématiciens et amateurs éclairés s'intéressent toujours aux problèmes anciens non résolus[4] et à de nouvelles questions. Il ne peut donc pas s'agir ici de brosser cette histoire même à grands traits, mais plutôt de lever le voile sur certains épisodes sélectionnés qui permettent d'en dégager quelques intérêts pour l'enseignement d'aujourd'hui, et d'illustrer l'universalité et l'interculturalité des questions sur les nombres (ici, entiers positifs) et leurs opérations.

C'est dans ce contexte qu'il faut entendre : « La mise en perspective historique de certaines connaissances (numération de position, apparition des nombres décimaux, du système métrique, etc.) contribue à enrichir la culture scientifique des élèves. » Voilà, le décor est planté. Il s'agit, d'après les instructions officielles – ici, le programme de cycle 3, cycle de consolidation[5] – d'« enrichir la culture scientifique des élèves ». Nous ne saurions être en accord avec ce point de vue que si la science (les mathématiques pour ce qui nous concerne) elle-même, et sa pratique, font intégralement partie de ladite « culture scientifique ». En effet, il est évident que la culture scientifique ne peut être envisagée indépendante de la science et nous insisterons, ici comme ailleurs, sur l'importance d'une telle culture scientifique pour les élèves, mais aussi pour les enseignants (Moyon, 2012).

Aussi, nous ne formulerons pas ci-après des recommandations sur le comment et le pourquoi intégrer l'histoire des mathématiques dans l'enseignement et l'apprentissage des mathématiques : la littérature sur

[3] https://www.cnrtl.fr/definition/arithmétique.

[4] Le meilleur exemple est probablement la démonstration d'Andrew Wiles en 1994 du fameux théorème de Fermat, clôturant ainsi plus de 3 siècles de recherche.

[5] Programme de cycle, 2020 ; BO n°31 du 30 juillet 2020.

le sujet est plurielle et généreuse[6]. Il ne s'agit pas plus d'une nouvelle étude empirique, au sens défini par Jankvist (2009b) et repris par Guillemette (2011), comme il en existe de nombreuses[7] :

> [Jankvist] *entend par études empiriques, les recherches allant de la petite étude qualitative à la grande étude quantitative qui, par l'expérimentation et l'emploi de tests, questionnaires, entrevues ou d'une méthodologie quelconque, discutent et élaborent des conclusions à partir de données recueillies sur le terrain. (Guillemette, 2011, p. 11)*

La seule ambition de cette contribution est donc de décrire des exemples documentés issus de l'histoire des mathématiques, accompagnés d'une large bibliographie, qui seraient propices aux travaux et autres réflexions arithmétiques en cycle 3 (voire en cycle 4 et au lycée). Mais nous ne ferons pas état d'analyses didactiques ou de « données recueillies sur le terrain », en dehors de certaines références bibliographiques. Aussi, nos exemples ne doivent pas être vus comme des incontournables ou des modèles : il faut les envisager comme des jalons illustrant une longue histoire, des épisodes historiques ayant laissé des traces (images, textes, artefacts…) qui nourrissent à la fois les réflexions pédagogiques et didactiques de tout enseignant, et les réflexions mathématiques des élèves lorsqu'elles sont opportunément utilisées en classe[8]. Il est donc indispensable de considérer ces exemples à leur juste valeur : des ressources (voire des supports) pour des situations d'apprentissage (à construire) variées et nombreuses permettant aux élèves d'apprécier le rôle des mathématiques dans le développement des sociétés (Fauvel et van Maanen, 2000, pp. 1-29). Reprenant la classification de Jankvist (2009a), nous pensons que ces exemples sont adaptés à une « approche par modules d'apprentissages » plutôt que nourrir des anecdotes ou des petites capsules historiques dont les valeurs didactiques restent discutables : l'histoire illustre un sujet mathématique central, incluant éventuellement l'utilisation de sources primaires.

Les manuscrits originaux[9] sont propices à un travail très intéressant, à l'image de la table de multiplication (en numération romaine) de la figure 1. L'observation est alors essentielle pour formuler des hypothèses (Que représente le document ? Comment est-il organisé ? Comment peut-on le comprendre ?...). Les élèves sont alors amenés à analyser le document, pour formuler des hypothèses et, le cas échéant, conclure. L'observation est nécessairement active : les élèves ne peuvent pas se limiter à la seule description visuelle du document. En effet, s'agissant de documents mathématiques, les comprendre implique de percer (tous) les secrets des nombres et des opérations, explicites comme implicites. C'est la voie à suivre pour que les élèves testent leurs hypothèses et justifient leur conclusion. Le document historique peut être le point de

[6] Voir la récente synthèse rédigée par Chorlay, Clark et Tzanakis (2022).

[7] Guillemette (2011) approfondit l'étude du cadre méthodologique employé dans les études empiriques analysées par Jankvist (2009b).

[8] Nous laissons ici aux lecteurs les éventuelles exploitations pédagogiques. Cette contribution n'a pas pour objet de construire des séances clés en main ou une quelconque ingénierie didactique. Au mieux, nous renvoyons à la littérature de référence, laissant le soin aux professionnels de l'enseignement et de la formation des enseignants de tirer un bon parti de ces ressources, de ces (nouveaux) éclairages.

[9] Les références des manuscrits seront systématiquement données ainsi que les liens (entre crochets droits) qui y donneraient accès, lorsque cela est possible.

départ d'un apprentissage (séance d'introduction) ou, au contraire une tâche finale ; cela dépend du document et du contrat didactique pensé par l'enseignant.

Figure 1 : Table de multiplication dans le De institutione arithmetica, *Boèce – Londres, British Library, ms. Harley 549, fol. 14r°, 12e s. [https://www.bl.uk/fr- fr/collection- items/boethius- de- institutione- arithmetica]*

Enfin, si l'enseignant fait le choix d'une lecture de textes anciens, alors Fried (2007) montre l'importance d'une double lecture : en tant que mathématicien (comprendre le texte, le raisonnement, en donner une écriture moderne pour s'assurer de la bonne compréhension) bien sûr, mais aussi en tant qu'historien (se plonger dans l'époque de la source, éviter les anachronismes, situer la source dans la longue histoire des mathématiques notamment)[10].

[10] Pour Fried (2007), la lecture de l'historien est dite "diachronique" tandis que celle du mathématicien est "synchronique" ; les deux lectures étant complémentaires. L'histoire est l'élément clé d'un enseignement qui inculquerait le sens de l'activité mathématique ayant des aspects à la fois non historiques et historiques afin d'avoir une vision plus complète des mathématiques elles-mêmes. À partir de la lecture de Diophante et Euler, Barbin (2022) met en évidence trois niveaux de lecture en fonction de l'objectif (épistémologique, culturel ou épistémique) et des pratiques pédagogiques (utiliser, introduire ou intégrer l'histoire des mathématiques en classe).

À travers les différents exemples proposés dans cette contribution[11], il s'agit, entre autres : (1) de donner à voir les mathématiques d'avant (les contenus, les écritures), mettant en lumière l'évolution progressive de la discipline (aussi bien dans le fond que dans la forme) ; (2) d'accéder à des sujets et problèmes variés ; (3) d'approfondir la compréhension des mathématiques ; (4) d'humaniser les mathématiques ; (5) de montrer que les mathématiques existent dans divers contextes et milieux.

Finalement, de manière générale, dans le cadre de l'éducation mathématique (ici, de l'arithmétique), l'histoire est plutôt envisagée comme un outil et non comme un objectif en soi. En effet, l'intention et l'ambition d'un enseignant (de mathématiques) à l'école, au collège ou au lycée est bien l'enseignement/l'apprentissage des mathématiques et non celui de l'histoire des mathématiques. Ainsi, l'enseignant de mathématiques (y compris le professeur des écoles) se doit de mettre les concepts propres à la discipline au centre de sa réflexion (et de celle des élèves), s'aidant de l'histoire et de l'épistémologie pour mieux les interroger ou/et les contextualiser.

II - DES NOMBRES FIGURÉS AUX PROPRIÉTÉS ARITHMÉTIQUES : LES NOMBRES POLYGONAUX

Les nombres figurés sont des nombres qui peuvent être représentés par un ensemble de points disposés dans des configurations géométriques particulières[12] : il s'agit alors d'une collection de points à compter. Les nombres figurés sont intéressants pour l'enseignement des mathématiques pour deux (au moins) raisons majeures. D'abord, ils offrent naturellement aux enseignants l'opportunité de travailler le fameux triptyque « manipuler, verbaliser, abstraire » à partir des points et des représentations géométriques. Ils permettent ensuite de faire le lien entre l'arithmétique (les nombres) et la géométrie[13].
Les nombres polygonaux, quant à eux, sont des nombres figurés particuliers où les 'configurations géométriques' correspondent à des polygones réguliers. De nombreux mathématiciens ont largement développé l'étude des nombres figurés en général, ou des nombres polygonaux et pyramidaux en particulier[14].

1. Les nombres polygonaux : quelques repères historiques

Au moins depuis l'*Introduction arithmétique* (figure 2) du néo-pythagoricien[15] Nicomaque de Gérase (1er/2e s. ap. J.C.) dans lequel l'auteur expose largement les nombres figurés et leurs propriétés (chapitres VII à XX du livre II), ils sont largement traités dans de nombreux textes d'arithmétique, souvent au sein

[11] Les trois parties suivantes peuvent être lues de manière indépendante.

[12] Voir d'autres exemples de représentations spatiales dans Schwer (2018).

[13] En représentant les nombres ainsi, il est possible, par exemple, de distinguer les nombres pairs des impairs, de caractériser les nombres premiers, de visualiser et manipuler la notion de divisibilité d'un nombre. Les nombres figurés permettent en particulier de travailler le lien entre un nombre et une de ses représentations spatiales, « un pilier des mathématiques » qui invite à visualiser les nombres dans l'espace. Voir, à ce sujet, la note du conseil scientifique de l'Éducation Nationale n°5, février 2022.

[14] Alors que je rédige cette contribution, le magazine *Tangente* publie un dossier spécial (n°215, décembre 2023) consacré aux nombres figurés, et notamment au travail du mathématicien Francesco Maurolico (1494-1575). J'en conseille la lecture.

[15] Pythagore (6e s. av. J.C. ?) pourrait être à l'origine des nombres figurés.

d'un chapitre dédié. Diophante (3e s. ap. J.C. ?) y consacre même un court livre composé de cinq propositions (dont la dernière est incomplète) avec son *De polygonis numeris*[16].

L'*Introduction arithmétique* de Nicomaque[17] est d'une grande importance dans l'histoire des mathématiques, notamment grâce aux traductions en arabe et en hébreu dont elle bénéficie (Hofstetter, 2021). Au 8e s., Ḥabīb ibn Bahrīz produit une version à partir d'une traduction, perdue, du grec vers le syriaque. Cette nouvelle traduction est commentée et modifiée, dans le cadre de son enseignement, par al-Kindī (m. 870)[18]. Thābit Ibn Qurra (m. 901) réalise une autre traduction au 9e s. Ibn *Ṭ*āhir al-Baghdadī (m. 1037), quant à lui, développe aussi pleinement et de manière originale ce chapitre dans son important traité d'arithmétique *al-Takmila fī l-ḥisāb* [le complément en calcul][19]. Encore au 14e s., l'*Introduction arithmétique* fait l'objet d'une traduction en hébreu[20] par l'érudit originaire d'Arles Qalonymos ben Qalonymos (m. après 1329). La connaissance précise du corpus néo-pythagoricien va permettre aux mathématiciens des pays d'Islam, en Orient comme nous venons de le voir mais aussi en Occident, de réaliser des développements originaux sur les nombres polygonaux et les progressions arithmétiques. Par exemple, les nombres polygonaux sont généralisés à un ordre quelconque et étendus grâce à une interprétation combinatoire à l'aide des coefficients binomiaux[21]. Parmi les auteurs de l'Occident musulman (Maghreb et al-Andalus), on peut citer Ibn Munᶜim (m. 1228) ou encore Ibn al-Bannā (m.1321) qui produisent, dans leur ouvrage respectif le *Fiqh al-ḥisāb* [La science du calcul] pour le premier et le *Rafᶜ al-ḥijāb* [Lever du voile] pour le second, d'importants développements sur les nombres figurés et les propriétés arithmétiques qu'ils permettent de démontrer (Djebbar, 2000, 2004). Enfin, très récemment, Djebbar (2022) a montré tout l'intérêt du *Kitāb al-iqtiṣār* [Livre de l'essentiel] d'Abū l-Ṣalt (m. 1134), encore inédit.

En latin, Boèce (m. 524) est sans aucun doute le représentant de la tradition néo-pythagoricienne le plus important et le plus répandu. Le *De institutione arithmetica* [Institution arithmétique] (figure 3) fournit des extraits significatifs des développements sur les nombres figurés.

---

16 La première édition grecque a été réalisée par C. G. de Bachet de Méziriac avec une traduction latine, en même temps que celles des six livres des *Arithmétiques* alors connus (Diophante d'Alexandrie, 1621). Après l'édition critique de P. Tannery (Diophante d'Alexandrie, 1893-95), P. Ver Ecke traduit le texte en français en 1959 (Diophante d'Alexandrie, 1959) et enfin, F. Acerbi en donne une nouvelle édition (Diophante d'Alexandrie, 2012) qui est aujourd'hui l'édition de référence (avec une traduction italienne).

17 La traduction française de référence reste celle de Janine Bertier ; (Nicomaque de Gérase, 1978).

18 Dans toute la suite du texte, je précise, après la première occurrence d'un auteur, sa date de mort à l'aide de l'abréviation m. (lorsqu'on la connaît), ou sa période d'activité.

19 Saidan (1997) résume les éléments nouveaux d'al-Baghdadī alors qu'il s'interroge à propos de « l'influence grecque sur l'arithmétique arabe ».

20 Voir l'étude séminale de Freudenthal et Lévy (2004) pour la tradition hébraïque.

21 Cette nouvelle extension dépasse le cadre de la présente contribution, voir (Rashed, 1983).

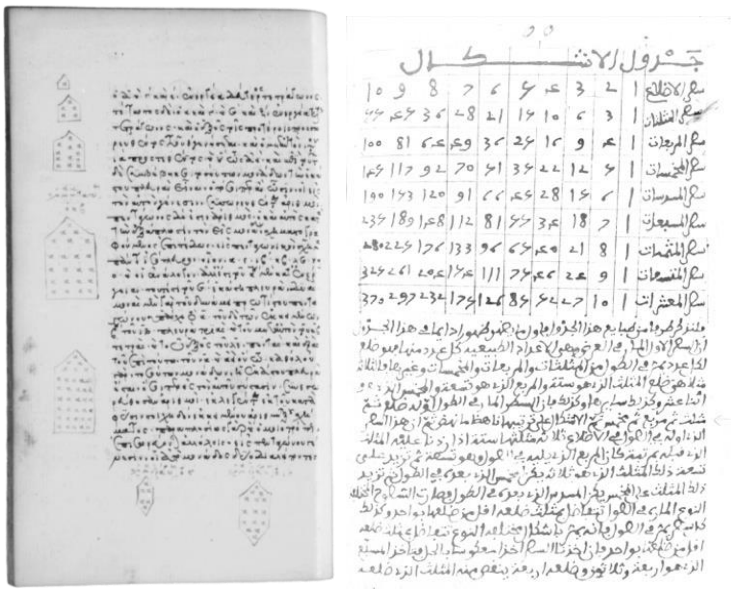


*Figure 2 : (à gauche) Copie du Livre II de l'*Introduction arithmétique *de Nicomaque de Gérase, Paris, BnF, Grec 2762, fol. 49v°, faisant apparaître en marge des nombres figurés. [https://gallica.bnf.fr/ark:/12148/btv1b107221294] (à droite) Copie du* Fiqh al-ḥisāb *[La science du calcul] d'Ibn Munᶜim*[22]*, ms. Rabat BG 416 Q, p. 300.*

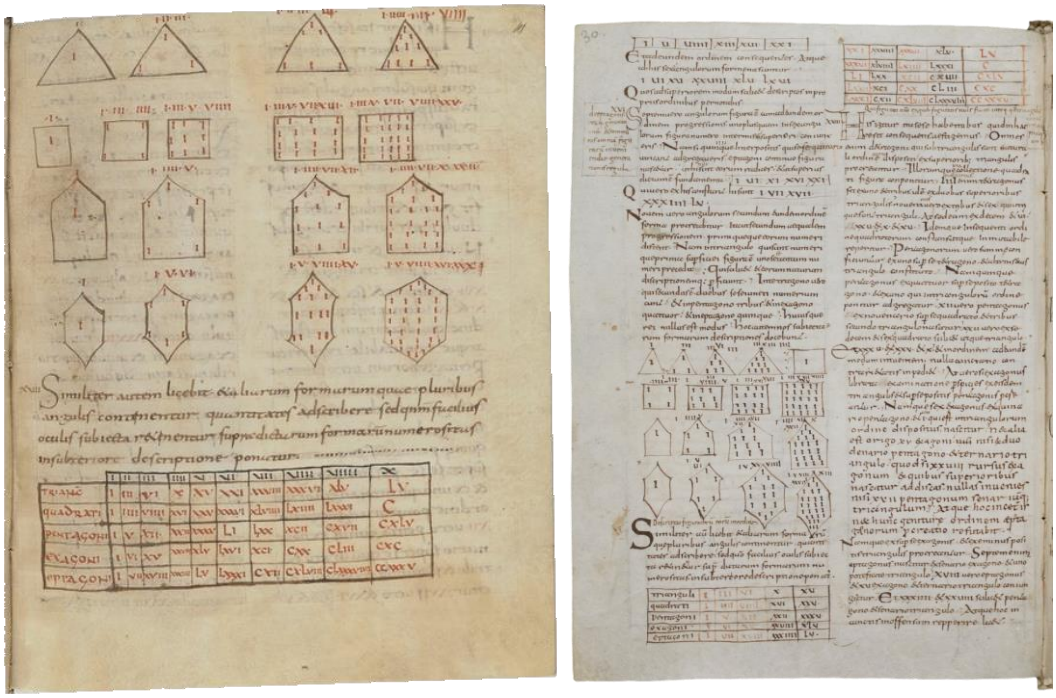


Figure 3 : Figures des nombres polygonaux dans des copies de la tradition boécienne avec tableau de correspondance (voir tableau 1). (à gauche) Paris, BnF, ms. lat. 10251, fol.41r° (manuscrit, 9ᵉ-10ᵉ s.) [https://gallica.bnf.fr/ark:/12148/btv1b105422015] (à droite) Bibliothèque de l'abbaye de Saint-Gall (Suisse), cod. Sang. 248, p. 30 (parchemin du milieu du 9ᵉ siècle) [https://www.e-codices.unifr.ch/fr/list/one/csg/0248]

Pour éviter tout problème de lecture et pour montrer explicitement l'intérêt d'une telle représentation tabulaire, le tableau 1 ci-dessous reprend (en chiffres indo-arabes) les nombres polygonaux des manuscrits

[22] Je remercie Ahmed Djebbar de m'avoir donné une copie de cette page.

de la figure 3 et celui de la figure 2 (à droite). Il s'agit des dix premiers termes des suites des nombres polygonaux (à partir des nombres triangulaires).

Tableau 1 : Tableau des premiers nombres polygonaux. Les lignes vertes ne sont écrites que dans la figure 2 (à droite); la figure 3 ne fait apparaître que les lignes noires.

	1er	2e	3e	4e	5e	6e	7e	8e	9e	10e
Triangle	1	3	6	10	15	21	28	36	45	55
Carré	1	4	9	16	25	36	49	64	81	100
Pentagone	1	5	12	22	35	51	70	92	117	145
Hexagone	1	6	15	28	45	66	91	120	153	190
Heptagone	1	7	18	34	55	81	112	148	189	235
[Octogone]	1	8	21	40	65	96	133	176	225	280
[Ennéagone]	1	9	25	46	75	111	174	204	261	325
[Décagone]	1	10	27	52	85	126	175	232	297	370

2. La formation des nombres polygonaux

La formation des nombres polygonaux n'est pas simple pour les élèves. Pour mieux comprendre, suivons le vieil adage « une image vaut mieux qu'un long discours » et observons ce que le mathématicien et ingénieur des travaux publics de l'État Émile Fourrey (m. 1959) a représenté dans ses *Récréations arithmétiques* au début du 20e siècle (figure 4).

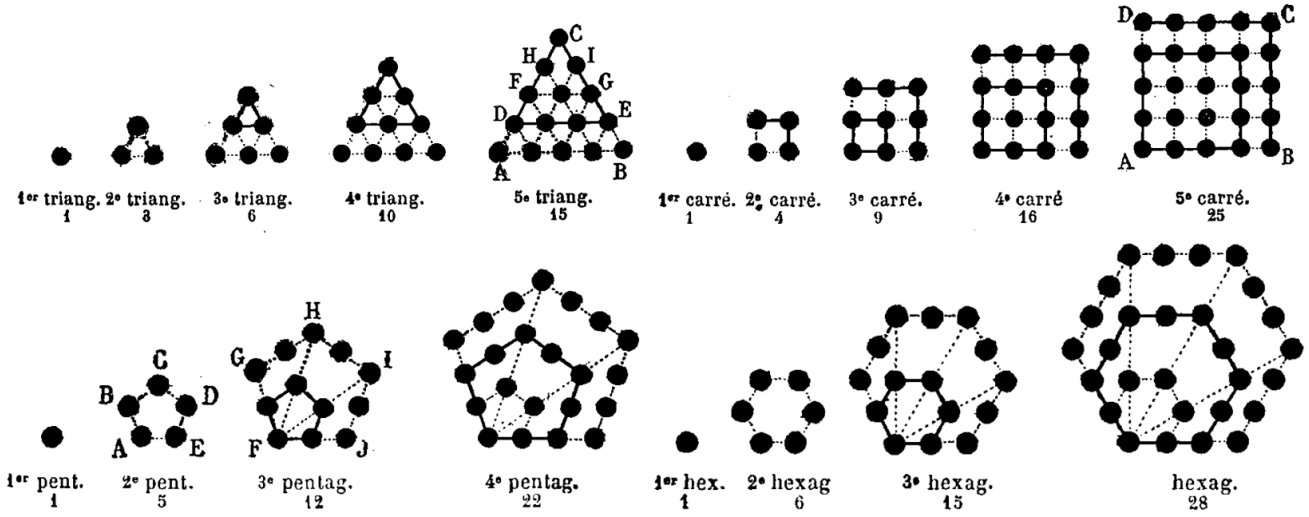


Figure 4 : La construction des nombres polygonaux dans Fourrey (1901, pp. 56-64)

Chaque nombre polygonal est obtenu à partir du précédent en ajoutant un « gnomon », c'est-à-dire une figure qui, ajoutée à la précédente, forme une nouvelle figure semblable à la précédente. Il s'agit de transformer le polygone en un nouveau polygone (semblable), avec un point de plus sur chacun de ses côtés. Prenons l'exemple des nombres hexagonaux (figure 5).

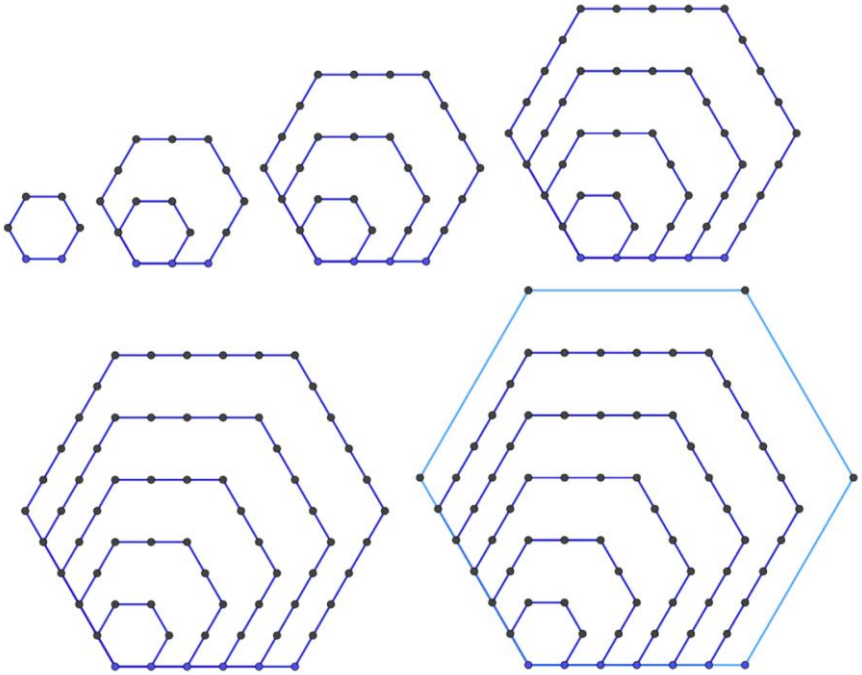


Figure 5 : Formation des nombres hexagonaux (6 ; 15 ; 28 ; 45 ; 66 ; 91)

Ainsi, par exemple, les nombres triangulaires correspondent aux nombres {1 ; 1+2 ; 1+2+3 ; 1+2+3+4 ;…} et le n-ième nombre triangulaire est : 1+2+3+4+…+n ; c'est-à-dire la somme des n premiers entiers. Le gnomon, soit la différence entre deux nombres consécutifs, est une simple ligne (la 'base' du nouveau triangle) ; la suite des gnomons correspond alors à la suite des nombres entiers à partir de 2.

Les nombres carrés sont les nombres $\{1^2 ; 2^2 ; 3^2 ; 4^2 ; 5^2 ;\ldots\}=\{1 ; 4 ; 9 ; 16 ; 25 ;\ldots\}$, c'est-à-dire la suite des nombres carrés et le n-ième terme est n^2. Le gnomon est ici une équerre – construit sur deux (= 4 – 2) côtés contenant respectivement 2 points et 1 seul – ; la suite des gnomons correspond alors aux nombres impairs successifs à partir de 3 : {1 ; 3 ; 5 ; 7 ;… ; 2k-1 ; …}.

Considérons les nombres pentagonaux. Ce sont les nombres {1 ; 1+4 ; 1+4+7 ; 1+4+7+10 ; …}, soit la suite {1 ; 5 ; 12 ; 22 ; …}. Le gnomon à l'ordre n est alors construit sur trois (= 5 – 2) côtés (ce qui complète le pentagone à partir du nombre précédent) de n points. Mais, comme ces côtés se rencontrent en 2 points : le gnomon compte $3n$ – 2 points.

Considérons enfin les nombres hexagonaux. Ce sont les nombres {1 ; 1+5 ; 1+5+9 ; 1+5+9+13 ; …}, soit la suite {1 ; 6 ; 15 ; 28 ; …}. Le gnomon à l'ordre n est alors construit sur quatre (= 6 – 2) côtés de n points. Mais, comme ces côtés se rencontrent en trois (= 6 – 3) points : le gnomon compte $4n$ – 3 points.

De manière générale[23], considérons un nombre k-polygonal (polygone à k côtés). Son gnomon à l'ordre n est construit sur (k-2) côtés contenant chacun n points, se coupant en (k-3) points. Le gnomon compte alors $n(k-2)-(k-3)$ points. C'est donc la suite de nombres {1 ; k – 1 ; 2k – 3 ; 3k – 5 ;…}. Aussi, on remarque

[23] La lecture de ce paragraphe (niveau lycée) n'est pas nécessaire pour comprendre la suite de la contribution, on peut s'en dispenser en première lecture. Il nous semble que les premiers exemples avec les représentations géométriques et le tableau 1 permettent d'une part de comprendre suffisamment les nombres polygonaux et d'autre part de mettre en place des séances de travail en classe de mathématiques, à partir de diverses manipulations.

que la suite des gnomons des nombres (k+2)-polygonal est {1 ; k + 1 ; 2k + 1 ; 3k + 1 ; …; (n-1)k + 1 ; …} : il s'agit de l'expression d'une suite arithmétique de raison k. Aussi la suite des nombres (k+2)-polygonaux est (1 ; k+2 ; 3k+3 ; 6k+4 ; ... ; $n+\frac{1}{2}n(n-1)k$; …) correspondant aux sommes partielles de la suite arithmétique précédente (avec n le rang du nombre (k+2)-polygonal). On retrouve facilement les nombres du tableau 1 précédent avec k = 1 pour les nombres triangulaires (1 + 2 = 3), k = 2 pour les nombres carrés (2+2 = 4), k = 3 pour les nombres pentagonaux…

3. Quelques propriétés arithmétiques élémentaires

> *Cette représentation des nombres entiers à travers des figures géométriques usuelles (nombres triangulaires, nombres carrés, nombres oblongs) a facilité l'établissement de règles arithmétiques entre ces nombres, par la seule considération de la disposition de leurs unités. (Chambon, 2020, p. 62)*

Dans cette partie, nous nous proposons de révéler quelques-unes de ces propriétés arithmétiques que les nombres polygonaux permettent de montrer[24]. Pour démontrer de façon plus académique – c'est-à-dire avec la rigueur que le programme de mathématiques exigerait –, le calcul littéral sera utile au collège, et au lycée, le raisonnement par récurrence peut être intéressant.

Parmi les propriétés les plus élémentaires, citons « la différence des carrés de deux nombres consécutifs est égale à la somme de ces deux nombres » (proposition 1) ou encore « la somme de deux nombres triangulaires consécutifs est égale à un carré » (proposition 2). Les figures 6 et 7 dévoilent explicitement ces énoncés pour un cas général (à condition d'accepter les implicites des points de suspension).

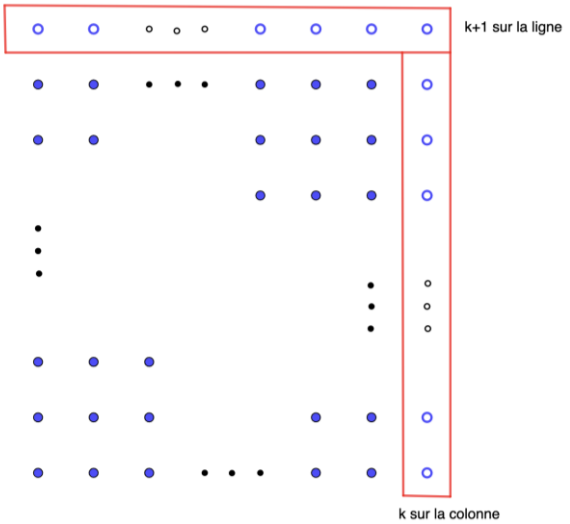


Figure 6 : Illustration de la proposition 1 : le gnomon (équerre) rouge est exactement la différence entre le grand carré (construit sur k+1) et le petit carré (construit sur k), donc, $C_{k+1} - C_k = (k+1) + k$ pour tout k entier, si C_k est le nombre carré d'ordre k (i.e. k^2).

[24] Bien d'autres propriétés peuvent être montrées et des problèmes résolus, nous avons limité ici (par contraintes éditoriales) notre choix aux plus simples. Certaines des propriétés les plus élémentaires sont énoncées et facilement démontrables au collège à condition d'accepter d'utiliser le calcul littéral. L'observation des nombres figurés et/ou polygonaux permet de faire travailler l'intuition chez les plus petits (avant l'introduction du calcul littéral) et de penser des dispositifs de remédiation (au moment de l'introduction de la lettre, par exemple).

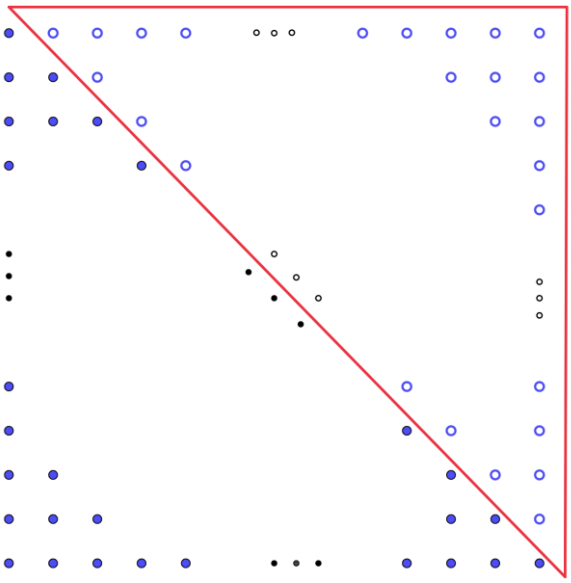


Figure 7 : Illustration de la proposition 2 : $T_k + T_{k-1} = k^2$ pour tout k entier, si T_k est le nombre triangulaire d'ordre k.

3.1. La somme des entiers

Si l'on considère un arrangement et une bonne combinaison (figure 8) du nombre triangulaire d'ordre n (pris deux fois), on observe qu'il produit le nombre rectangulaire ou oblong (n ; n+1).

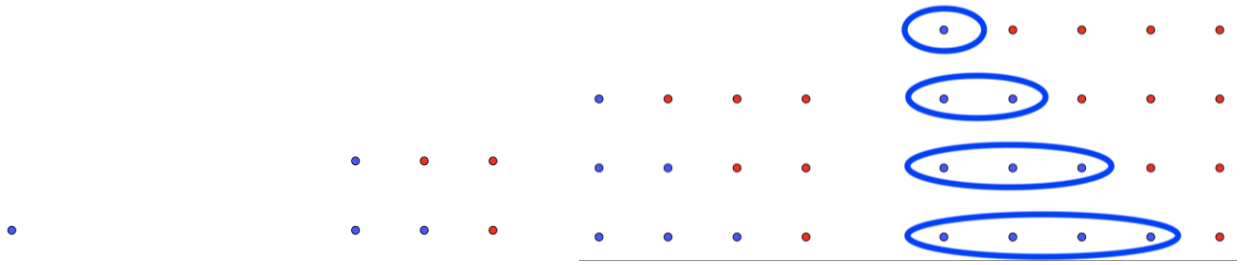


Figure 8 : Combinaison de nombres triangulaires (d'ordre 1, 2, 3 et 4)

Or, il a été montré précédemment que le nombre triangulaire d'ordre n correspond à la somme des n premiers nombres entiers (ce qui se vérifie visuellement sur la figure 8, les points entourés en bleu).

Ainsi, on a :

$$2 \times (1 + 2 + 3 + 4 + \cdots + n) = n \times (n + 1)$$

Ou encore,

$$(1 + 2 + 3 + 4 + \cdots + n) = \frac{n \times (n + 1)}{2}$$

L'exemple avec le nombre triangulaire d'ordre 4 donne :

$$(1 + 2 + 3 + 4) = \frac{4 \times (5 + 1)}{2} = 10$$

3. La somme des impairs

Prenons maintenant la suite des nombres carrés (figure 9). Il a été précédemment expliqué que chaque nombre carré d'ordre *n* est construit à partir du nombre carré d'ordre *n-1* en ajoutant un gnomon (équerre) correspondant à (2*n*-1).

À l'aide du calcul littéral, on peut écrire : $n^2 = (n-1)^2 + (2n-1)$.

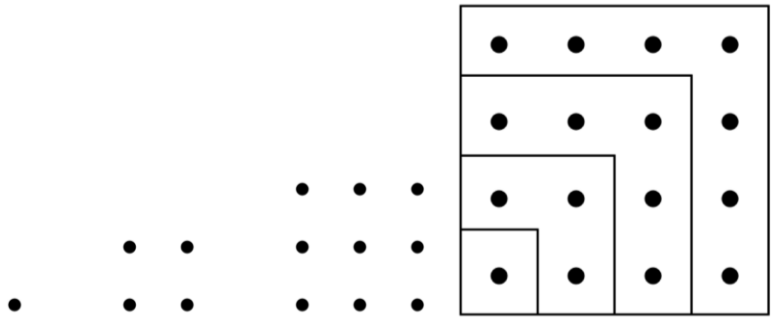


Figure 9 : Premiers nombres carrés (1; 4; 9; 16)

Mais, à partir de l'observation des nombres polygonaux carrés, on obtient en réalité une décomposition de chaque nombre carré en somme de nombres impairs. Autrement dit :

$$n^2 = 1 + 3 + 5 + 7 + \cdots + (2n-1)$$

Ainsi, on retient que la somme des *n* premiers nombres impairs est égale à n^2.

L'exemple avec le nombre carré d'ordre 4 donne :

$$4^2 = 1 + 3 + 5 + 7 = 16$$

III - LA DIVISION EUCLIDIENNE : LE QUOTIENT ET LE RESTE À PARTIR D'ANCIENNES MONNAIES

La division euclidienne apparaît dans les programmes de l'école, du collège et même du lycée avec notamment, l'étude des congruences. De nombreuses activités (notamment la « course à 20 » de Brousseau et ses variantes) existent pour travailler le sens et la technique de cette opération fondamentale où il est nécessaire de comprendre le résultat, constitué de deux nombres : le quotient et le reste.

Dans cette partie, il s'agit de construire le sens du quotient et du reste d'une division euclidienne grâce à la manipulation d'anciennes monnaies, à partir de l'exploitation d'archives historiques de comptabilités médiévales des villes ligériennes (Orléans, Tours, Blois)[25].

[25] Plusieurs animateurs IREM (moi-même, Vincent Beck d'Orléans, Sylviane Schwer de Paris-Nord et Agnès Gateau de Dijon) ont été impliqués, aux côtés d'historiens médiévistes, dans le projet CorMéCoULi [https://cormecouli.univ-tours.fr]. Une mallette

1. Contexte : les monnaies de compte

Les comptabilités médiévales des villes d'Orléans, Tours et Blois (comme d'autres villes françaises) sont en livres (parisis ou tournois), sous et deniers avec les conversions suivantes : 1 livre (£)=20 sous/sols (s) et 1 sou= 12 deniers (d). En outre, les comptes sont rédigés à l'aide de la numération romaine[26] (Moyon, à paraître). Les archives sont intéressantes à observer et à comprendre : elles sont propices à la rédaction de véritables problèmes arithmétiques et divers autres calculs[27].

Considérons un exemple, avec l'énoncé de la figure 11 qui décrit l'achat de bombardes (figure 10). Il s'agit d'une quittance de paiement (en livres tournois) à Pierre de Fosse pour l'achat de deux bombardes : l'une est grosse et pèse 614 (*vi^{c} xiiii*) livres (la livre est à la fois une unité de monnaie et une unité de masse), l'autre – moyenne – pèse 140 (*vii^{xx}*) livres. D'après le texte, les bombardes s'achètent à 3 (*iii*) sous et 4 (*iiii*) deniers la livre de poids. Ainsi, les deux bombardes coûtent 125 (*vi^{xx}v*) livres, 13 (*xiii*) sous et 4 (*iiii*) deniers. Cette somme est à la fois inscrite en première ligne et en marge de la dernière ligne (figure 11).

Figure 10 : Siège d'Orléans (1428-1429), avec une bombarde au premier plan.
https://commons.wikimedia.org/wiki/File:Siege_orleans.jpg

pédagogique a été élaborée à partir de ces comptabilités ; les matériaux pédagogiques sont téléchargeables sur https://www.centre-sciences.org/ressources/cormecouli-corpus-medieval-des-comptabilites-urbaines-ligeriennes.

[26] Même si ce n'est pas le propos de la présente contribution, j'attire l'attention du lecteur sur l'écriture de la numération romaine, notamment avec l'utilisation des exposants. La lecture et la compréhension de ces nombres peuvent être féconds tout au long du cycle 3.

[27] Dans ce cadre, la mallette pédagogique du projet susmentionné propose plusieurs problèmes additifs et multiplicatifs, plongés dans leur contexte historique des comptabilités des villes médiévales (défense de la ville, réparation, gestion des ordures, achats de matériel divers, organisation de banquets et fêtes religieuses…).

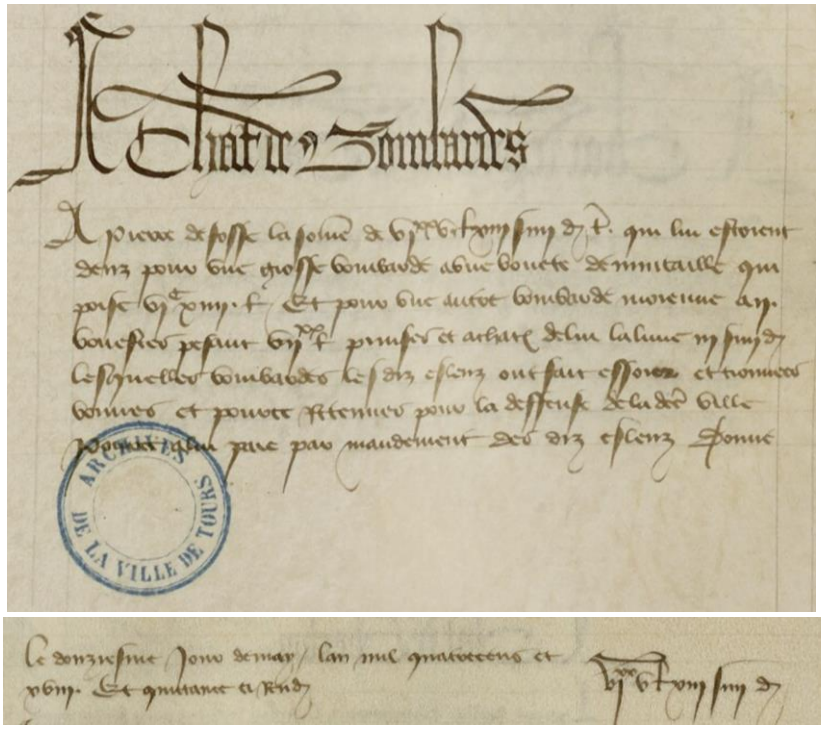


Figure 11 : « Achats de bombardes », extraits des fol. 45r° et fol. 45v° du manuscrit CC17 de Tours, © https://cormecouli.univ-tours.fr/FRAC037261-CCR017_091 (pièce datée de 1417-1418)

Le calcul du coût des deux bombardes est pédagogiquement intéressant car il implique le calcul de deux produits avec des nombres complexes (au sens de l'enseignement primaire, à savoir un nombre composé d'unités diverses, comme ceux en heures/minutes/secondes), respectivement 614 (140) par 3s. 4d. Une addition est alors nécessaire pour ajouter le prix des deux bombardes : 2 262 sous et 3 016 deniers. Une conversion[28] est ensuite nécessaire pour avoir une somme en livres (125), sous (13) et deniers (4). Cette conversion impose le calcul de divisions euclidiennes, en enregistrant à la fois le quotient et le reste. En effet, pour savoir combien 3 016 deniers font en livres/sous/deniers, divisons 3 016 par 240 (nombre de deniers dans une livre, 20 × 12) :

$$3\,016 = 240 \times 12 + 136$$

Comme $136 \geq 12$, je divise 136 par 12 (nombre de deniers dans 1 sou) :

$$136 = 12 \times 11 + 4$$

Ainsi, 3 016 deniers sont égaux à 12 livres, 11 sous et 4 deniers (*).

De même, pour 2 262 sous :

$$2\,262 = 113 \times 20 + 2$$

2 262 sous sont égaux à 113 livres et 2 sous (**).

[28] Bien sûr, une conversion peut être menée avant l'addition pour le prix de chaque bombarde, mais dans ce cas-là, une nouvelle conversion peut se révéler nécessaire avec la somme finale (c'est ici le cas).

L'addition de (*) et (**) donne bien la somme voulue : 125 livres, 13 sous et 4 deniers.

Ce type d'exercices est séduisant car il est planté dans un contexte historique vivant, réel, sans enrobage scolaire pseudo-réaliste. Le traitement des nombres complexes implique la manipulation de diverses unités dans un même système[29]. Ces exercices invitent les élèves à effectuer de nombreuses opérations sans s'en rendre réellement compte ; elles sont nécessaires pour vérifier les comptes, à l'image des officiers comptables royaux.

2. L'abaque à jetons

Pour faire les calculs (somme, différence, produit, division) sur les nombres précédents, les officiers de la comptabilité utilisaient des abaques à jetons : les jetons (ou *gects* en ancien français) (figure 12) représentent les nombres sur une table de compte, ou seulement un tapis. « Jeter » est alors synonyme de calculer. L'intérêt pédagogique des abaques à jetons a d'ores et déjà été démontré (Daval et Tournès, 2018). En outre, les abaques font traditionnellement partie du matériel pédagogique, même avant la mise en place d'un enseignement systématique du calcul pour toutes et tous. En effet, dans la seconde édition du *Dictionnaire* de Ferdinand Buisson (en 1911), Carlo Bourlet précise :

> *Si indispensable qu'il nous semble aujourd'hui, le calcul ne s'est introduit qu'assez tard et difficilement dans l'enseignement populaire. Il se borna pendant des siècles à l'usage des* abaques […] *Il existait quelques livres ou livrets à leur usage dès le seizième siècle […] On trouve aussi, sous le nom d'Antoine Cathalan, une* Arithmétique et manière d'apprendre à chiffrer et à compter par la plume et par les gects en nombre entier et rompu *(fractions), Lyon, 1555. (Bourlet, 1911, p. 1259)*

L'abaque, et notamment l'abaque à jetons, est particulièrement adapté aux calculs arithmétiques élémentaires[30]. Les additions et soustractions se font sans obstacle réel ; la multiplication et la division sont plus complexes à manipuler aujourd'hui mais ne posaient pas de difficultés insurmontables aux comptables médiévaux[31]. À ce titre, il est opportun de penser l'introduction d'un abaque à jetons dans les classes : là encore, il offre des manipulations qui peuvent remédier à certaines difficultés des élèves (problème des retenues notamment, le passage d'un ordre à un ordre supérieur, le 'cassage' pour la soustraction…). L'introduire dans un contexte historique est encore mieux : les comptabilités médiévales se présentent alors comme un cadre idéal.

*Figure 12 : Jeton de compte r°/v° avec un maître d'abaque (*rechenmeister*), Nuremberg, avant 1601. Diamètre : 29,6mm, masse : 3,99g*

[29] Il faut néanmoins veiller à ce que ce type d'exercices n'induise pas chez l'élève une conception erronée du nombre décimal, comme deux entiers juxtaposés (deux nombres entiers séparés par une virgule).

[30] À la suite du projet CorMéCoULi, une présentation du travail « Numérations, calculs et grandeurs : utilisation de l'abaque pour rendre visible les concepts communs » a été réalisée par Beck et Schwer au colloque de la Copirelem (Marseille, juin 2023).

[31] Certains ouvrages consacrés aux calculs avec les jetons expliquent même comment extraire des racines carrées.

Dans l'ouvrage imprimé d'Étienne de la Roche (m. 1530), en marge, sont représentés (figure 14) les jetons d'un abaque[32]. On observe les différentes unités décimales (*nombre* pour unité, *dizeine* = dizaine, *centeine* = centaine et *millier*) afin de mener les calculs en base 10, comme on est habitué à le faire aujourd'hui. En plus de ces lignes, on peut observer des espaces pour les *deniers* (sous les nombres), les *sous (solz)* (à gauche) et les livres (à droite). Ce type d'abaque est donc prévu pour une utilisation double : calcul sur la monnaie de compte (livres, sous, deniers) et calcul sur la numération décimale. La manipulation des jetons se fait de la même manière dans les deux systèmes, à condition de respecter les bases de conversion, à savoir 12 deniers pour 1 sous, et 20 sous pour 1 livre.

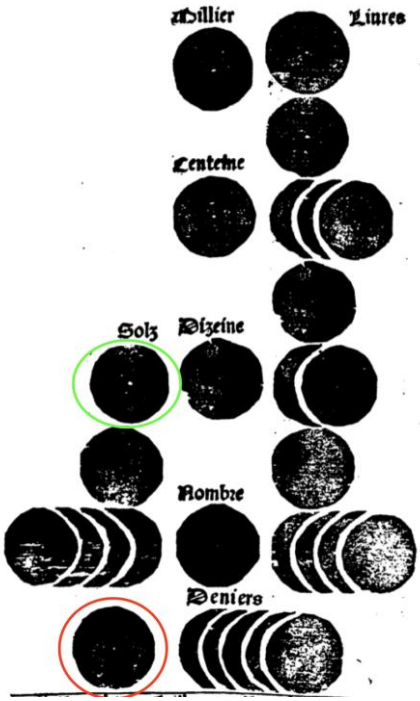


Figure 13 : Détail de l'abaque chez Étienne de la Roche (1538)

En effet, là où l'abaciste utilise la quinaire (1 jeton pour 5, i.e. la moitié de 10 ; 1 jeton pour 50, i.e. la moitié de 100…) posée dans l'espace intermédiaire (entre les lignes de l'unité et de la dizaine, entre celles de la dizaine et de la centaine…)[33], il utilise pour les deniers, de la même manière, un jeton pour 6 deniers (la moitié d'un sou) dans l'espace rouge de la figure 13, et un jeton pour 10 sous (la moitié d'une livre) dans l'espace vert de la figure 13 (il utilise aussi la quinaire pour 5 sous). C'est l'opération de réduction. Ainsi, si l'abaciste est amené à poser deux jetons dans l'espace rouge (12 deniers), c'est en fait 1 jeton dans les sous qu'il posera. De même, dès qu'il est invité à poser deux jetons dans l'espace vert (20 sous), c'est 1 jeton dans les unités de livres qu'il posera. C'est l'opération de conversion.

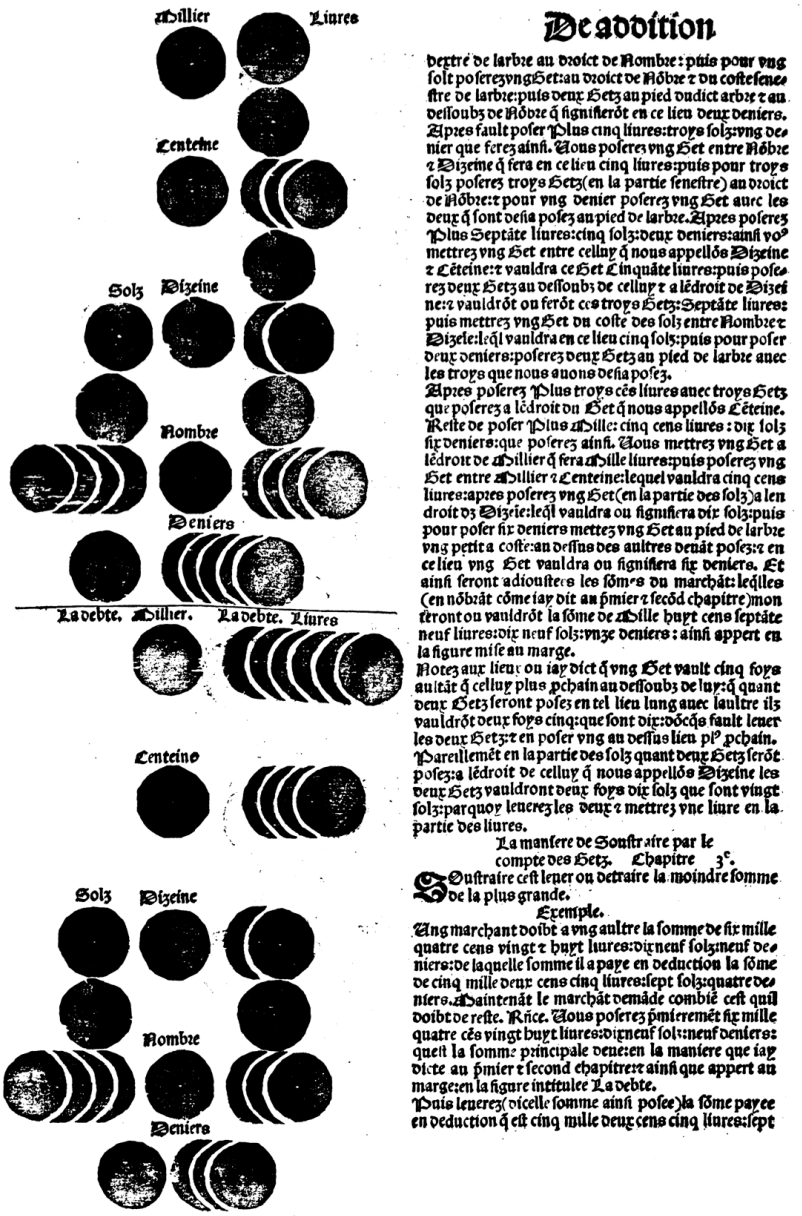
Par exemple, dans la figure 13, si l'abaciste pose 1 denier de plus, il arrivera à 12 ($6 + 5 \times 1 + \mathbf{1}$) deniers, donc à 2 (1+1) jetons dans l'espace rouge : il a alors en réalité 1 sou de plus. En cascade, il obtient 1 quinaire de plus (4**+1** sous), ce qui lui donne 2 quinaires (10 sous), et donc 2 (1+1) jetons dans l'espace vert, c'est-à-

[32] De nombreux autres livres sont imprimés à partir du 15e siècle. Nous ne discutons pas ici cette abondante littérature. Voir, par exemple, (Schärlig, 2022).

[33] L'utilisation de la quinaire permet de réduire largement le nombre de jetons à utiliser pour un calcul et donc gagner en visibilité.

dire 1 livre de plus ! C'est exactement la matérialisation des retenues dans nos algorithmes actuels : ainsi, les jetons permettent de manipuler le concept de retenue.

Nous considérons alors l'abaque à jetons comme un manipulatif[34], à savoir un matériel concret utilisé pour l'apprentissage de concepts mathématiques. Les deux opérations de réduction et de conversion sont grandement facilitées par la manipulation des jetons. Néanmoins, il est ensuite strictement nécessaire de verbaliser ce que sont, en termes arithmétiques, ces deux opérations, et ainsi amener les élèves vers les situations plus abstraites des algorithmes opératoires usuels.



De addition

dextre de larbre au droict de Nombre : puis pour vng solt poserez vng Get au droict de Nõbre et du coste senestre de larbre : puis deux Getz au pied dudict arbre et au dessoubz de Nõbre q̃ signifiera en ce lieu deux deniers. Apres fault poser Plus cinq liures : trois solz : vng denier que ferez ainsi. Vous poserez vng Get entre Nõbre et Dizeine q̃ fera en ce lieu cinq liures : puis pour trois solz poserez trois Getz (en la partie senestre) au droict de Nõbre : et pour vng denier poserez vng Get auec les deux q̃ sont desia posez au pied de larbre. Apres poserez Plus Septãte liures : cinq solz : deux deniers : ainsi vo⁹ mettrez vng Get entre celluy q̃ nous appellõs Dizeine et Cẽteine : et vaudra ce Get Cinquãte liures : puis poserez deux Getz au dessoubz de celluy et a ledroit de Dizeine : et vaudrõt ou ferõt ces trois Getz : Septãte liures : puis mettrez vng Get du coste des solz entre Nombre et Dizeine : lequel vaudra en ce lieu cinq solz : puis pour poser deux deniers : poserez deux Getz au pied de larbre auec les trois que nous auons desia posez.

Apres poserez Plus trois cẽs liures auec trois Getz que poserez a ledroit du Get q̃ nous appellõs Cẽteine. Reste de poser Plus Mille cinq cens liures : dix solz six deniers : que poserez ainsi. Vous mettrez vng Get a ledroit de Millier q̃ fera Mille liures : puis poserez vng Get entre Millier et Centeine : lequel vaudra cinq cens liures : apres poserez vng Get (en la partie des solz) a len droit dz Dizeie : lequel vaudra ou signifiera dix solz : puis pour poser six deniers mettez vng Get au pied de larbre vng petit a coste : au dessus des aultres deuãt posez : et en ce lieu vng Get vaudra ou signifiera six deniers. Et ainsi seront adioustees les sõmes du marchãt : lesquelles (en nõbrãt cõme iay dit au pmier et secõd chapitre) monteront ou vaudrõt la sõme de Mille huyt cens septãte neuf liures : dix neuf solz : vnze deniers : ainsi appert en la figure mise au marge.

Notez aux lieux ou iay dict q̃ vng Get vault cinq foys aultãt q̃ celluy plus pchain au dessoubz de luy : q̃ quant deux Getz seront posez en tel lieu lung auec laultre ilz vaudrõt deux foys cinq : que sont dix : dõcqs fault leuer les deux Getz : et en poser vng au dessus lieu pl⁹ pchain. Pareillemẽt en la partie des solz quant deux Getz serõt posez : a ledroit de celluy q̃ nous appellõs Dizeine les deux Getz vaudront deux foys dix solz que sont vingt solz : parquoy leuerez les deux et mettrez vne liure en la partie des liures.

La maniere de Soustraire par le compte des Getz. Chapitre 3e.

Soustraire cest leuer ou detraire la moindre somme de la plus grande.

Exemple.

Vng marchant doibt a vng aultre la somme de six mille quatre cens vingt et huyt liures : dix neuf solz : neuf deniers : de laquelle somme il a paye en deduction la sõme de cinq mille deux cens cinq liures : sept solz : quatre deniers. Maintenãt le marchãt demãde combiẽ cest quil doibt de reste. Rice. Vous poserez pmieremẽt six mille quatre cẽs vingt huyt liures : dix neuf sol⁹ neuf deniers : queſt la somme principale deue : en la maniere que iay dicte au pmier et second chapitre et ainsi que appert au marge : en la figure intitulee La debte.

Puis leuerez (de celle somme ainsi posee) la sõme payee en deduction q̃ est cinq mille deux cens cinq liures : sept

Figure 14 : « La manière de faire tous comptes par les getz », dans (Étienne de la Roche, 1538)

[34] Voir l'étude de Carbonneau, K. J., Marley S. C. et Selig J. P. (2013) sur l'effet de la manipulation à l'aide de « manipulatifs », notamment avec les mises en garde nécessaires pour que la manipulation soit efficace sur l'apprentissage.

IV - DE L'ÉGYPTE À *L'INITIATION MATHÉMATIQUE* DE CHARLES-ANGE LAISANT

1. Le Papyrus Rhind et la duplication

Dans l'Égypte du Moyen Empire[35] (à l'époque de la construction des pyramides), la multiplication est réalisée par les scribes à l'aide de la seule utilisation des doubles. Cette opération s'appelle la duplication[36]. Elle consiste en la décomposition d'un nombre en somme de puissances entières positives ou nulle de 2. Si tous les entiers admettent bien une telle décomposition, elle n'est pas nécessairement unique[37]. Si les scribes égyptiens manipulaient ce résultat, d'aucun ne l'avait ni énoncé comme propriété, ni démontré.

Dans le problème #32 du papyrus de Rhind[38], le scribe Ahmès doit déterminer la quantité qui, si on l'augmente de son tiers et de son quart, on obtient 2. Au cours de la résolution[39], le scribe est amené à effectuer le produit de 12 par 12 (figure 15).

18	.	12
19	2	24
20	\ 4	48
21	\ 8	96
22	*dmḏ*	144

Figure 15 : Problème #32 du papyrus Rhind faisant apparaître une multiplication (lignes 18 à 22) : texte (à gauche) et transcription (à droite) extraits de Imhausen (2003, 216).

[35] Pour une présentation complète des mathématiques égyptiennes, voir Michel (2014).

[36] Ce procédé est aussi utilisé pour la division (Ritter, 2000, p. 126). Par ailleurs, « dans la mesure où il convient assez bien au calcul sur abaque, il est attesté et enseigné jusqu'au 16e siècle de notre ère » (Caveing, 1994, p. 253).

[37] Voir (Caveing, 1994, pp. 253-258) pour le « 'théorème fondamental' de l'arithmétique égyptienne » : « Soit la série non-limitée des puissances croissantes de 2 : $2^0, 2^1, 2^2, \ldots, 2^k, \ldots$, tout entier naturel ou bien figure dans la liste des termes de cette série, ou bien est la somme de termes qui y figurent ».

[38] Le papyrus de Rhind tient son nom de son acheteur, l'avocat écossais Alexander Henry Rhind, en 1858. Il est aujourd'hui conservé au British Museum : https://www.britishmuseum.org/collection/object/Y_EA10058.

[39] Dans cet exemple, il n'est pas difficile de reconnaître les hiéroglyphes de l'opération (numération décimale additive : le bâton représente l'unité, l'anse la dizaine et la corde enroulée la centaine). D'après mon expérience personnelle, dès la première année du cycle 3, un élève peut comprendre les lignes 18 à 22, en expliquant que le signe transcrit par *dmḏ* peut signifier « somme » ou « total ».

Revenons sur les quatre premières lignes (tableau 2 ci-dessous).

.	12	On considère 12, un des deux facteurs du produit (souvent le plus grand des deux).
2	24	On double 12.
4	48	On double 24.
8	96	On double 48.

Tableau 2 : Explication des premières lignes du produit de 12 par 12

Il faut maintenant expliquer la cinquième ligne, appelée « somme » (tableau 3).

.	12	On considère 12, le nombre de départ.
2	24	On double 12, on obtient 24.
\ 4	48	On double 24, on obtient 48.
\ 8	96	On double 48, on obtient 96.
somme	144	On calcule 144 comme la somme de 48 et 96, en prenant la ligne du 4 et du 8 (marquées à l'aide de \)

Tableau 3 : Explication du produit de 12 par 12

Mathématiquement, Ahmès utilise la distributivité de la multiplication sur l'addition. Exprimée ici en termes modernes, on a :

$$12 \times 12 = (4 + 8) \times 12 = 4 \times 12 + 8 \times 12 = 48 + 96$$

Par ailleurs, en doublant systématiquement à chaque ligne, le scribe arrive à formuler une décomposition du multiplicande en somme de puissance de 2 (tableau 4).
Ainsi, $12 = 2^2 + 2^3 = 0 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3$. Et, 1 1 0 0 est alors l'écriture de 12 en base 2 (ou en notation binaire).

1	2^0
2	2^1
4	2^2
8	2^3
16	2^4
…	$2^{\cdots}$

Tableau 4 : Premières puissances de 2

Le procédé utilisé par le scribe égyptien pour multiplier deux nombres peut être résumé ainsi : il s'agit de décomposer l'un des deux nombres (souvent le plus petit, le multiplicande) comme une somme de puissances de deux[40], doubler l'autre nombre (le multiplicateur) en fonction de la puissance de 2 correspondante, et utiliser ensuite implicitement la distributivité pour calculer une somme. Aussi, les

[40] D'autres exemples existent où la décomposition est réalisée à l'aide d'un autre nombre que 2 (ou ses puissances) – comme 10, par exemple – mais ils ne sont pas nécessairement génériques mais plutôt adaptés aux problèmes proposés. Voir des exemples dans Imhausen (2016, 86-88).

égyptiens n'avaient besoin de connaître que la table de multiplication par 2 ; toutes les autres sont inutiles (tableau 5). L'intérêt historique rejoint ici l'intérêt pédagogique[41], à savoir, « son double caractère de généralité et de relative simplicité comparativement à l'acquisition laborieuse par la mémoire de la table de multiplication nécessaire au système décimal » (Caveing, 1994, p. 253).

\ .	3	On considère 3, le nombre de départ.
2	6	On double 3, on obtient 6.
\ 4	12	On double 6, on obtient 12.
somme	15	5 = 1+4, donc $3 \times 5 = 3 + 12 = 15$

Tableau 5 : Calcul du produit de 3 par 5 dans le problème #25 du papyrus Rhind

Pour des produits avec de petits facteurs, l'algorithme peut paraître plus long que l'utilisation des tables de multiplication. Néanmoins, dès que les facteurs sont plus importants (comme, par exemple, dans le tableau 6), le procédé est vite efficace.

\ .	63	On considère 63.
\ 2	126	On double 63.
\ 4	252	On double 126.
\ 8	504	On double 252.
\ 16	1 008	On double 504.
\ 32	2 016	On double 1 008.
somme	3 717	59 = 1+2+8+16+32, donc $59 \times 63 = 63 + 126 + 504 + 1\,008 + 2\,016 = 3\,717$

Tableau 6 : Calcul du produit de 59 par 63

En outre, ce procédé est aussi utilisé pour les produits d'un entier par une fraction[42], ou d'une fraction par une fraction comme le montrent, par exemple, les problèmes #27 et #70 du papyrus Rhind. Le scribe utilise des produits par des fractions élémentaires comme $\frac{1}{2}$ ou $\frac{2}{3}$ (voir la cinquième ligne du tableau 7, à droite) soit parce qu'il les connaît par cœur, soit parce qu'il utilise des calculs intermédiaires.

\ .	$3 + \frac{1}{2}$
2	7

.	$7 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8}$
2	$15 + \frac{1}{2} + \frac{1}{4}$
\ 4	$31 + \frac{1}{2}$

[41] J'y ajoute aussi l'intérêt scientifique. Aujourd'hui, les informaticiens tirent encore profit de cette méthode notamment, dans le cadre de l'exponentiation rapide (algorithme de calcul de grandes puissances entières utilisé, entre autres, en cryptographie).

[42] En Égypte, les fractions sont systématiquement exprimées comme sommes de fractions de numérateurs égaux à 1 (à l'exception de la fraction $\frac{2}{3}$ qui a sa propre représentation). Dans (Moyon, 2023), je reviens sur les fractions dites égyptiennes dans l'enseignement des mathématiques et leur traitement dans les manuels scolaires.

\ 4	14
somme	$17+\frac{1}{2}$

\ 8	63
$\backslash \frac{2}{3}$	$5+\frac{1}{4}$
somme	$99+\frac{1}{2}+\frac{1}{4}$

Tableau 7 : (à gauche) $5\times\left(3+\frac{1}{2}\right)$ *dans le problème #27; (à droite)* $\left(12+\frac{2}{3}\right)\times\left(7+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}\right)$*, dans le problème #70*

2. Une récréation mathématique : C.-A. Laisant et É. Lucas

En prolongement de la découverte du procédé de duplication chez les Égyptiens, il est utile et plaisant de développer des activités autour de la numération binaire[43] – c'est-à-dire en base 2 – écrite à l'aide des deux signes 0 et 1.
On a remarqué plus haut que 1 1 0 0 est l'écriture de 12 en base 2 puisque

$$12 = 2^2 + 2^3 = 0\times 2^0 + 0\times 2^1 + 1\times 2^2 + 1\times 2^3.$$

Aussi, l'écriture binaire de 59 est 1 1 1 0 1 1.

$$59 = 1\times 2^0 + 1\times 2^1 + 0\times 2^2 + 1\times 2^3 + 1\times 2^4 + 1\times 2^5.$$

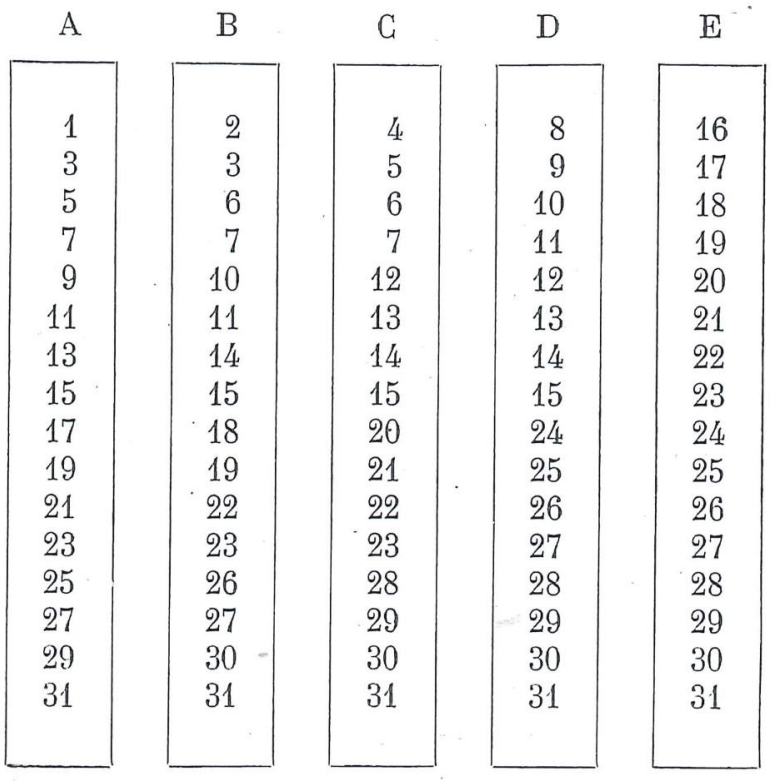
Intéressante, la numération binaire a été utilisée par de nombreux mathématiciens, en particulier à la suite de Gottfried Wilhelm Leibniz (m. 1716) et de son *De Progressione Dyadica*[44] *(manuscrit daté* de 1679*), notamment pour développer des curiosités ou récréations mathématiques, voire des tours de magie*. L'intérêt des récréations mathématiques pour l'enseignement n'est plus à démontrer, notamment par l'amusement qu'elles développent chez les apprenants ou la manipulation que certaines nécessitent (Rougetet, 2023, pp. 111-120). Nous choisissons ici de présenter un « petit jeu » emprunté au mathématicien et polytechnicien Charles-Ange Laisant (m. 1920) : « on a imaginé un petit jeu de salon qui repose sur l'emploi de la numération binaire, et dont Éd. Lucas a reproduit la description dans son Arithmétique amusante sous le nom d'Éventail mystérieux » (Laisant, 1915, p. 106). Lisons Édouard Lucas (m. 1891) détailler la règle de de jeu[45] :

> *L'éventail mystérieux se compose de cartons disposés en éventail sur lesquels on inscrit des nombres […] d'une certaine manière ; il s'agit, en présentant l'éventail, de deviner le nombre […] pensé par une personne. (Lucas, 1895, pp. 168-169)*

[43] Cette partie est largement développée dans Moyon (2024) où je présente davantage les deux mathématiciens Charles-Ange Laisant et Édouard Lucas, leur correspondance et leur idéal pédagogique.

[44] Serra (2017) offre une étude détaillée du manuscrit de Leibniz.

[45] *L'Arithmétique amusante* signée de Lucas est en réalité éditée à titre posthume en 1895 par Laisant, Henri Delannoy (m. 1915) et Émile Lemoine (m. 1912), à partir de trois cahiers préparés de son vivant à partir de 1888.



A	B	C	D	E
1	2	4	8	16
3	3	5	9	17
5	6	6	10	18
7	7	7	11	19
9	10	12	12	20
11	11	13	13	21
13	14	14	14	22
15	15	15	15	23
17	18	20	24	24
19	19	21	25	25
21	22	22	26	26
23	23	23	27	27
25	26	28	28	28
27	27	29	29	29
29	30	30	30	30
31	31	31	31	31

Figure 16 : Les cartons de l'éventail mystérieux dans (Laisant, 1915, 107).

Si l'on suit *L'Arithmétique amusante*, il nous reste (1) à deviner un nombre pensé par un joueur et (2) à comprendre la manière d'inscrire les nombres dans les cartons.

(1) Prenons un exemple : le nombre 27. Si l'on sait dans quelle(s) colonne(s) il apparaît (et il suffit de le demander au joueur qui a pensé ledit nombre), il est aisé de le retrouver. En effet, ici, 27 apparaît dans les colonnes A, B, D et E : il suffit « de faire la somme des nombres écrits en tête de chacun des cartons où le nombre se trouve » (Lucas, 1895, p. 169). Ainsi, additionnons 1, 2, 8 et 16, la somme est 27 ; c'est bien le nombre pensé.

(2) Sont inscrits sur les cinq cartons de la figure 16 tous les nombres de 1 à 31 en fonction de leur écriture binaire (ou de leur décomposition en somme de puissances de 2). Prenons, à nouveau l'exemple du nombre 27, comme $27 = 1 \times 2^0 + 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 + 1 \times 2^4$, il s'écrit : 1 1 0 1 1 en notation binaire et il apparaît alors dans les première (A), deuxième (B), quatrième (D) et cinquième (E) colonnes (là où l'écriture binaire donne 1) et n'apparaît pas dans la troisième colonne (C) (là où l'écriture binaire donne 0).
Prenons maintenant le nombre 23 :

$$23 = 1 \times 2^0 + 1 \times 2^1 + 1 \times 2^3 + 0 \times 2^3 + 1 \times 2^4$$

Donc l'écriture binaire de 23 est 1 0 1 1 1 : il est dans les colonnes A, B, C et E.

Jouer à l'éventail mystérieux peut être une belle occasion de faire vivre l'arithmétique en classe comme avec d'autres jeux arithmétiques : certains tours de magie et autres casse-têtes, comme, par exemple, les tours de Hanoï ou le baguenaudier (Rougetet, 2023). Mais, Laisant propose aussi de « pousser ce jeu jusqu'à 63 au lieu de 31, avec 6 cartons au lieu de 5, et jusqu'à 127 avec 7 cartons. » (Laisant, 1915, p. 110)

L'idée est ambitieuse mais intéressante car cela amène les élèves à penser le code binaire, si important dans toutes les technologies du numérique (Annexe 1).

V - CONCLUSION

En conclusion, notre promenade historique à travers le patrimoine arithmétique n'a pas eu d'autres objectifs que de donner à voir les mathématiques telles qu'elles ont été pratiquées et/ou écrites par leurs concepteurs ou utilisateurs (qu'ils soient ou non mathématiciens professionnels), avec des scribes égyptiens, des néo-pythagoriciens, des comptables médiévaux, des abacistes, des combinatoriciens ou autres récréateurs, plongés en leurs temps.

Ainsi, globalement, à partir de l'observation d'un matériel historique (textes, images ou artefacts) et de son analyse historico-mathématique, il s'est agi de favoriser la construction d'une autre représentation des mathématiques pour les enseignants et pour leurs élèves. Lorsqu'on enseigne les mathématiques, il est évident que l'objectif commun est bien d'améliorer l'enseignement/apprentissage des élèves, considérant alors l'histoire des mathématiques comme un outil pour non seulement promouvoir les mathématiques, mais aussi pour construire les connaissances mathématiques (Furinghetti, 2020).

Au cours de cette promenade, nous avons plusieurs fois mentionné les récréations mathématiques dont l'importance est réelle dans l'histoire de la discipline (Chemla, 2014) et pour son enseignement. Aussi, nous terminons cette contribution en faisant nôtre le projet pédagogique de Laisant, amplement illustré dans son *Initiation mathématique* (1915) : s'instruire en s'amusant, s'aider d'exemples concrets pour amener peu à peu l'esprit à l'intelligence de l'abstrait et solliciter l'initiative (plutôt que la mémoire) à l'aide d'exercices qui soient l'occasion de créer (Moyon, 2023). L'introduction d'une perspective historique paraît alors trouver une place naturelle dans l'enseignement des mathématiques en général, et dans celui de l'arithmétique en particulier.

VI - BIBLIOGRAPHIE

Barbin, É. (2022). On the role and scope of historical knowledge in using the history of mathematics in education. *ZDM – Mathematics Education 7* (54), 1597-1611.

Bourlet, C. (1911). Mathématiques. In F. Buisson (dir.) *Nouveau dictionnaire de pédagogie et d'instruction primaire* (p. 1259). Paris, France : Hachette et cie.

Bouvier A., George M. et Le Lionnais F. (1993). *Dictionnaire des mathématiques*. Paris : Presses universitaires de France.

Busser, É., Hauchecorne, B. (2021). *Dictionnaire décalé des mathématiques*. Paris, France : Ellipses.

Carbonneau, K. J., Marley S. C. et Selig J. P. (2013). A meta-analysis of the efficacy of teaching mathematics with concrete manipulatives. *Journal of Educational Psychology* 2(105), 380-400.

Caveing M. (1994). *Essai sur le savoir mathématique dans la Mésopotamie et l'Égypte anciennes*, Villeneuve d'ascq, France : Presses Universitaires de Lille.

Chambon G. (2020), *Histoire des nombres*, Paris, France : Que sais-je ?

Chemla, K. (2014). Explorations in the history of mathematical recreations: An introduction. *Historia Mathematica 4*(41), 367-376.

Chorlay, R., Clark, K. M. et Tzanakis C. (2022). History of mathematics in mathematics education: Recent developments in the field. *ZDM – Mathematics Education 7*(54), 1407-1420.

Daval, N. et Tournès, D. (2018). De l'abaque à jetons au calcul posé. *In* Moyon M. et Tournès, D. (dir.). *Passerelles : enseigner les mathématiques par leur histoire au cycle 3* (pp. 39-64). Bouc-Bel-Air, France : ARPEME.

Deledicq, A. et Launay, M. (2021). *Dictionnaire amoureux des mathématiques*. Paris, France : Plon.

Diophante d'Alexandrie (1621). Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Bachet de Méziriac, C.G. (éd.). Paris, France : Hieronymi Drouart.

Diophante d'Alexandrie (1893-95). Diophanti Alexandrini opera omnia cum graeciis commentariis. Tannery, P. (éd.). 2 vol. Leipzig : B.G. Teubner,.

Diophante d'Alexandrie (1959). *Les six livres arithmétiques et le livre des nombres polygones*, Ver Eecke, P (trad.) Paris, France : A. Blanchard.

Diophante d'Alexandrie (2011). *De polygonis numeris*, Acerbi, F. (édit., trad.). Pise, Italie : Fabrizio Serra Editore.

Djebbar, A. (2000). Figurate Numbers in the mathematical tradition of al-Andalus and the Maghrib, *Suhayl 1*, 57-70.

Djebbar, A. (2004), Du nombre pensé à la pensée des nombres : quelques aspects de la pratique arithmétique arabe et de ses prolongements en Andalus et au Maghreb, *Sciences et Techniques en Perspective 1*(8), 303-322.

Djebbar, A. (2022). Ibn Khaldūn et les mathématiques, à la lumière des recherches des dernières décennies. *In* Hedfi, H. et Abdeljaouad, M. (dir.), *Actes du 14e colloque Maghrébin sur l'Histoire des Mathématiques Arabes* (pp. 1-31). Tunis : Publication de l'association tunisienne des sciences mathématiques.

Étienne de la Roche, (1538). *L'arismetique & Geometrie […]*, Lyon, France : Gilles & Jaques Huguetan.

Fauvel, J. et Van Maanen, J. (2000). *History in mathematics education : the ICMI study*, Dordrecht, Pays-Bas : Kluwer.

Fourrey, É. (1901). *Récréations arithmétiques* (2e édition). Paris, France : Nony.

Freudenthal, G. et Lévy, T. (2004). De Gérase à Bagdad : Ibn Bahrīz, al-Kindī, et leur recension arabe de l'Introduction arithmétique de Nicomaque, d'après la version hébraïque de Qalonymos ben Qalonymos d'Arles. *In* Morelon, R. et Hasnawi, A. (dir.), *De Zénon d'Elée à Poincaré : recueil d'études en hommage à Roshdi Rashed* (pp. 479-544). Louvain, Belgique – Paris, France : Peeters.

Fried, M. (2007). Didactics and History of Mathematics : Knowledge and Self-Knowledge, *Educational Studies in Mathematics, 2*(66), 203-223.

Furinghetti, F. (2020). Rethinking history and epistemology in mathematics education. *International Journal of Mathematical Education in Science and Technology 6* (51), 967-994.

Guillemette D. (2011). L'histoire dans l'enseignement des mathématiques : sur la méthodologie de recherche, *Petit x 86*, 5-26.

Hofstetter, C. (2021). D'Ammonius à Qalonymos : la transmission d'un enseignement néoplatonicien sur Nicomaque. *Revue de philologie, de littérature et d'histoire anciennes 1*(XCV), 29-55.

Imhausen, A. (2003). *Ägyptische Algorithmen : eine Untersuchung zu den mittelägyptischen mathematischen Aufgabentexten*. Wiesbaden, Allemagne : Harrassowitz Verlag.

Imhausen, A. (2016). *Mathematics in Ancient Egypt : a contextual history*, Princeton, États-Unis, Princeton University Press.

Jankvist U. T. (2009a). A categorization of the "whys" and "hows" of using history in mathematics education, *Educational Studies in Mathematics 3*(71), 235-261.

Jankvist, U. T. (2009b). *Using history as a « goal » in mathematics education*, [Thèse de doctorat, Roskilde University]. http://thiele.ruc.dk/imfufatekster/pdf/464.pdf.

Laisant. C.-A. (1915). *Initiation mathématique : ouvrage étranger à tout programme, dédié aux amis de l'enfance*. Paris, France : Hachette & Cie.

Lucas, É. (1895). *L'arithmétique amusante*, Paris, France : Gauthier-Villars et fils.

Michel, M. (2014). *Les mathématiques de l'Égypte ancienne : numération, métrologie, arithmétique, géométrie et autres problèmes*. Bruxelles, Belgique : Éditions Safran.

Moyon, M. (2012). Penser les mathématiques à travers leur épistémologie et leur histoire : un enjeu de/dans la formation des maîtres. In J.-L. Dorier & S. Coutat (Eds) *Enseignement des mathématiques et contrat social : enjeux et défis pour le 21e siècle - Actes du colloque EMF2012* (pp. 641-652). Genève, Suisse : Université de Genève.

Moyon, M. (2023), Fractions égyptiennes et algorithme de Fibonacci : histoire des mathématiques versus manuels scolaires contemporains. *ACERVO - Boletim do Centro de Documentação do GHEMAT-SP 5*, 2023, 1-36.

Moyon, M. (2023). S'initier à "la mathématique" avec Charles-Ange Laisant : manipuler, visualiser, s'étonner, *Bulletin de la société des amis du musée, de la bibliothèque et de l'histoire de l'école polytechnique* 70, 131-143.

Moyon, M. (2024). Binary Numeration: From Ancient Egypt to a 19th Century French Mathematical Recreation, *Revista de Matemática, Ensino e Cultura – REMATEC* 19(47), 1-20.

Moyon, M. (à paraître). Plume, jetons, papier et abaque : Compter et calculer au Moyen Âge. *In* Boisseuil, D. et Dumasy, J. (éds), *Formes et enjeux des comptabilités urbaines médiévales : l'exemple ligérien*. Rennes : Presses universitaires de Rennes.

Nicomaque de Gérase (1978). *Introduction arithmétique*, Bertier, J. (trad.). Paris, France : Vrin.

Ritter, J. (2008). Egyptian Mathematics. *In* Selin, H. (dir.), *Encyclopaedia of the History of Science, Technology, and Medicine in Non-Western Cultures* (pp. 1378-1381). Berlin, Heidelberg, New York : Springer.

Rashed, R. (1983). Nombres amiables, parties aliquotes et nombres figurés aux XIII^{ème} et XIV^{ème} siècles. *Archive for History of Exact Sciences* 2(28), 107-147.

Rougetet, L. (2023). *Le binaire au bout des doigts : Un casse-tête entre récréation mathématique et enseignement*. Les Ullis, France : EDP sciences.

Saidan, A. S. (1997). Numération et arithmétique. *In* Roshdi, R. (dir.), *Histoire des sciences arabes : Mathématiques et Physique* (pp. 11-29). Paris, France : Éditions du Seuil.

Serra, Y. (2010). Le manuscrit « De Progressione Dyadica » de Leibniz, *Bibnum. Textes fondateurs de la science*.

Schärlig A. (2022). *Calculer avec des jetons : avant les chiffres arabes*, Lausanne, Suisse : Presses polythechniques et universitaires romandes.

Schwer, S. R. (2018). Les rapports de nombres. *In* Moyon, M. et Tournès, D. (dir.), *Passerelles : enseigner les mathématiques par leur histoire au cycle 3* (pp. 92-120). Bouc-Bel-Air, France : ARPEME.

VII - ANNEXE : L'ÉVENTAIL MYSTÉRIEUX AVEC 6 CARTONS

Inspiré de la proposition de Laisant (1915, 110), voici l'extension de l'éventail mystérieux proposé par Lucas (1895) et Laisant (1915) avec six cartons (de 1 à 63) à la place de cinq (de 1 à 31), eux-mêmes présentés à la figure 16.

1	2	4	8	16	32
3	3	5	9	17	33
5	6	6	10	18	34
7	7	7	11	19	35
9	10	12	12	20	36
11	11	13	13	21	37
13	14	14	14	22	38
15	15	15	15	23	39
17	18	20	24	24	40
19	19	21	25	25	41
21	22	22	26	26	42
23	23	23	27	27	43
25	26	28	26	28	44
27	27	29	29	29	45
29	30	30	30	30	46
31	31	31	31	31	47
33	34	36	40	48	48
35	35	37	41	49	49
37	38	38	42	50	50
39	39	39	43	51	51
41	42	44	44	52	52
43	43	45	45	53	53
45	46	46	46	54	54
47	47	47	47	55	55
49	50	52	56	56	56
51	51	53	57	57	57
53	54	54	58	58	58
55	55	55	59	59	59
57	58	60	60	60	60
59	59	61	61	61	61
61	62	62	62	62	62
63	63	63	63	63	63

Ateliers

L'ARITHMÉTIQUE, C'EST TOUTE UNE HISTOIRE !

Frédéric LAURENT
Formateur, INSPE, UNIVERSITE CLERMONT AUVERGNE
& IREM DE CLERMONT-FERRAND
Frederic.Laurent@uca.fr

Résumé
C'est durant l'Antiquité que les mathématiciens grecs distinguent l'arithmétique de la logistique, l'art du calcul. L'arithmétique est, quant à elle, consacrée aux propriétés des nombres entiers qui, comme le rapporte Aristote, sont « les causes et les principes des choses » selon l'école pythagoricienne, fondatrice de cette science. Dans ses *Éléments*, vers 300 avant J.-C., Euclide y consacre trois de ses livres (les livres VII, VIII et IX) : on y trouve de nombreuses propriétés encore enseignées aujourd'hui au collège ou au lycée, autour des notions de divisibilité, de PGCD, de nombres premiers, etc.
Le but de cet atelier n'est pas de retracer la longue histoire de l'arithmétique, mais plutôt de s'arrêter sur quelques moments de cette histoire par le biais de l'étude de textes historiques. Si lire Euclide semble incontournable, les lectures ne seront pas limitées aux *Éléments*. Au contraire, elles mettront en évidence quelques contributions intéressantes, et peut-être moins connues, de mathématiciens qui ont œuvré durant la période qui sépare les *Éléments* des *Recherches arithmétiques* de C. F. Gauss (au début du XIXe s.). Sans aucun caractère visant à l'exhaustivité, le corpus de textes choisis a été élaboré autour de la justification de critères de divisibilité moins communs que les critères de divisibilité par 2, 3, 4, 5 ou 9. Il pourra constituer une source d'inspiration pour construire des activités pour la classe, du collège au lycée, basées sur l'étude de sources primaires.

I - QUESTIONS LIMINAIRES

L'apprentissage des critères de divisibilité, dans notre système décimal positionnel d'écriture des nombres entiers naturels, débute dès le cycle 3. En effet, dans les repères de progressivité datés de 2019, il est stipulé que l'étude des critères de divisibilité par 3 et 9 doit commencer au plus tard lors de la période 4 du CM2. De plus, dans le programme officiel du cycle 3[1], il est indiqué que les élèves doivent connaître les critères de divisibilité par 2, 3, 5, 9 et 10 (le critère de divisibilité par 4, non explicitement au programme, est parfois enseigné). Tous ces critères sont entretenus tout au long du cycle 4 dans le but d'être disponibles, notamment pour la simplification des fractions et la réduction sous forme irréductible de ces dernières (qui constitue un attendu de la classe de 3e)[2]. L'enseignant, comme l'élève, peut légitimement se demander s'il existe des critères de divisibilité par 6 ou par 7 vu qu'il en existe pour d'autres entiers à un chiffre. Une autre question concerne les entiers à plus de deux chiffres : s'il on dispose facilement d'un critère de divisibilité par 10, comment est-il possible de reconnaître un entier divisible par 11 ou par 12 par exemple ?

[1] Programme en vigueur à la rentrée 2023, d'après le BOEN n°31 du 30 juillet 2020 et le BOEN n°25 du 22 juin 2023.

[2] Dans le programme du cycle 4 en vigueur à la rentrée 2020, d'après le BOEN n°31 du 30 juillet 2020, on peut lire « fractions irréductibles » dans la liste des connaissances en arithmétique. Parmi les compétences associées dans ce domaine, il est stipulé : « utiliser les critères de divisibilité par 2, 3, 5, 9 et 10 » et « simplifier une fraction pour la rendre irréductible ».

Ces questions peuvent constituer une première motivation autour de l'invention de critères et de leur preuve.

À titre d'exercice, chacun pourra chercher à compléter le tableau suivant dans lequel il faut statuer, pour chaque entier donné, s'il est divisible par 6, 12 ou 7. Seul le calcul mental est autorisé, comme pour tout critère de divisibilité qui se respecte !

	Divisible par 6	Divisible par 12	Divisible par 7
69814			
341898			
553924			
6515796			

Une méthode attendue possible (si on soumet l'exercice précédent à une classe) pour reconnaître un nombre divisible par 6 est de vérifier qu'il est divisible par 2 et par 3. Par exemple, 341898 est divisible par 6 car il est pair et divisible par 3 puisque la somme de ses chiffres vaut 33 qui est lui-même un multiple de 3. De la même façon, un nombre est divisible par 12 s'il est divisible par 3 et par 4. La propriété sous-jacente à ces critères est la suivante : « pour tous entiers naturels a, b et c, si a et b sont premiers entre eux et divisent c alors leur produit ab divise c ». Nous noterons (P) cette propriété par la suite. Auprès des élèves, il est important de souligner l'importance de l'hypothèse « a et b sont premiers entre eux » : si on la supprime, la propriété devient fausse et on pourra donner comme contre-exemple 12 qui est divisible par 2 et par 4 mais qui n'est pas divisible par 8.

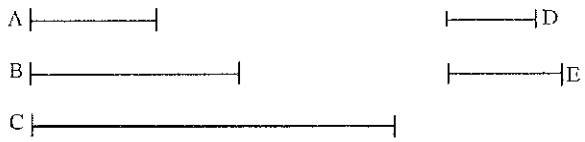
Pour ce qui est de la reconnaissance de la divisibilité par 7, une idée pourrait être d'effectuer mentalement la division euclidienne de l'entier par 7 et de voir si le reste est nul. Prenons le nombre 553924 et appliquons-lui l'algorithme de division usuel. Le reste de la division euclidienne de 55 par 7 est 6 ; on abaisse le 3, on obtient 63 qui est divisible par 7, il reste donc 0 ; on abaisse le 9, il reste 2 ; on abaisse le 2, le reste de la division de 22 par 7 est 1 ; on abaisse le 4 et on obtient 14 dont le reste est nul dans la division euclidienne par 7. Ainsi, 553924 est divisible par 7. Le procédé fonctionne bien, mais ne correspond pas tout à fait à ce que l'on entend par « critère de divisibilité ». En effet, une telle méthode ne contient ni une « astuce sur les chiffres », ni une spécificité liée au diviseur. Son caractère général permet en théorie de l'utiliser pour tout autre nombre choisi comme diviseur, à la seule condition d'être suffisamment solide en calcul mental pour effectuer les divisions euclidiennes successives sans les poser ! Par exemple, on peut procéder par divisions euclidiennes successives pour savoir si un entier est divisible par 3 (au lieu de faire la somme des chiffres) ou par 6 (au lieu de tester la divisibilité par 2 et par 3).

Le premier objectif des différentes lectures qui vont suivre est de savoir si la propriété (P) pourrait avoir sa place dans les ouvrages anciens d'arithmétique et, si oui, de quelle façon ? Sur quelles bases axiomatiques pourrait-elle être établie ? Le second objectif est de montrer que des méthodes ingénieuses pour tester la divisibilité par 7 sont attestées dans l'histoire.

II - TEXTE 1 : UN EXTRAIT DES *ÉLÉMENTS* D'EUCLIDE

Le premier texte qui a retenu notre attention conformément aux objectifs précédemment fixés est la proposition 30 du livre VII des *Éléments* d'Euclide (vers 300 av. J.-C.). Nous la donnons en figure 1 dans la traduction de Bernard Vitrac.

Si deux nombres se multipliant l'un l'autre produisent un certain [nombre] et si un certain nombre premier mesure leur produit, il mesurera aussi l'un des nombres initiaux.



En effet, que deux nombres A, B, se multipliant l'un l'autre produisent C, et qu'un certain nombre premier D mesure C. Je dis que D mesure l'un des [nombres] A, B.

En effet, qu'il ne mesure pas A. Et D est premier; donc A, D sont premiers entre eux (VII. 29). Et qu'autant de fois que D mesure C, autant il y ait d'unités dans E. Or puisque D mesure C selon les unités dans E, le [nombre] D multipliant E a donc produit C. Mais A multipliant B a aussi produit C; donc le produit des D, E est égal au produit des A, B. Donc comme D est à A ainsi [est] B à E (VII. 19). Mais D, A sont premiers entre eux, et les premiers sont les plus petits (VII. 21), et les plus petits mesurent ceux qui ont le même rapport qu'eux autant de fois, le plus grand le plus grand, et le plus petit le plus petit (VII. 20), c'est-à-dire l'antécédent, l'antécédent, et le conséquent, le conséquent. Donc D mesure B.

Alors semblablement nous démontrerons que s'il ne mesure pas B, il mesurera A. Donc D mesure l'un des [nombres] A, B. Ce qu'il fallait démontrer.

Figure 1. Proposition VII-30 des Éléments d'Euclide (Euclide, 1991, p. 338)

Dans cette proposition, que l'on nomme souvent « lemme d'Euclide » en arithmétique, ce dernier établit le fait que si un nombre premier divise le produit de deux nombres entiers naturels alors il divise l'un d'eux. Euclide n'emploie pas le verbe « diviser » mais « mesurer ». De la même façon qu'une ligne peut en mesurer une autre en géométrie, c'est-à-dire que la seconde peut contenir exactement un nombre entier de fois la première par juxtaposition, un nombre entier peut en « mesurer » un autre. Ce verbe issu du vocabulaire géométrique rappelle, tout comme la représentation grecque des nombres par des segments (cf. figure 1), le projet pythagoricien de trouver dans le nombre entier l'explication de toutes les choses. Mais la découverte de l'incommensurabilité de la diagonale d'un carré avec le côté de ce dernier (on peut

dire, de façon anachronique, l'irrationnalité de racine de 2) a conduit les mathématiciens grecs à séparer le numérique du géométrique.

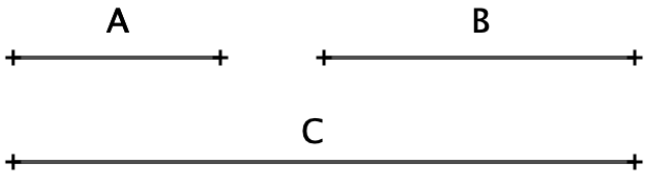
Ainsi, Euclide pose C le nombre obtenu en multipliant deux entiers A et B donnés et note D un diviseur premier de C dont il suppose qu'il ne divise pas A. Son objectif est de prouver, dans ce cas, que D divise B. La situation est parfaitement symétrique en échangeant les rôles de A et de B, ce qu'il signale à la fin de sa preuve. La phrase « autant de fois que D mesure C, autant il y ait d'unités dans E » exprime le fait que C s'obtient en « juxtaposant » un certain nombre de fois D et que si l'on juxtapose autant de fois l'unité, on obtient le nombre E. Autrement dit, de façon moderne, C est égal à E fois D, ce qu'Euclide traduit en disant que « D multipliant E a donc produit C ». Il parvient ainsi à deux expressions possibles de C : comme produit de A par B et comme produit de C par E. C'est alors qu'interviennent plusieurs propositions établies précédemment dans le livre VII. L'égalité des produits est d'abord traduite en termes de rapports : « comme D est à A ainsi [est] B à E » signifie que le rapport entre les nombres D et A est le même qu'entre les nombres B et E (on écrirait aujourd'hui que $\frac{D}{A} = \frac{B}{E}$). De cette façon, il se ramène à la théorie des proportions dont il a jeté les bases dans les domaines géométrique (au livre VI) et numérique (au livre VII). Il procède en deux temps. D'abord, parmi les couples de nombres qui sont dans un même rapport, les nombres qui sont premiers entre eux sont les plus petits nombres (il s'agit de la proposition VII-21). Cette proposition peut s'appliquer aux nombres A et D qui sont premiers entre eux. En effet, Euclide a déjà établi au préalable que si un nombre premier (comme D) ne divise pas un autre nombre (comme A) alors ces deux nombres sont premiers entre eux. Ainsi, les nombres D et A sont les plus petits nombres de tous ceux qui ont le même rapport avec eux. Ensuite, il recourt à la proposition VII-20 : « les plus petits nombres parmi ceux qui ont le même rapport qu'eux mesurent ceux qui ont le même rapport autant de fois, le plus grand le plus grand et le plus petit le plus petit » (Euclide, 1991, p. 325). Dans notre situation, vu que les nombres B et E constituent un couple qui a le même rapport que les nombres D et A, qui sont les plus petits possibles, alors le nombre B contient autant de fois D que le nombre E contient A. En particulier D divise B, ce qu'il fallait démontrer !

Comme on le voit, Euclide base son édifice déductif sur une théorie des proportions très sophistiquée dont l'un des résultats essentiels rappelle cependant une propriété admise et bien connue de nos collégiens : si une fraction $\frac{a}{b}$ a pour représentant la fraction irréductible $\frac{p}{q}$ (autrement dit, avec p et q premiers entre eux) alors il existe un entier naturel n tel que $a = np$ et $b = nq$. Cela doit nous questionner quant à l'organisation de notre enseignement. En effet, le « lemme d'Euclide » y est en général établi à l'aide du théorème (ou lemme) de Gauss : pour tous entiers naturels a et b, si un entier d divise le produit de a et b et que d est premier avec a, alors d divise b. Le « lemme d'Euclide » apparaît comme un cas particulier du théorème de Gauss dans le cas où l'entier d est un nombre premier : s'il ne divise pas le facteur a, alors les entiers a et d sont premiers entre eux, ce qui permet l'utilisation du théorème de Gauss pour affirmer que d divise b. Cependant ce dernier théorème, dont la démonstration demande un bagage en arithmétique un peu plus conséquent, n'est abordé que dans les classes de mathématiques expertes de terminale générale.

Nous avons la même difficulté avec les critères de divisibilité par 6 ou 12 dont les énoncés paraissent très accessibles dès le collège mais dont la justification est basée sur la propriété générale (P) qui ne fait pas partie du corpus des connaissances exigibles au collège. Pourtant, sa preuve pourrait être envisagée avec les outils euclidiens des proportions. Autrement dit, elle pourrait reposer sur la caractérisation des fractions irréductibles vue précédemment. Pour le montrer, nous pourrions pour cela étudier la

démonstration de la proposition (P) par Euclide, or il se trouve que cette propriété ne fait pas partie de l'édifice des livres arithmétiques des *Éléments* où elle aurait naturellement trouvé sa place. Nous allons donc réaliser un travail d'imitation et montrer comment Euclide aurait pu rédiger une démonstration en utilisant des outils similaires et en conservant au mieux son style.

Proposition. Si deux nombres sont premiers entre eux et mesurent un même nombre, leur produit mesurera aussi ce nombre.



En effet, que deux nombres premiers entre eux A et B mesurent un même nombre C. Je dis que le produit des A, B mesure C.

Que A mesure C autant de fois qu'il y a d'unités dans D et que B mesure C autant de fois qu'il y a d'unités dans E. Donc le produit des A, D est égal à C et le produit des B, E est égal à C. Mais les choses égales à une même chose sont aussi égales entre elles. Donc le produit des A, D est égal au produit des B, E. Ainsi A est à B comme E est à D. Mais A et B sont premiers entre eux, et les premiers sont les plus petits, et les plus petits mesurent ceux qui ont même rapport qu'eux autant de fois, le plus grand le plus grand, et le plus petit le plus petit. Donc A mesure E. Que A mesure E autant de fois qu'il y a d'unités dans F, donc le produit des A, F est égal à E. Donc le produit des A, B, F est égal à C. Donc le produit AB mesure C. Ce qu'il fallait démontrer.

Figure 2. Démonstration de la proposition (P) à la façon d'Euclide.

III - TEXTE 2 : UN EXTRAIT DE *L'ARITHMÉTIQUE* DE PIERRE FORCADEL

Le second texte que nous avons retenu dans notre corpus est un extrait de *L'arithmétique* de Pierre Forcadel (1500 – 1576 ou 1577). Outre cet ouvrage datant de 1556, ce biterrois est connu pour ses traductions d'Euclide (les six premiers livres des *Éléments*), de Proclus, d'Archimède, d'Oronce Fine, de Gemma Frisius… Nous présentons ce texte très légèrement adapté par nos soins pour le rendre plus facilement lisible :

> *Il est ainsi, qu'ayant considéré, que de chaque dizaine qui ôte 9, 1 se trouve pour restant, on s'est aperçu, que qui indifféremment ajoute toutes les figures d'un nombre et du nombre de l'addition ôte tous les 9 ; le nombre restant de la soustraction, ou de la continuelle soustraction, est le même restant du nombre divisé par 9. […] Par cela donc, quand nous voulons savoir si quelque nombre peut se diviser par 9 également, qui est, si de quelque nombre nous pouvons prendre la $\frac{1}{9}$ partie sans aucun restant, quand du nombre de l'addition des figures laissant tous les 9, il reste rien, qui est 0 ; alors ce nombre pourra se diviser par 9 et par 3 ; comme il est ainsi, que de 9 on peut prendre la tierce partie. […]*

> *À l'imitation donc de l'autre considération, je me suis avisé de la vraie façon de ce tiers présage, en cette sorte. Considérant que de 10 à 7 la différence est 3, toute dernière figure doit être multipliée par 3, ôtant les 7, et au reste ajoutant la figure précédente, jusqu'à ce qu'on ajoute la première figure du nombre. […} Et se doit noter, que de tel nombre comme 95, 2 la différence de 9 à 7, doit seulement être multiplié par 3 et de 89, 1 la différence de 8 à 7 doit être multiplié par 3 et au produit 2, la différence de 9 à 7, doit être ajoutée et ainsi des autres. Davantage il faut noter, que s'il reste 0, quand de tous les triples et additions les 7 sont ôtés, cela montre que tout le nombre peut justement être divisé par 7 ; ce qui n'a encore [jamais] été trouvé jusqu'ici. Et puis qu'ainsi est, que la première invention de cette façon est venue de moi… […] Il faut donc commencer à la dernière figure 4, qui par 3 fait 12 ; duquel reste 5, qui avec 2, fait 7, duquel reste rien ; puis 5 par 3, fait 15, duquel reste 1, qui avec 6, fait 7, duquel reste rien ; qui montre que 4956 être nombre lequel divisé par 7 reste 0. (Forcadel, 1556, p. 59-60)*

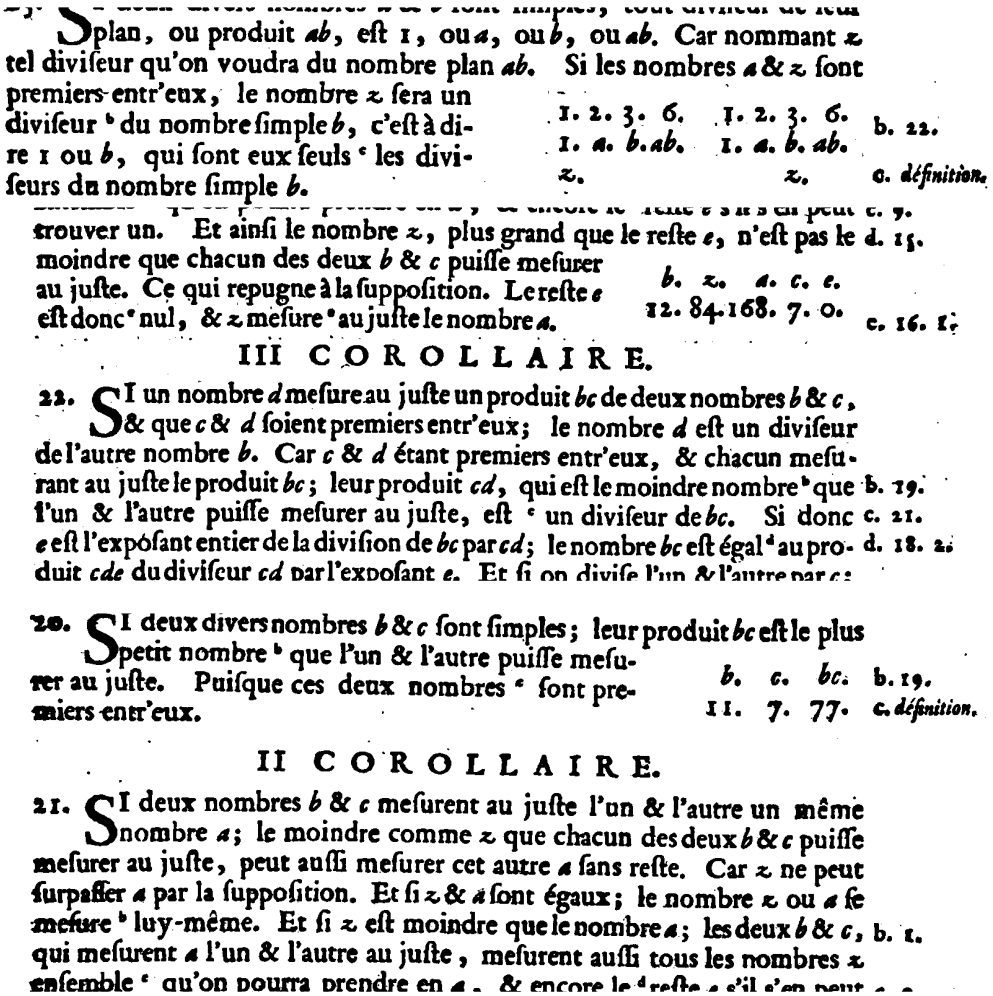
Dans ce texte nous reconnaissons d'abord le critère bien connu de divisibilité par 9 : « quand du nombre de l'addition des figures laissant tous les 9, il reste rien, qui est 0 ; alors ce nombre pourra se diviser par 9. » Forcadel parle de « l'addition des figures » là où nous dirions aujourd'hui « somme des chiffres ». Laisser tous les 9 consiste à enlever autant de fois le nombre 9 que possible, autrement dit, effectuer la division euclidienne par 9. Si ce reste est 0, alors le nombre donné est divisible par 9. De cette règle, il déduit de façon immédiate que si la somme des chiffres du nombre est un multiple de 9 alors non seulement le nombre est divisible par 9 mais aussi par 3, puisque 9 est lui-même divisible par 3.

La seconde partie du texte montre que Forcadel a trouvé une façon de tester si un nombre donné est divisible par 7, à l' « imitation » du procédé précédent. Forcadel précise même, de façon laconique, que cette règle trouve sa justification dans le fait que 3 est le complément à 10 de 7 (« de 10 à 7 la différence est 3 ») de la même façon que le critère de divisibilité par 9 trouve sa justification dans le fait que 1 est le complément à 10 de 9 (« ayant considéré, que de chaque dizaine qui ôte 9, 1 se trouve pour restant, on s'est aperçu que… »). La méthode décrite par Forcadel est de type algorithmique. Il faut commencer par la « dernière figure », ce qui correspond, pour nous, au premier chiffre dans l'écriture décimale du nombre. Pour comprendre la procédure, prenons un exemple, comme le fait Forcadel : le nombre 553924 auquel nous nous sommes intéressés plus haut. On commence par multiplier 5 par 3, ce qui donne 15, duquel on retire autant de fois 7 que possible, il reste 1. La règle consiste alors à ajouter le chiffre suivant à ce reste, puis d'en prendre le reste dans la division euclidienne par 7 : ici le chiffre suivant est 5, on ajoute donc 1 et 5, ce qui donne 6 et 6 étant inférieur à 7, c'est le reste cherché. À partir de là, on itère la procédure, à savoir multiplier par 3, ôter le plus grand multiple de 7 possible, ajouter le chiffre suivant, puis ôter à nouveau le plus grand multiple de 7 possible au résultat. On fait donc : 6 multiplié par 3 donne 18, il reste 4 que l'on ajoute au chiffre suivant 3, ce qui donne 7, il reste donc 0. On recommence pour le chiffre suivant qui est un 9. Mais comme 9 est supérieur à 7, Forcadel précise que, dans ce cas, il est inutile d'ajouter 9, mais il suffit d'ajouter 2 (une fois 7 retiré de 9). Le dernier reste vaut donc 2 que l'on multiplie par 3, soit 6 auquel on ajoute le chiffre suivant, ce qui donne 8, donc il reste 1. On multiplie par 3 et on ajoute le dernier chiffre 4, ce qui donne 7. Le dernier reste est donc 0 ce qui assure que 553924 est divisible par 7.

En réalité, le dernier reste obtenu dans cette procédure est le reste de la division euclidienne du nombre donné par 7. Nous verrons un peu plus loin une justification possible de ce résultat.

IV-TEXTE 3 : UN EXTRAIT DES *NOUVEAUX ÉLÉMENTS DE MATHÉMATIQUES* DE JEAN PRESTET

Défenseur de la méthode exposée par René Descartes dans son *Discours de la méthode* de 1637, Jean Prestet (1648 – 1690) s'est attaché à contribuer à l'élaboration de manuels destinés à renouveler l'enseignement selon les principes cartésiens. Pour lui, l'arithmétique et l'algèbre sont le fondement de toutes les sciences. Il publie un premier ouvrage intitulé *Les éléments des mathématiques* en 1675 puis une seconde version *Les nouveaux éléments des mathématiques*, en deux volumes, en 1695. C'est du premier volume de ce dernier ouvrage que nous tirons les textes présentés en figure 3. Il s'agit de trois corollaires (numérotés 20, 21 et 22) faisant suite au théorème 19.



plan, ou produit *ab*, eſt 1, ou *a*, ou *b*, ou *ab*. Car nommant *z* tel diviſeur qu'on voudra du nombre plan *ab*. Si les nombres *a* & *z* ſont premiers entr'eux, le nombre *z* ſera un diviſeur [b] du nombre ſimple *b*, c'eſt à dire 1 ou *b*, qui ſont eux ſeuls [c] les diviſeurs du nombre ſimple *b*.

1. 2. 3. 6. 1. 2. 3. 6. b. 22.
1. *a*. *b*. *ab*. 1. *a*. *b*. *ab*.
z. *z*. c. définition.

trouver un. Et ainſi le nombre *z*, plus grand que le reſte *e*, n'eſt pas le d. 15.
moindre que chacun des deux *b* & *c* puiſſe meſurer au juſte. Ce qui repugne à la ſuppoſition. Le reſte *e* eſt donc [e] nul, & *z* meſure [e] au juſte le nombre *a*.

b. *z*. *a*. *c*. *e*.
12. 84. 168. 7. 0. c. 16. 1.

III COROLLAIRE.

22. SI un nombre *d* meſure au juſte un produit *bc* de deux nombres *b* & *c*, & que *c* & *d* ſoient premiers entr'eux; le nombre *d* eſt un diviſeur de l'autre nombre *b*. Car *c* & *d* étant premiers entr'eux, & chacun meſurant au juſte le produit *bc*; leur produit *cd*, qui eſt le moindre nombre [b] que b. 19.
l'un & l'autre puiſſe meſurer au juſte, eſt [c] un diviſeur de *bc*. Si donc c. 21.
e eſt l'expoſant entier de la diviſion de *bc* par *cd*; le nombre *bc* eſt égal [d] au pro- d. 18. 2.
duit *cde* du diviſeur *cd* par l'expoſant *e*. Et ſi on diviſe l'un & l'autre par *c*;

20. SI deux divers nombres *b* & *c* ſont ſimples; leur produit *bc* eſt le plus petit nombre [b] que l'un & l'autre puiſſe meſurer au juſte. Puiſque ces deux nombres [c] ſont premiers entr'eux.

b. *c*. *bc*. b. 19.
11. 7. 77. c. définition.

II COROLLAIRE.

21. SI deux nombres *b* & *c* meſurent au juſte l'un & l'autre un même nombre *a*; le moindre comme *z* que chacun des deux *b* & *c* puiſſe meſurer au juſte, peut auſſi meſurer cet autre *a* ſans reſte. Car *z* ne peut ſurpaſſer *a* par la ſuppoſition. Et ſi *z* & *a* ſont égaux; le nombre *z* ou *a* ſe meſure [b] luy-même. Et ſi *z* eſt moindre que le nombre *a*; les deux *b* & *c*, b. 1.
qui meſurent *a* l'un & l'autre au juſte, meſurent auſſi tous les nombres *z* enſemble [c] qu'on pourra prendre en *a*. & encore le [d] reſte *e* s'il s'en peut

Figure 3. Trois corollaires tirés des Nouveaux éléments des mathématiques de Prestet (Prestet, 1695, p. 147)

Commençons par analyser le premier corollaire : « si deux nombres *b* et *c* sont simples, leur produit *bc* est le plus petit nombre que l'un et l'autre puisse mesurer au juste ». Reformulée de façon contemporaine, cette propriété s'énonce de la façon suivante : si deux nombres *b* et *c* sont premiers, leur produit *bc* est leur plus petit commun multiple. On remarque au passage que Prestet utilise l'expression « mesurer » dans la tradition grecque. La preuve de ce corollaire s'appuie essentiellement sur le théorème 19 (dont l'utilisation est d'ailleurs indiquée en marge de la preuve grâce à la lettre b en exposant dans le texte) dont il est possible de reconstituer l'énoncé. Ce théorème affirme que si deux nombres sont premiers entre eux alors

leur PPCM est leur produit. Son application est immédiate ici dans la mesure où les nombres *b* et *c* sont supposés premiers et que l'on sait que deux nombres premiers sont nécessairement premiers entre eux.

Le deuxième corollaire affirme que si deux nombres *b* et *c* divisent un même entier *a*, alors leur PPCM divise *a*. Dans le troisième, on reconnaît le théorème que l'on nomme aujourd'hui théorème (ou lemme) de Gauss : si un nombre *d* divise le produit de deux entiers *b* et *c* et que *d* est premier avec *c* alors *d* divise *b*. La démonstration de ce dernier résultat utilise encore le théorème 19, il ne sera pas difficile au lecteur de la comprendre. Ce théorème de Gauss (avant Gauss !) n'est pas présent dans les *Éléments* d'Euclide, c'est donc une propriété supplémentaire dans le corpus de résultats liés à la divisibilité et aux nombres premiers entre eux. Cependant, à l'instar des *Éléments* la propriété (P) que nous avons énoncée au début de cet article et qui nous intéresse particulièrement pour justifier le critère de divisibilité par 6, n'est pas non plus présente dans les *Nouveaux éléments de mathématiques* de Prestet.

Tout comme nous l'avons fait précédemment avec Euclide, nous pouvons énoncer et démontrer cette propriété (P) à la façon de Prestet : « si deux nombres *b* et *c* sont premiers entr'eux et mesurent au juste l'un et l'autre un même nombre *a*, leur produit *bc* peut aussi mesurer cet autre *a* (sans reste) ». Quant à la preuve, elle proviendrait, dans l'édifice axiomatico-déductif de Prestet, d'abord de l'application du théorème 19 : comme *b* et *c* sont supposés premiers entre eux, alors leur produit *bc* est leur PPCM. Or le deuxième corollaire affirme que si *b* et *c* mesurent au juste l'un et l'autre un même nombre *a*, leur PPCM divise aussi le nombre *a*. Comme ce PPCM est le produit *bc*, on conclut que *bc* divise *a*.

V - TEXTE 4 : UN EXTRAIT DES *RECHERCHES ARITHMÉTIQUES* DE CARL FRIEDRICH GAUSS

Les *Recherches arithmétiques* de Gauss (1777 – 1855) ont été composées en latin (*Disquisitiones arithmeticae*) et publiées en 1801 alors que Gauss n'avait que 24 ans. Mais c'est d'une version en français (traduite par A. C. M. Poullet-Delisle) et éditée en 1807 que nous tirerons les extraits suivants. Dans la première section de ce texte, Gauss expose la notion de congruence qu'il a élaborée et commence par prouver un certain nombre de propriétés immédiates de cette relation entre deux entiers relatifs.

> *Si un nombre a divise la différence des nombres b et c, b et c sont dits congrus suivant a, sinon incongrus. a s'appellera le module ; chacun des nombres b et c, résidus de l'autre dans le premier cas et non résidus dans le second. Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire sans aucun signe. Ainsi -9 et $+16$ sont congrus par rapport au module 5 ; -7 est résidu de 15 par rapport au module 11 ; et non résidu par rapport au module 3. Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque. […]*
>
> *Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses ; ainsi, $-16 \equiv 9\ (mod\ 5)$, $-7 \equiv 15\ (mod\ 11)$.[…]*
>
> *Chaque nombre aura un résidu, tant dans la suite 0, 1, 2, …, $(m-1)$, que dans celle-ci 0, -1, -2, …, $-(m-1)$; nous les appellerons résidus minima ; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. (Gauss, 1807, p. 1-4)*

Une fois énoncées les propriétés de compatibilité avec les opérations, Gauss se propose de montrer l'avantage de la notion de congruence pour établir des propriétés déjà bien connues : les critères de divisibilité par 9 et 11 :

> *Plusieurs théorèmes que l'on a coutume d'exposer dans les traités d'arithmétique, s'appuient sur ceux que nous avons présentés ; par exemple, la règle pour connaître si un nombre est divisible par 9, 11 ou tout autre nombre. Suivant le module toutes les puissances de 10 sont congrues à l'unité ; donc si le nombre est de la forme* $a + 10b + 100c + 1000d + etc.$ *il aura, suivant le module 9 le même résidu minimum que* $a + b + c + d + etc.$ *Il est clair d'après cela, que si l'on ajoute les figures du nombre, sans avoir égard au rang qu'elles occupent, la somme que l'on obtiendra, et le nombre proposé auront les mêmes résidus minima ; si donc ce dernier est divisible par 9, la somme des chiffres le sera aussi, et seulement dans ce cas. (Gauss, 1807, p. 4-5)*

En s'appuyant sur la décomposition canonique d'un nombre entier naturel dans le système décimal de position, Gauss parvient à expliquer simplement le critère de divisibilité par 9 en s'appuyant sur le fait que chaque puissance de 10 est congrue à 1 modulo 9. Voyons plus en détail les arguments sous-jacents à la preuve de Gauss, en considérant un nombre de quatre chiffres *N* écrit sous la forme *dbca* dans le système décimal. On a donc $N = 1000d + 100c + 10b + a$. Or $1000 \equiv 1\ (mod\ 9)$, donc, par compatibilité avec la multiplication, on déduit que $1000d \equiv d\ (mod\ 9)$. De la même manière, $100c \equiv c\ (mod\ 9)$, $10b \equiv b\ (mod\ 9)$. De plus $a \equiv a\ (mod\ 9)$. Donc, vu que l'on peut sommer membre à membre des congruences, on en déduit que $N \equiv d + c + b + a\ (mod\ 9)$. La conclusion dit que $N \equiv 0\ (mod\ 9)$ (ou *N* est divisible par 9) si et seulement si $d + c + b + a \equiv 0\ (mod\ 9)$. Pour Forcadel, la justification du critère de divisibilité par 9 ne résidait que dans le simple fait que 10 est congru à 1 modulo 9 (on rappelle la formulation de Forcadel vue au-dessus : « ayant considéré, que de chaque dizaine qui ôte 9, 1 se trouve pour restant »). Cela laisse penser que ce dernier ne recourrait pas à toutes les puissances de dix, mais seulement à la dizaine dans sa preuve. Cela est tout à fait possible en considérant une autre décomposition d'un entier que la décomposition canonique dans le système décimal, comme nous allons le voir.

Grâce à leur symbolisme efficace et aux propriétés de compatibilité avec les opérations de l'arithmétique, les congruences deviennent un outil démonstratif parfaitement adapté pour lever le voile sur l'algorithme de Forcadel pour tester la divisibilité d'un entier naturel par 7. Prenons à nouveau, pour simplifier, un nombre de quatre chiffres *N* écrit *dbca* dans le système décimal (le lecteur pourra généraliser). Mais au lieu de décomposer *N* de façon canonique, nous l'écrivons sous la forme équivalente suivante qui ne fait intervenir que la dizaine au lieu des puissances de 10 successives : $N = 10(10(10d + c) + b) + a$. On peut rapprocher cette écriture à l'algorithme, dit de Horner, pour générer les polynômes. De cette façon, nous mettons en évidence l'argument essentiel de Forcadel : « de 10 à 7 la différence est 3 », qui, traduit dans le langage des congruences, revient à $10 \equiv 3\ (mod\ 7)$. Ainsi, grâce aux propriétés liant congruences et opérations, nous tirons $10d \equiv 3d\ (mod\ 7)$. Notons d' le résidu modulo 7 de $3d$. Donc $10d + c \equiv d' + c\ (mod\ 7)$. Notons c' le résidu modulo 7 de $d' + c$. Alors $10d + c \equiv c'\ (mod\ 7)$. Apparaissent ainsi les premières justifications de l'algorithme : commencer par « le dernier chiffre » comme le dit Forcadel (le premier, *d*, pour nous), le multiplier par 3, supprimer tous les 7 pour déterminer d', puis additionner le chiffre suivant *c*, puis à nouveau supprimer tous les 7 pour trouver c'. Ces instructions doivent être répétées jusqu'au chiffre *a* comme le montre l'expression $N = 10(10(10d + c) + b) + a$, puisqu'à chaque étape, on multiplie par 10. Les congruences expliquent aussi pourquoi Forcadel propose de substituer 2 ou 1 respectivement aux chiffres 9 ou 8 dans l'écriture du nombre, puisque $9 \equiv 2\ (mod\ 7)$ et $8 \equiv 1\ (mod\ 7)$ et que ces substitutions sont licites en vertu de leurs propriétés.

VI- TEXTE 5 : UN SECOND EXTRAIT DES *RECHERCHES ARITHMÉTIQUES* DE CARL FRIEDRICH GAUSS

Pour terminer nos lectures historiques, nous étudierons deux autres extraits de la seconde section des *Recherches arithmétiques* de Gauss dans l'édition française de 1807.

13. THÉORÈME. *Le produit de deux nombres positifs plus petits qu'un nombre premier donné, ne peut être divisé par ce nombre premier.*

Soit p le nombre premier et $a < p$ et > 0; je dis qu'on ne pourra trouver aucun nombre positif b, plus petit que p, qui rende

$$ab \equiv 0 \text{ (module } p\text{)}.$$

En effet, s'il peut y en avoir, supposons que ce soient les nombres $b, c, d,$ etc, tous plus petits que p, ensorte qu'on ait $ab \equiv 0$, $ac \equiv 0$, etc., (mod. p), soit b le plus petit de tous, desorte qu'on n'en puisse supposer un plus petit que b, on aura évidemment $b > 1$; car si $b = 1$, on aurait $ab = a < p$ et partant non divisible par p. Or p comme nombre premier ne peut être divisé par b, mais tombera entre deux multiples de b, mb et $(m+1)b$. Soit $p - mb = b'$, b' sera positif et $< b$. Or nous avons supposé $ab \equiv 0$ (mod. p), on aura donc $mab \equiv 0$; et retranchant de $ap \equiv 0$, on aura $a(p - mb) = ab' \equiv 0$; donc b' devrait être mis au rang des nombres $b, c, d,$ etc., et serait plus petit que le plus petit de tous, ce qui est contre la supposition.

14. *Si aucun des deux nombres* a *et* b *n'est divisible par un nombre premier* p, *le produit* ab *ne le sera pas non plus.*

Soient α et β les résidus *minima* positifs des nombres a et b, suivant le module p, aucun d'eux ne sera nul par hypothèse. Or si l'on avait $ab \equiv 0$, comme $ab \equiv \alpha\beta$, on aurait $\alpha\beta \equiv 0$, ce qui serait contraire au théorème précédent.

Figure 4. Début de la seconde section des Recherches arithmétiques de Gauss (Gauss, 1807, p. 6)

Le théorème énoncé au début de la seconde section (paragraphe 19) est un lemme permettant d'établir le théorème du paragraphe suivant. Ce dernier n'est autre que le « lemme d'Euclide » reformulé dans sa forme contraposée. Sa démonstration est tout autre que celle d'Euclide. Elle ne se base que sur la notion de division euclidienne et utilise le formalisme des congruences. À son propos, Gauss écrit :

> *La démonstration de ce théorème a déjà été donnée par Euclide, El. VII, 32. Nous n'avons pas cependant voulu l'omettre, tant parce que plusieurs auteurs modernes ont présenté des raisonnements vagues au lieu de démonstration, ou bien ont négligé ce théorème ; que dans le but de faire mieux saisir, par ce cas très simple, l'esprit de la méthode que nous appliquerons par la suite à des points bien difficiles. (Gauss, 1807, p. 6)*

Nous constatons que les organisations axiomatico-déductives chez Gauss, Prestet et Euclide sont différentes. Gauss établit le lemme d'Euclide comme un préalable au théorème fondamental de l'arithmétique, théorème central de sa seconde section. Il nous montre une preuve qui ne fait pas appel au théorème qui porte son nom ! Bien souvent, dans notre enseignement de mathématiques expertes de

terminale, le théorème de Gauss précède le théorème fondamental, car il permet d'établir l'unicité de la décomposition en facteurs premiers. D'autres articulations sont donc possibles et le lemme d'Euclide peut se substituer au théorème de Gauss à cet effet. Dans tous les cas, la preuve que Gauss donne de ce lemme nous paraît très instructive pour une classe. Au niveau des connaissances utiles, on sollicite essentiellement la division euclidienne. Au niveau du raisonnement, elle fait travailler le raisonnement par l'absurde, basé ici sur le plus petit élément d'une partie non vide de $\mathbb{N}$, puis la contraposition. Une fois le théorème fondamental de l'arithmétique établi, Gauss déduit différents résultats dont certains sont présentés en figure 5.

19. *Si les nombres* a, b, c, etc. *sont premiers avec* k, *leur produit l'est aussi.*

En effet, puisqu'aucun des nombres a, b, c, etc. n'a de facteurs premiers communs avec k, et que le produit de ces nombres ne peut avoir de facteurs premiers qui n'appartiennent à quelqu'un d'entr'eux, ce produit n'aura non plus aucun facteur premier commun avec k.

Si les nombres a, b, c, *etc. sont premiers entr'eux, et que* k *soit divisible par chacun d'eux, il le sera aussi par leur produit.*

C'est une suite des nos 17 et 18. Soit en effet p un diviseur premier quelconque du produit abc etc. et qu'il ait l'exposant π, quelqu'un des nombres a, b, c, etc. sera divisible par p^{π}, parconséquent k, qui est divisible par ce nombre, le sera aussi par p^{π} : il en sera de même des autres diviseurs du produit.

Donc, *si deux nombres* m, n *sont congrus suivant plusieurs modules* a, b, c, etc. *premiers entr'eux, ils le seront aussi suivant leur produit.* En effet, puisque $m-n$ est divisible par chacun des nombres a, b, c, etc., il le sera aussi par leur produit.

Enfin, *si* a *est premier avec* b, *et que* ak *soit divisible par* b, k *sera aussi divisible par* b. En effet, puisque ak est divisible par a et par b, il le sera par leur produit; donc $\frac{ak}{ab}=\frac{k}{b}$ sera un entier.

Figure 4. Conséquences du théorème fondamental de l'arithmétique (Gauss, 1807, p. 9)

Parmi ces corollaires, nous voyons apparaître la propriété (P) dans une forme généralisée : « si les nombres *a*, *b*, *c*, etc. sont premiers entr'eux, et que *k* soit divisible par chacun d'eux, il le sera aussi par leur produit », mais également le théorème de Gauss : « si *a* est premier avec *b*, et que *ak* est divisible par *b*, *k* sera aussi divisible par *b* ».

VII - CONCLUSION

Nous espérons que ces quelques textes (dont il faut rappeler le caractère non exhaustif) auront donné au lecteur l'envie de découvrir davantage l'histoire de l'arithmétique. Au-delà du dépaysement que procure la lecture de textes anciens, l'histoire permet de nous interroger sur les notions que l'on manipule et que l'on enseigne aujourd'hui, ainsi que sur les pratiques du raisonnement et de la démonstration. Choisis pour leur rapport avec la question liminaire de l'extension des critères de divisibilité, notamment aux nombres 6 et 7, les textes ont montré un triple intérêt.

Au niveau mathématique, ils mettent en lumière les liens étroits entre trois théorèmes : le lemme d'Euclide, le théorème de Gauss et le théorème fondamental de l'arithmétique. Les équivalences logiques qui les unissent donnent lieu à diverses démonstrations. Il n'y a donc pas unicité de la façon d'articuler

ces différents théorèmes. Les textes montrent aussi la diversité des types de raisonnement en arithmétique (raisonnements directs, par l'absurde, algorithmique, par contraposition, utilisation du plus petit élément, etc.) et sur quelles connaissances s'appuie chacun d'eux.

Au niveau historique, nous voyons des constructions axiomatiques différentes, pensées par leurs auteurs en fonction de leurs préoccupations et de leurs objectifs. Euclide adosse son livre VII des *Éléments* à la théorie des proportions pour les nombres, de la même façon qu'il donne des applications de cette théorie pour les grandeurs continues en géométrie dans le livre VI. Gauss base son édifie sur la division euclidienne de laquelle il tire la relation de congruence. L'évolution de la pensée se traduit aussi dans le vocabulaire, dans les expressions utilisées, mais aussi dans le développement du formalisme des congruences au XIXe siècle : « le nombre a mesure b » ou « a mesure b sans reste » se traduisent chez Gauss par $b \equiv 0\ (mod\ a)$. Enfin, plonger dans l'histoire permet d'interroger la dénomination des théorèmes. Dans nos déambulations, nous avons vu que le « lemme d'Euclide » est présent dans les *Éléments* et que le « théorème de Gauss » est effectivement énoncé par Gauss ! Mais nos lectures doivent nous inciter à la prudence. Lorsqu'un théorème porte le nom d'un mathématicien cela n'assure ni que ce mathématicien l'ait énoncé ou démontré (il suffit de penser aux célèbres théorèmes de Thalès ou de Pythagore), ni, dans le cas contraire, qu'il soit le premier à le faire. Nous avons vu ici apparaître le « théorème de Gauss » dans un ouvrage de Prestet composé un peu plus de cent ans avant les *Recherches arithmétiques*. Dans ce dernier ouvrage, ce théorème est énoncé dans une liste de conséquences du théorème fondamental de l'arithmétique et Gauss ne semble pas lui accorder une place plus importante qu'aux autres corollaires qu'il déduit ; place qui justifierait sa postérité. Au contraire, il semble réhabiliter le « lemme d'Euclide » comme étant un outil plus essentiel. Dans ce dédale axiomatico-déductif, la propriété (P) n'apparaît pas toujours dans les traités d'arithmétique anciens malgré sa simplicité et son utilité pour les critères de divisibilité.

Au niveau didactique, les textes doivent interroger l'enseignant sur la production d'un discours normé. Comme nous l'avons vu, plusieurs approches sont possibles lorsqu'il s'agit de construire un enchaînement déductif de propriétés arithmétiques. En ouvrant des manuels de mathématiques expertes de terminale générale, où ce type de propriétés est au programme, nous avons constaté une uniformisation de la construction du cours d'arithmétique, sans doute formaté par la rédaction des programmes officiels (dont des extraits sont fournis en annexe 1). L'organisation classique est : PGCD et algorithme d'Euclide, caractérisation des nombres premiers entre eux par l'identité de Bézout, théorème de Gauss (dont on trouvera la preuve dans divers manuels en annexe 2) démontré à l'aide de l'identité de Bézout, puis l'étude des nombres premiers et du théorème fondamental de l'arithmétique. En ayant exploré notre corpus, l'enseignant sera conscient que cet ordre n'est pas avéré dans l'histoire et pourra peut-être mieux répondre aux sollicitations des élèves sur l'origine des notions.

Par le choix de notre problématique initiale, très simple, concernant l'extension naturelle des critères de divisibilité par tous les entiers de 2 à 12, nous voulions montrer que des questions élémentaires peuvent conduire à des résultats relativement sophistiqués et motiver des preuves. Les textes nous enseignent qu'il y a parfois moyen de raisonner en admettant des outils plus élémentaires, comme la caractérisation des fractions par leur écriture irréductible ou l'écriture d'un entier naturel à la « manière de Horner ». Ils peuvent constituer une source d'inspiration pour la conception d'activités historico-mathématiques en classe. La lecture et l'analyse d'un texte constituent des tâches envisageables, mais il en existe d'autres. Par exemple, le travail d'imitation auquel nous nous sommes prêtés au cours de cet article est un excellent

moyen pour pratiquer les mathématiques d'une époque donnée et mieux se les approprier. Il est également possible de comparer des textes pour faire sortir les différences d'approches discursives. Enfin, le travail de traduction consistant à produire une preuve ancienne avec des outils modernes, comme nous l'avons fait avec la preuve de la divisibilité par 7 grâce aux congruences, est lui aussi très formateur. L'histoire des mathématiques a de nombreuses vertus, tant dans la formation des professeurs que dans la pratique de la classe, que nous ne cesserons de faire connaître et de louer.

VIII - BIBLIOGRAPHIE

Sources primaires

Euclide (1990). *Les Éléments* (traduit par B. Vitrac), vol. 2. Paris : PUF.

https://www.academia.edu/1229085/Les_Éléments_Livres_V_VI_Proportions_et_similitudes_Livres_VII_IX_Arithmétique

Forcadel, P. (1556). *L'arithmeticque*. Paris : Gallina in Pingui.

https://books.googleusercontent.com/books/content?req=AKW5QacgmschOSQrq6XOKR-zJuMbjTJCnjGD_zAeOgiNZm_pipwH6XIEuoe8Y6ooFnBSzdTSAo1cm2G_QGMT1Gmihf2jgfUU1YL5NHB7JdQarU_MEE_aIwOX_uforvfj_oWnrNcEv385fY9TUdfK4YZXv2dHnYSj_ykU9Oi8vkl3-QveiuVHkWYG6IQqpfLtgQEdNiqwcDRs7314atvFi85nUCjPYOqn4H92VcfXzJMesE3jOMU7_D93anjGTHceSmtDvu72jTTA

Gauss, C. F. (1807). *Recherches arithmétiques* (traduit par A.-C.-M. Poullet-Delisle). Paris : Courcier.

https://gallica.bnf.fr/ark:/12148/bpt6k29060d

Prestet, J. (1695). *Nouveaux élémens des mathématiques ou principes généraux de toutes les sciences qui ont les grandeurs pour objet*, Premier volume. Paris : André Pralard.

https://books.google.fr/books/about/Nouveaux_elemens_des_mathematiques_ou_Pr.html?id=bnIheoK3D-EC&redir_esc=y

Sources secondaires

Barbin, É. (2019). *Faire des mathématiques avec l'histoire au lycée*. Paris : Ellipses.

Bühler M. et Michel-Pajus, A. (2007). Sur différents types de démonstration rencontrées spécifiquement en arithmétique. *Mnémosyne*, *19*, 19-60.

https://publimath.univ-irem.fr/numerisation/PS/IPS07001/IPS07001.pdf

Goldstein, C. (1992). On a Seventeenth Century Version of the "Fundamental Theorem of Arithmetic". *Historia Mathematica*, *19*, 177-187.

https://www.sciencedirect.com/science/article/pii/031508609290075M?via%3Dihub

Henry, M. (2001). Le théorème de Gauss dans les Éléments d'Euclide ?! *Bulletin APMEP*, *433*, 204-218.

Groupe Géométrie et Arithmétique de l'IREM d'Aquitaine (1999). Initiation à l'arithmétique, *IREM d'Aquitaine*.

https://publimath.univ-irem.fr/numerisation/BO/IBO99001/IBO99001.pdf

IX - ANNEXE 1 : EXTRAITS DU PROGRAMME DE MATHÉMATIQUES EXPERTES DE TERMINALE GÉNÉRALE

- **Histoire des mathématiques**

L'arithmétique des entiers est présente chez les mathématiciens grecs, par exemple dans les *Éléments* d'Euclide, chez Nicomaque de Gérase, Théon de Smyrne ou encore Diophante, dont certains développements touchent à la combinatoire. Les aspects algorithmiques sont présents depuis l'origine : méthodes de fausse position, algorithme d'Euclide, algorithme d'Euclide étendu de Bachet (1612) puis Bézout (1766), applications aux fractions continues chez Euler (1737), nombre de racines d'une équation chez Sturm (1835).

L'histoire de la théorie des nombres, qui permet d'évoquer les travaux de Fermat, Lagrange, Gauss, Dirichlet et de bien d'autres, fourmille de théorèmes d'énoncés simples aux preuves difficiles, ainsi que de conjectures de formulation élémentaire mais non résolues.

Des questions issues de l'arithmétique, apparemment gratuites, ont donné lieu à des applications spectaculaires en cryptographie ou codage. On peut noter enfin l'intérêt historique de l'étude de nombres particuliers par exemple ceux de Fermat, Mersenne, Carmichael ou Sophie Germain.

Contenus

- Divisibilité dans $\mathbb{Z}$.
- Division euclidienne d'un élément de $\mathbb{Z}$ par un élément de $\mathbb{N}^*$.
- Congruences dans $\mathbb{Z}$. Compatibilité des congruences avec les opérations.
- PGCD de deux entiers. Algorithme d'Euclide.
- Couples d'entiers premiers entre eux.
- Théorème de Bézout.
- Théorème de Gauss.
- Nombres premiers. Leur ensemble est infini.
- Existence et unicité de la décomposition d'un entier en produit de facteurs premiers.
- Petit théorème de Fermat.

Capacités attendues

- Déterminer les diviseurs d'un entier, le PGCD de deux entiers.
- Résoudre une congruence $ax \equiv b\ [n]$. Déterminer un inverse de a modulo n lorsque a et n sont premiers entre eux.
- Établir et utiliser des tests de divisibilité, étudier la primalité de certains nombres, étudier des problèmes de chiffrement.
- Résoudre des équations diophantiennes simples.

Démonstrations

- Écriture du PGCD de a et b sous la forme $ax + by$, $(x,y) \in \mathbb{Z}^2$.
- Théorème de Gauss.
- L'ensemble des nombres premiers est infini.

$

X - ANNEXE 2 : EXTRAITS DE MANUELS DE MATHÉMATIQUES EXPERTES DE TERMINALE GÉNÉRALE

Les extraits suivants montrent quelques démonstrations du théorème de Gauss dans des manuels de mathématiques expertes de terminale générale.

Manuel Le livre scolaire, 2020

DÉMONSTRATION

Supposons que a divise bc et que a et b sont premiers entre eux.

Alors $\text{PGCD}(a\,;b)=1$ donc d'après le théorème de Bézout, il existe $(u\,;v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

On a donc $auc+bvc=c$. Or $a \mid bc$ par hypothèse et $a \mid auc$ donc $a \mid (auc+bvc)$.

Ainsi, $a \mid c$.

Manuel Sésamath, Magnard, 2020

Démonstration

Démontrons à l'aide du théorème de Bézout.

- a divise bc donc il existe un entier relatif k tel que : $bc=ka$. (Éq. 1)
- a et b sont premiers entre eux donc d'après le théorème de Bézout, il existe un couple d'entiers relatifs $(u\,;v)$ tel que : $au+bv=1$. (Éq. 2)
- (Éq. 2) $\times c$: $acu+bcv=c \overset{\text{(Éq. 1)}}{\Rightarrow} acu+kav=c \Rightarrow a(cu+kv)=1$

  Donc a divise c.

Manuel Barbazo, Hachette éducation, 2020

Rédiger une démonstration

1 On souhaite démontrer la propriété suivante.

Soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

- On suppose que a divise bc. En déduire une écriture de bc en fonction de a.
- Justifier qu'il existe des entiers relatifs u et v tels que $au+bv=1$.
- Multiplier cette égalité par c.
- En utilisant l'écriture de bc obtenue au premier point. Factoriser l'égalité par a et conclure.

2 On souhaite démontrer la propriété suivante.

Soient a, b et c trois entiers relatifs non nuls.
Si a divise c et b divise c avec a et b premiers entre eux alors ab divise c.

- Exprimer c en fonction de a et c en fonction de b.
- Quelle égalité peut-on en déduire ?
- Appliquer le théorème de Gauss et conclure.

Manuel Hyperbole, Nathan, 2020.

A Le théorème de Gauss

Théorème de Gauss

a, *b* et *c* désignent trois nombres entiers relatifs non nuls.
Si ***a* divise le produit *bc*** et si ***a* et *b* sont premiers entre eux**, alors ***a* divise *c***.

Démonstration

a et *b* sont premiers entre eux, d'après le théorème de Bézout, il existe des nombres entiers relatifs *u* et *v* tels que $au + bv = 1$.

En multipliant chaque membre de l'égalité par *c*, on obtient $auc + bvc = c$.
a divise *auc* et par hypothèse, *a* divise *bc* donc *bvc*, alors *a* divise $auc + bvc$, c'est-à-dire *a* divise *c*.

Remarque : l'hypothèse *a* et *b* sont premiers entre eux est essentielle. En effet, *a* peut diviser *bc* sans diviser ni *b*, ni *c*. Par exemple 6 divise 300 sans diviser ni 15 ni 20.

Exemple

Résolution de l'équation $7x = 11y$ avec $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$.
• Si $7x = 11y$, alors 11 divise $7x$.
Or 7 et 11 sont premiers entre eux, donc d'après le théorème de Gauss, 11 divise x.
Par conséquent, il existe un entier relatif *k* tel que $x = 11k$.
Alors de $7x = 11y$, on déduit que $7 \times 11k = 11y$, soit $y = 7k$.
• Réciproquement, tous les couples $(11k\,;7k)$ avec $k \in \mathbb{Z}$, sont solutions de l'équation $7x = 11y$.
En effet, $7 \times 11k = 11 \times 7k$.
• **Conclusion**
Les solutions de l'équation $7x = 11y$ sont les couples $(11k\,;7k)$ avec $k \in \mathbb{Z}$.

CONJECTURES ET PREUVES

Stéphane VINATIER
Enseignant-chercheur, université de Limoges
XLIM UMR 7252 CNRS – Univ. Limoges
stephane.vinatier@unilim.fr

Résumé
Nous décrivons les activités conçues par le groupe « Conjectures et preuves » de l'IREM de Limoges pour initier les élèves aux différents types d'énoncés mathématiques suivants : question, conjecture et propriété. Ces activités mettent les élèves en position de recherche en leur faisant appliquer des procédures relativement simples sur les nombres. Une des fiches d'activités conçues par le groupe figure en annexe en fin de document.

INTRODUCTION

Le groupe « Conjectures et preuves » de l'IREM de Limoges est composé actuellement de trois enseignants en collège :

- Jessica BARRIÈRE : collège Cabanis à Brive-la-Gaillarde
- Patrick GUILLOU : collège Ronsard à Limoges (désormais retraité)
- Guillaume VERGNE : collège Jean Moulin à Brive-la-Gaillarde

et de deux universitaires :

- Christophe CLAVIER et Stéphane VINATIER : université de Limoges

Même si sa composition a évolué au fil des années, ce groupe a une histoire propre de plus d'une décennie et la particularité de se réunir depuis ses débuts en Corrèze (à Tulle pendant longtemps, désormais à Brive-la-Gaillarde).

Le thème du travail présenté au colloque de Talence provient d'ailleurs des travaux précédents du groupe. Mélangeant géométrie, arithmétique et programmation, l'idée était de motiver l'initiation à Scratch par la réalisation de polygones étoilés (inscrits dans des polygones convexes dans un second temps) et d'en profiter pour explorer leurs propriétés arithmétiques (surprenantes !). La recherche de procédures efficaces de tracé de ces figures (voir Figure 1) a fait réfléchir les membres du groupe, qui se sont pris à tester diverses méthodes, conjecturer certaines propriétés et s'extasier quand le programme qui en découlait produisait le résultat voulu, validant d'une certaine façon la conjecture et incitant à en chercher une preuve mathématique.

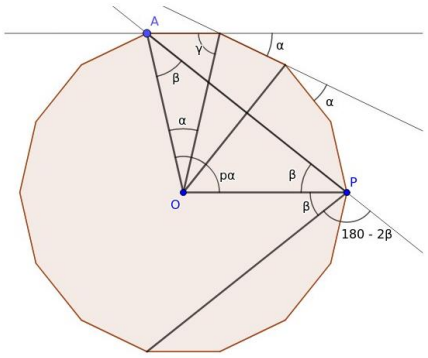


Figure 1. La mesure de l'angle de rotation du lutin au sommet d'un polygone étoilé.

Le caractère stimulant de cette activité de recherche imprévue a donné envie au groupe d'en faire profiter les élèves ! L'idée initiale était de concevoir des activités pour leur faire formuler des conjectures, notamment en utilisant des outils informatiques, de les faire réfléchir à partir de ces conjectures : formulation d'énoncés, explications, débat et enfin de les faire cheminer vers la rédaction.

Comme on le verra, le produit final est un peu différent de ce qui était envisagé mais en conserve les idées principales.

AU PROGRAMME

Ce qui concerne le raisonnement en mathématiques apparaît essentiellement dans le préambule des programmes de mathématiques, et très peu, voire pas du tout, dans les contenus qui sont la partie sur laquelle se concentrent en général les enseignements, en particulier les évaluations. À cette réserve importante près, une bonne place est accordée à cet aspect essentiel de l'activité mathématique dans le programme du cycle 4 (de la rentrée 2018) que nous regardons maintenant de plus près.

1. Considérations générales

Citons quelques extraits du préambule du programme de mathématiques du cycle 4, en mettant en gras les passages où nous considérons que les activités que nous proposons peuvent contribuer à la réalisation des objectifs cités.

> *Une place importante doit être accordée à la résolution de problèmes. Mais pour être en capacité de résoudre des problèmes, il faut à la fois* ***prendre des initiatives, imaginer des pistes de solution*** *et s'y engager sans s'égarer en procédant par analogie, en rattachant une situation particulière à une classe plus générale de problèmes (…)*

La prise d'initiative peut être tout simplement le choix d'un entier à 3 ou 4 chiffres, au début d'une activité, pour lui appliquer la procédure qui a été décrite. Ce simple choix d'un nombre parmi des centaines ou des milliers semble être un obstacle pour beaucoup d'élèves ! Ce qui montre la pertinence des activités en question pour travailler cette compétence, à la base de la résolution de nombreux problèmes. La recherche

de « pistes de solution » apparaît un peu plus loin dans la plupart des activités, lorsqu'il faut expliciter ou expliquer les faits qui ont été observés sur un certain nombre d'exemples.

> *La **formation au raisonnement et l'initiation à la démonstration** sont des objectifs essentiels du cycle 4. Le raisonnement, au cœur de l'activité mathématique, doit prendre appui sur des situations variées (…)*

Nos activités sont centrées sur la distinction entre les statuts de « question », de « conjecture » ou de « propriété » pour un énoncé qu'on aura découvert, ce qui implique de travailler la notion de démonstration pour distinguer entre les deux derniers.

> *Le programme du cycle 4 permet d'initier l'élève à différents types de raisonnement, le raisonnement déductif, mais aussi le raisonnement par disjonction de cas ou par l'absurde. La démonstration, forme d'argumentation propre aux mathématiques, vient compléter celles développées dans d'autres disciplines et **contribue fortement à la formation de la personne et du citoyen** (domaine 3 du socle). L'apprentissage de la démonstration doit se faire de manière progressive, à **travers la pratique (individuelle, collective, ou par groupes)**, mais aussi par l'exemple.*

Nous reviendrons sur le lien entre nos activités et la formation de la personne et du citoyen dans la partie IV.3, où nous faisons part des commentaires des enseignants qui ont testé les activités en classe.

2. Statut des énoncés mathématiques

L'extrait suivant peut paraître mystérieux en première lecture :

> *Enfin, il vaut mieux déclarer « admise » une propriété non démontrée dans le cours (qui pourra d'ailleurs l'être ultérieurement), plutôt que de la présenter comme une « règle ». Une propriété admise gagne à être explicitée, commentée, illustrée. (...)*

Il nous semble être éclairé par le passage suivant qu'on trouve peu après :

> *En particulier, il est essentiel de distinguer le statut des énoncés (**définition, propriété** – admise ou démontrée –, **conjecture, démonstration, théorème**) et de respecter les enchaînements logiques.*

Nous y voyons la volonté, dans l'esprit des concepteurs des programmes, que les mathématiques soient présentées autant que faire se peut aux élèves pour ce qu'elles sont, c'est-à-dire une construction logique dans laquelle les propriétés découlent des axiomes (et des propriétés déjà démontrées) par le raisonnement déductif. Là où le mot « règle » pourrait donner une impression d'arbitraire et d'autorité supérieure (la règle d'un jeu résulte des choix des concepteurs et sa validité n'a donc pas à être remise en question), l'expression « propriété admise » renvoie pensons-nous à ce système déductif dans lequel les propriétés peuvent être prouvées depuis les fondements, pour peu qu'on ait les connaissances adéquates des notions utilisées au cours du chemin déductif qui les relient. Il ne faut pas laisser penser faussement aux élèves qu'elles seraient imposées arbitrairement par une autorité supérieure (celle de l'enseignant ?).

Il s'agit donc de ne pas mettre les élèves sur une mauvaise piste concernant ce que sont les mathématiques. On voit qu'il s'agit aussi, plus précisément, de les amener à distinguer entre différents types d'énoncés mathématiques, que nous avons tous mis en gras dans le texte ci-dessus même si nos activités n'abordent pas spécifiquement la notion de définition (nous y reviendrons plus loin).

3. Compétences

Le préambule indique un certain nombre de types d'activités à mettre en œuvre en cours de mathématiques et continue comme suit.

> *La pratique régulière et équilibrée de ces différentes activités (...) permet de développer six compétences spécifiques, qui sont les composantes majeures de l'activité mathématique : **chercher**, modéliser, représenter, **raisonner**, calculer, **communiquer**.*

Là encore nous faisons ressortir les compétences les plus visées par les activités que nous proposons. Nous verrons que, selon les choix pédagogiques faits par les enseignants (avec ou sans calculatrice, notamment), la plupart d'entre elles sont susceptibles de faire travailler fortement la compétence « calculer », même si ce n'est pas l'objectif principal.

Passons en revue les trois compétences que nous avons soulignées.

3.1. Chercher

Cette compétence est décrite comme suit dans le programme.

- *Extraire d'un document les informations utiles, les reformuler, les organiser, les confronter à ses connaissances.*
- *S'engager dans une démarche scientifique, observer, **questionner, manipuler, expérimenter** (sur une feuille de papier, avec des objets, à l'aide de logiciels), **émettre des hypothèses, chercher des exemples ou des contre-exemples, simplifier ou particulariser une situation, émettre une conjecture.***
- ***Tester, essayer plusieurs pistes de résolution.***
- *Décomposer un problème en sous-problèmes.*

Dans nos activités, l'expérimentation sera très présente et se fera essentiellement sur le papier ; il s'agira de mener certaines procédures de calcul sur un ou plusieurs exemples. Le mot « hypothèse » paraît ambigu ici. Il semble être utilisé comme dans le contexte de la démarche scientifique, où il désigne un énoncé établi à partir des résultats d'une ou plusieurs expériences, qu'on va tenter de confirmer ou d'infirmer en menant d'autres expérimentations, pour lesquelles l'hypothèse devrait permettre de faire des prédictions de résultats. Dans le contexte mathématique, le mot « hypothèse » indique plutôt les conditions de validité d'une propriété (par exemple, l'hypothèse du théorème de Pythagore est que le triangle soit *rectangle*, du moins dans son sens « direct »). Il nous semble qu'il serait plus approprié d'utiliser les expressions « poser des questions » et « émettre des conjectures », c'est ainsi que nous le comprenons en tout cas et c'est dans ce sens que nous le soulignons.

3.2. Raisonner

Cette compétence est décrite comme suit dans le programme.

- *Résoudre des problèmes impliquant des grandeurs variées (géométriques, physiques, économiques) : mobiliser les connaissances nécessaires, analyser et exploiter ses erreurs, mettre à l'essai plusieurs solutions.*

- ***Mener collectivement une investigation en sachant prendre en compte le point de vue d'autrui.***
- ***Démontrer : utiliser un raisonnement logique et des règles établies (propriétés, théorèmes, formules) pour parvenir à une conclusion.***
- ***Fonder et défendre ses jugements en s'appuyant sur des résultats établis et sur sa maîtrise de l'argumentation.***

Noter le retour subreptice du mot « règle » banni un peu plus haut par le même programme… Difficile d'échapper aux termes couramment utilisés en français, même lorsqu'on voudrait employer un langage technique ! C'est d'ailleurs le premier point de la compétence suivante.

Nos activités peuvent toutes amener à mettre en commun les résultats des élèves, résultats de calculs ou de recherche, et donnent donc de nombreuses occasions de mettre en œuvre la recommandation du 2e point ci-dessus. La nécessité de construire des démonstrations a déjà été évoquée. La validation des démonstrations trouvées pourra amener à travailler le dernier point.

3.3. Communiquer

Cette compétence est décrite comme suit dans le programme.

- *Faire le lien entre le langage naturel et le langage algébrique. Distinguer des spécificités du langage mathématique par rapport à la langue française.*
- ***Expliquer à l'oral ou à l'écrit (sa démarche, son raisonnement, un calcul, un protocole de construction géométrique, un algorithme), comprendre les explications d'un autre et argumenter dans l'échange.***
- *Vérifier la validité d'une information et distinguer ce qui est objectif et ce qui est subjectif ; lire, interpréter, commenter, produire des tableaux, des graphiques, des diagrammes.*

La différence entre le dernier item de la compétence « Raisonner » et le 2e de celle-ci est sans doute subtile.

III - ACTIVITES

1. Fiches

Le groupe a rédigé des fiches d'activité sur les 5 thèmes suivants :

- Nombres de Kaprekar (6 pages, reproduites en annexe)
- Persistance multiplicative (13 pages)
- Suites de type Fibonacci (4 pages)
- Sommes de palindromes (11 pages)
- Les nombres heureux (12 pages)

Depuis l'atelier, toutes les fiches ont été complétées et comportent maintenant une partie pour les élèves, destinée à guider leur travail, et une partie « enseignant » contenant des éléments de contexte, des réponses aux questions, des pistes pour aller plus loin. Toutes les fiches à l'exception de la dernière ont

été testées, avec des élèves de 6e, 5e ou 4e, en classe ou en AP, en collège de centre-ville ou en REP+. Deux thèmes supplémentaires ont donné lieu à une activité similaire, proposée par l'un des enseignants du groupe à ses élèves, sur la somme des angles d'un triangle et sur le nombre de régions du disque découpées par les cordes reliant des points sur le cercle en nombre croissant (d'abord 1 région, puis 2, 4, 8, 16 et … 31 !).

2. Structure

Les activités comportent deux étapes importantes :

- une consigne avec une ou plusieurs questions à traiter : souvent un exemple pour commencer, des pistes pour aller plus loin… ; le but est que les élèves découvrent des faits plus ou moins remarquables ou intéressants ;
- une réflexion sur le statut des « énoncés » mathématiques découverts dans la 1re phase, à classer par les élèves dans le tableau ci-dessous.

Les deux phases peuvent être entremêlées, dès que suffisamment d'énoncés ont été découverts, on peut commencer à réfléchir à leur statut, en gardant les questions suivantes pour plus tard.

3. Tableau

Voici la version, au moment de l'atelier, du tableau proposé aux élèves pour classer les énoncés découverts :

C'est vrai, j'en suis sûr(e) ! Je pourrai le prouver si on me le demande	
Cela me semble vrai Je ne sais pas le prouver mais j'y crois	
Y aurait-il un piège ? Je me pose la question de savoir si c'est vrai ou pas	

Le but du tableau est de donner aux élèves l'intuition des trois types d'énoncés mathématiques qui peuvent émerger après une recherche :

- les *propriétés*, lorsqu'on a une preuve que l'énoncé est vrai ;
- les *conjectures*, lorsqu'on a de bonnes raisons de penser qu'il est vrai mais qu'on ne sait pas le prouver ;

- les *questions* qu'on est amené à se poser, lorsque aucune réponse ne semble plus plausible que les autres.

On note que seule la notion de propriété ne prête pas à discussion (encore que, un travail sur la validation des preuves peut aussi être mené). Certains participants à l'atelier ont tout de même suggéré qu'on ajoute une case pour les propriétés *fausses* (« C'est faux ! Je pourrais le prouver »), arguant que la manière de raisonner n'est pas la même pour prouver un énoncé selon qu'il est vrai ou faux. On pourrait alors aussi, par symétrie, ajouter une case pour ce qu'on conjecture être faux. Il nous semble cependant préférable de ne pas augmenter le nombre de lignes du tableau, ce qui complexifierait la tâche des élèves et risquerait de faire obstacle à leur compréhension des principaux types d'énoncés. On peut d'ailleurs toujours exprimer qu'une proposition est fausse en énonçant que sa négation est vraie. Enfin, nos activités, et peut-être même l'activité mathématique en général, nous semblent plutôt orientées vers la recherche de propositions vraies (même si parfois il faut se résoudre à constater que certaines conjectures ou propositions qu'on aurait aimées être vraies sont fausses).

La frontière est plus floue entre les deux derniers types d'énoncés, conjecture ou question. Pour choisir d'attribuer le statut de conjecture, on peut s'appuyer sur :

- l'analogie avec une situation similaire où la réponse est connue ;
- une preuve partielle, par exemple dans des cas particuliers ;
- le nombre d'exemples trouvés par les élèves pour lesquels la réponse est vraie.

La mise en commun des résultats de tous les élèves, s'ils confirment tous un même phénomène, pourra donner du sens à la différenciation entre question et conjecture.

4. Formulations

Nous reprenons de la conférence de Daniel Perrin la citation suivante de Pierre de Fermat, à propos des nombres qui portent son nom.

> *Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme 3, 5, 17, 257, 65 537, 4 294 967 297 et le suivant de 20 lettres 18 446 744 073 709 551 617 ; etc. Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurois peine à me dédire.*

Voici une manière bien emphatique de décrire ce qu'est une conjecture ! Où l'on constate, de plus, qu'il ne suffit pas d'avoir des « grandes lumières » pour énoncer des conjectures solides… En effet Euler a établi en 1732 la factorisation :

$$4\,294\,967\,297 = 641 \times 6\,700\,417$$

Autrement dit le nombre de Fermat $F_5 = 2^{2^5} + 1$ est composé. On a vérifié depuis qu'il en va de même pour F_k jusqu'à $k = 32$ (et on ne sait pas pour les suivants).

Indiquons également que la formulation « Y aurait-il un piège ? » a semblé inadéquate à certains participants à l'atelier. Elle avait été choisie par le groupe à la suite de tests en classe en remplacement de la formule plus neutre « Je ne me prononce pas », pour traduire l'état d'esprit de certains élèves échaudés par des tentatives précédentes de conjectures qui se révélaient fausses. Dans la dernière version des fiches, on a remis la formule moins équivoque « Je ne me prononce pas ». Bien sûr les utilisateurs de fiches peuvent les remanier à leur guise.

5. Thèmes

Nous donnons maintenant quelques indications sur les thèmes traités. Pour des détails, on renvoie aux fiches elles-mêmes, à retrouver sur le site web de l'IREM de Limoges[1].

5.1. Nombres de Kaprekar

Ce thème est assez connu et apparaît dans d'autres fiches d'activités (avec des objectifs différents), plus souvent sous l'appellation « algorithme de Kaprekar ». Comme pour plusieurs des thèmes que nous présentons, il consiste à itérer une opération qui fait intervenir l'écriture en base 10 des entiers. Ici, on choisit un nombre à 4 chiffres (par exemple) et on soustrait le plus petit nombre qu'on peut écrire avec ces quatre chiffres au plus grand. Ainsi :

1753 donne 7531 – 1357 = 6174

6174 donne 7641 – 1467 = 6174

et le processus s'arrête puisqu'on est arrivé sur un point fixe de l'opération (ce qui mettra plus de temps avec d'autres nombres de départ). Un tel point fixe est une *constante de Kaprekar*, que nous avons appelé ici *nombre de Kaprekar* (attention à la confusion avec une autre notion). La fiche complète est incluse en annexe.

5.2. Persistance multiplicative

On part de nouveau d'un entier écrit en base 10 et, cette fois, on fait le produit de ses chiffres :

4861 donne 4 x 8 x 6 x 1 = 192

192 donne 1 x 9 x 2 = 18

18 donne 1 x 8 = 8

et le processus s'arrête puisqu'on arrive à un point fixe de l'opération (le produit des chiffres d'un nombre à 1 chiffre est égal à ce nombre). La *persistance multiplicative* de l'entier dont on est parti est le nombre d'étapes nécessaires pour arriver à un nombre à 1 chiffre : c'est 3 pour 4861.

5.3. Suites de type Fibonacci

On choisit deux nombres a et b et on calcule leur somme $c = a + b$, puis de proche en proche les sommes $d = b + c$, $e = c + d$, $f = d + e$; enfin, si e est non nul, on calcule $(a + b + c + d + e + f) / e$.

[1] Ainsi que sur la page de l'auteur : www.unilim.fr/pages_perso/stephane.vinatier

Cette activité plus simple peut servir d'introduction à ce type d'activités, ainsi qu'au calcul littéral dont elle illustre à merveille l'utilité et l'efficacité.

5.4. Palindromes

Un entier est un palindrome si on trouve le même nombre en renversant l'ordre des chiffres de son écriture en base 10, autrement dit si cette écriture est symétrique par rapport à son « centre ». On s'intéresse alors aux entiers qui s'écrivent somme de deux ou trois palindromes (en référence à un article récent qui prouve que tout entier est somme de trois palindromes). Par exemple, on observe que 201 = 191 + 9 + 1 est somme de trois palindromes mais pas de deux (c'est le seul entier à 3 chiffres qui n'est pas somme de deux palindromes).

5.5. Nombres heureux

L'opération à l'œuvre ici consiste à faire la somme des carrés des chiffres de l'écriture en base 10 d'un entier :

$$44 \text{ donne } 4^2 + 4^2 = 32$$

$$32 \text{ donne } 3^2 + 2^2 = 13$$

$$13 \text{ donne } 1^2 + 3^2 = 10$$

$$10 \text{ donne } 1^2 + 0^2 = 1$$

et le processus s'arrête puisque 1 en est un point fixe. Les *nombres heureux* sont ceux qui terminent sur 1, comme 44.

IV - QUELQUES RETOURS

1. Palindromes

Cette activité a été testée en 6e, en AP (collège centre-ville) et en classe entière travaillant en binômes (collège REP+). Les enseignants ont noté une bonne adhésion des élèves, qu'ils soient motivés au départ ou non, voire même de l'enthousiasme pour certains ; cependant les élèves habituellement en réussite ont parfois eu du mal à quitter le confort des séances classiques. Le contenu de la fiche est très riche : en 1h, seules les questions 1 à 3 ont été traitées, pour certaines avec des indications de l'enseignant ou la mise en commun des idées de tous. Le tableau a nécessité des explications supplémentaires. Certains élèves réclamaient une séance supplémentaire pour terminer l'activité !

2. Retours sur d'autres activités

L'activité « suite de type Fibonacci » a été testée avec deux classes de 5e REP+ : la classe la plus faible a plus cherché et mieux réussi ; la classe plus forte n'a pas compris l'énoncé, les élèves rechignaient à se mettre dans une posture de recherche. L'enseignant fait état d'une rédaction très différente selon les binômes et d'une bonne participation orale collective (remplissage tableau et preuve).

Sur une 2e activité faite à la suite (découpage du disque), les élèves montraient une bonne assimilation de la différence entre propriété et conjecture. Le tableau semble leur parler.

3. Commentaires des enseignants

Ces activités sont importantes à plusieurs niveaux.

- Elles remotivent des élèves qui se sentent en échec dans les activités mathématiques plus classiques, en permettant à de nouvelles compétences de s'exprimer (prise d'initiative, …).
- Elles préparent les élèves aux démonstrations qu'ils verront en cours plus tard, notamment celles de géométrie en 4e et 3e ou celles du lycée.
- Elles contribuent à l'éducation à la laïcité et à la citoyenneté : réfléchir sur la distinction entre conjecture et preuve permet de comprendre, par analogie la différence entre croyance et connaissance.

V - PERSPECTIVES

1. Définitions

Nous nous sommes concentrés sur la distinction entre propriété, conjecture et question. Les preuves apparaissent aussi naturellement dans l'activité, pour justifier le classement de certains énoncés dans la première case plutôt que dans la deuxième, même si cet aspect n'est pas traité dans les fiches et est dévolu à l'enseignant qui mène la séance. La rédaction des preuves peut aussi faire apparaître des énoncés de type définition, qui permettent souvent de clarifier, voire d'alléger, les démonstrations en introduisant les concepts appropriés.

2. Compétences travaillées

Ces exemples d'activités mettent en avant ou développent certaines notions propres au raisonnement et à la recherche mathématique.

- La prise d'initiative : choisir un exemple et se lancer !
- Les capacités d'explication, de rédaction, de synthèse : traduire des phénomènes observés en énoncés mathématiques.
- La capacité à discerner les statuts des énoncés : question, conjecture, propriété, preuve, exemple, contre-exemple …
- La capacité à travailler sur un problème ouvert aussi bien que vers un objectif donné (prouver une propriété).

3. Institutionnalisation ?

On pourrait imaginer avoir tout un répertoire d'activités, pour chacune des notions listées ci-dessus, afin de :

- les faire découvrir aux élèves ;
- permettre aux élèves de les assimiler ;

- évaluer leur acquisition par les élèves.

Ce type d'activité pourrait alors intégrer le corps du programme de mathématiques du cycle 4 (et pas seulement le préambule) et être travaillé pour lui-même. Réaliser un tel répertoire demanderait certainement un travail conséquent et, en retour, contribuerait fortement à l'acquisition des compétences visées par les élèves. D'un autre côté, l'institutionnalisation de ce type d'activité le rendrait peut-être moins attractif pour les élèves. Se pose donc la question de savoir si une telle institutionnalisation serait souhaitable ?

4. Progression

On peut envisager d'expliciter des compétences plus sophistiquées, développées à partir de celles acquises au travers de ces activités :

- la capacité à organiser les idées, le raisonnement ;
- l'accès à un raisonnement modulaire où on sépare les tâches qui peuvent être traitées indépendamment ;
- la capacité à faire une hypothèse et à en déduire une conclusion (la brique de base du raisonnement déductif, par exemple pour montrer une équivalence par double implication) ;
- l'accès à des raisonnements plus sophistiqués, comme prouver qu'une assertion est équivalente à une autre qui contient une implication.

BIBLIOGRAPHIE

- Sur wikipédia, Kaprekar : https://fr.wikipedia.org/wiki/Dattatreya_Ramachandra_ Kaprekar et son algorithme : https://fr.wikipedia.org/wiki/Algorithme_de_Kaprekar
- La biographie (en anglais) de Kaprekar sur Mac Tutor Index : https://mathshistory. st-andrews.ac.uk/Biographies/Kaprekar/
- Une activité sur l'algorithme de Kaprekar sur le site de l'académie de Créteil : https://maths.ac-creteil.fr/IMG/pdf/kaprekar.pdf
- La page de Gérard Villemin intitulée « Algorithme, itération, procédé, opération ou cycle de Kapreka » : http://villemin.gerard.free.fr/Wwwgvmm/Iteration/Kaprekar. htm; lui aussi désigne 6174 comme un *nombre de Kaprekar*.

ANNEXE : FICHE D'ACTIVITÉ « NOMBRES DE KAPREKAR »

On inclut ci-dessous la fiche complète consacrée à l'algorithme et à la constante de Kaprekar (6174), ainsi qu'à ses analogues pour les nombres à deux ou trois chiffres. Elle contient l'activité pour les élèves, les objectifs, un historique, les réponses aux questions, des variantes de l'algorithme et quelques références sur internet.

Activité n°1 : nombres de Kaprekar

1. Choisir un nombre à 4 chiffres.
2. Écrire le plus grand nombre possible avec ces chiffres, ainsi que le plus petit possible (Aide : dans quel ordre faut-il écrire les chiffres pour obtenir le plus grand ?), puis calculer la différence entre ces deux nombres.
3. Recommencer à partir de l'étape 2 avec le résultat obtenu.
4. Que remarques-tu ?
5. Que remarquez-vous ?

Classe tes réponses aux questions dans le tableau page suivante.

C'est vrai, j'en suis sûr(e) ! Je pourrai le prouver si on me le demande	
Cela me semble vrai Je ne sais pas le prouver mais j'y crois	
Je ne me prononce pas Je me pose la question de savoir si c'est vrai ou pas	

POUR L'ENSEIGNANT

1. Objectifs

L'activité a un double objectif :

(i) faire découvrir aux élèves des énoncés mathématiques de différents statuts : propriétés, conjectures ou simples questions ; c'est l'objet des questions 1. à 6. ;

(ii) les faire réfléchir au statut des énoncés qui ont été découverts : c'est à cet effet qu'on leur demande, à la fin, de classer leurs réponses (c'est-à-dire les énoncés qui ont été mis au jour) dans le tableau de la page 2.

Les rubriques du tableau tentent de donner une idée intuitive de ce qu'on entend par propriété (case « C'est vrai, j'en suis sûr »), conjecture (case « Cela me semble vrai ») ou simple question (case « Je ne me prononce pas »), laquelle est précisée par une phrase plus explicite. Le vocabulaire lui-même n'est pas au programme du cycle 4 (ce qui bien sûr n'empêche pas de l'utiliser si on le souhaite), ce qui paraît important pour la suite des apprentissages mathématiques est de faire émerger chez les élèves la conscience que tous les énoncés (mathématiques, ou autre !) n'ont pas le même statut et de les entraîner, dans des cas simples, à déterminer le statut de tel ou tel énoncé.

2. Histoire

Dattatreya Ramachandra Kaprekar (1905 – 1986, de nationalité indienne), passionné par les nombres depuis l'enfance, suit une carrière d'instituteur tout en poursuivant des recherches personnelles pour assouvir sa passion. Vers 1949, travaillant sur l'écriture des nombres, il découvre la constante de Kaprekar : le nombre 6174 = 7641 − 1467, vers lequel converge toute suite construite avec un nombre de quatre chiffres (non tous égaux) auquel on applique l'algorithme de Kaprekar.

Travaillant sur un autre algorithme, « ajouter à un nombre la somme de ses chiffres en écriture décimale », il découvre la notion de nombre généré et d'auto-nombre. Il s'intéresse aussi aux nombres de Demlo. Enfin, il a étudié les nombres de Kaprekar : nombres égaux à la somme des deux nombres obtenus en prenant le carré du nombre de départ et en le découpant en deux parties (9 est un nombre de Kaprekar car 92 = 81 et 8 + 1 = 9). Il contribue aussi à la découverte des nombres harshad, appelés aussi nombres de Niven : nombres divisibles par la somme de leurs chiffres.

Boudé par ses contemporains, ses travaux seraient passés inaperçus s'ils n'avaient pas été relayés par Martin Gardner, spécialiste de mathématiques récréatives, qui le fait connaître dans la revue Scientific American à partir de 1975.

L'essentiel des éléments de contexte ci-dessus proviennent de la page Wikipédia consacrée à Kaprekar (voir Bibliographie). Notre activité porte sur l'algorithme et la constante de Kaprekar, malgré son intitulé choisi par souci de simplicité.

3. Réponses attendues

On note avec une simple flèche (. → .) le passage d'un nombre au suivant dans le processus.

1. Prenons 4432.

2. On place les chiffres de 4432 (4, 4, 3 et 2) dans l'ordre décroissant pour avoir le plus grand nombre qui s'écrit avec quatre chiffres : c'est 4432, et dans l'ordre croissant pour avoir le plus petit : c'est 2344. On calcule la différence :

$$4432 \rightarrow 4432 - 2344 = 2088$$

3. On continue le processus à partir de 2088 :

$$4432 \rightarrow 2088 \rightarrow 8820 - 0288 = 8532 \rightarrow 8532 - 2358 = 6174$$

et on constate que 6174 est fixe : $6174 \rightarrow 7641 - 1467 = 6174$.

On place l'énoncé « 6174 est un point fixe pour le processus » dans la case « C'est vrai, j'en suis sûr(e) » car on a immédiatement la preuve en faisant le calcul (il suffit de s'assurer que celui-ci est correct).

Prenons un deuxième exemple, 6287 :

$$6287 \rightarrow 8762 - 2678 = 6084 \rightarrow 8172 \rightarrow 7443 \rightarrow 3996 \rightarrow 6264 \rightarrow 4176 \rightarrow 6174$$

et un troisième, 5413 :

$$5413 \rightarrow 4086 \rightarrow 8172$$

qui termine donc comme 6287.

Aide pour les élèves : on pourra autoriser la calculatrice et les faire travailler en binôme en chargeant l'un des deux de contrôler la saisie de l'autre pour éviter les erreurs de calculs qui risquent d'empêcher de tomber sur 6174 ou de remarquer que ce nombre est fixe.

En se familiarisant avec le processus, on peut énoncer une autre propriété.

On vérifie immédiatement que deux entiers qui s'écrivent avec les mêmes chiffres dans un ordre différent ont la même suite d'images après une étape. On place cet énoncé dans la première case « C'est vrai, j'en suis sûr(e) ».

4. Je remarque que les trois nombres que j'ai choisis tombent tous sur 6174.

À ce stade, on peut poser la question : tombe-t-on toujours sur 6174 ?

5. En mettant tous les exemples en commun, de deux choses l'une :

   a) soit on remarque qu'ils tombent tous sur 6174. Comme il y en a un nombre important :

   On conjecture que tous les nombres à quatre chiffres tombent sur 6174, c'est-à-dire on place cet énoncé dans la case « Cela me semble vrai ».

Cette conjecture, bien qu'assez raisonnable, va s'avérer fausse, voir le 2e cas ;

b) soit on a essayé un multiple de 1111, par exemple 1111 lui-même :

$$1111 \rightarrow 1111 - 1111 = 0 \rightarrow 0000 - 0 = 0$$

et 0 est lui aussi un point fixe. On a cependant un nombre important d'exemples à quatre chiffres non tous égaux qui tombent tous, eux, sur 6174.

On peut tout de même conjecturer que tous les nombres à quatre chiffres non tous égaux tombent sur 6174, c'est-à-dire placer cet énoncé dans la case « Cela me semble vrai ».

4. Variantes

Les zéros. Il y a une certaine imprécision dans les consignes données au début, qui apparaît par exemple en appliquant le processus au nombre 1000, puisqu'on obtient alors un nombre à trois chiffres :

$$1000 \rightarrow 1000 - 0001 = 999$$

Que fait-on ? Si on applique la même règle que précédemment pour ce nombre à trois chiffres, on obtient 999 − 999 = 0, ce qui produit un nouveau cas particulier par rapport à ceux qu'on a trouvés ci-dessus ; si au contraire on décide de rester dans le domaine des nombres à quatre chiffres, l'ensemble des entiers compris entre 1000 et 9999, on ajoute le chiffre 0 à gauche du résultat trouvé, dont l'image est alors :

$$0999 \rightarrow 9990 - 0999 = 8991 \rightarrow 8082 \rightarrow 8532 \rightarrow 6174$$

Avec ce choix, 1000 suit la règle générale.

D'après Wikipédia (voir Bibliographie), Kaprekar suivait une règle encore plus stricte, il éliminait tous les zéros au moment de prendre le plus grand et le plus petit nombre qu'on peut écrire avec les chiffres donnés, si bien que :

$$1000 \rightarrow 1 - 1 = 0$$

Il faut faire un choix, qui semble assez arbitraire ; peut-être le fait de ne pas créer de nouvelles exceptions en conservant le même nombre de chiffres à chaque étape est-il à privilégier pour faire découvrir la conjecture et tenter ensuite de la prouver ? C'est le choix qu'on conserve ici.

Nombres à deux chiffres. On est partis d'un nombre à quatre chiffres comme dans la version initiale de Kaprekar. On peut tout aussi bien appliquer le processus aux nombres à deux ou trois chiffres. On voit un phénomène intéressant se produire à deux chiffres :

$$37 \rightarrow 36 \rightarrow 27 \rightarrow 45 \rightarrow 9 \rightarrow 90 - 09 = 81 \rightarrow 63 \rightarrow 27 \rightarrow \ldots$$

Ici on ne tombe pas sur un point fixe dans le cas général (il n'y a que 0 !), mais sur une boucle qui se répète à l'infini :

$$81 \to 63 \to 27 \to 45 \to 9 \to 81 \qquad (1)$$

On conjecture que tous les nombres à deux chiffres distincts tombent sur la boucle (1). On place (temporairement) cet énoncé dans la 2e case du tableau.

L'avantage est qu'on peut assez facilement prouver la conjecture, par exemple avec un peu de calcul littéral : tous les nombres à deux chiffres s'écrivent sous la forme 10a+b avec $1 \leq a \leq 9$ et $0 \leq b \leq 9$ donc

$$(10a + b) - (10b + a) = 9(a - b)$$

est, si $a > b$, un multiple > 0 de 9 à au plus deux chiffres ; il suffit donc d'étudier les images des entiers de la « table de 9 ». Or ils sont tous, à l'ordre près de leurs chiffres, dans la boucle (1). On peut aussi utiliser le critère de divisibilité par 9 : deux nombres qui s'écrivent avec les mêmes chiffres ont la même somme des chiffres, à laquelle ils sont congrus modulo 9, donc leur différence est congrue à 0 modulo 9, c'est-à-dire divisible par 9.

On peut maintenant remonter l'énoncé ci-dessus en 1re case du tableau.

Nombres à trois chiffres. Pour les nombres à trois chiffres, on retrouve un point fixe qui est 495, les exceptions à la règle (qui est de tomber sur le point fixe) sont les multiples de 111.

On conjecture que les entiers à trois chiffres non tous égaux tombent sur 495.

On pourrait envisager une preuve par ordinateur menant un calcul exhaustif pour tous les entiers à trois chiffres. Ou on généralise l'argument ci-dessus :

$$(100a + 10b + c) - (100c + 10b + a) = 99(a - c)$$

donc il suffit de vérifier la propriété pour les multiples de 99 à trois chiffres : 099, 198, 297, 396, 495 et leurs « symétriques » 594, 693, 792, 891 et 990. On vérifie que :

$$990 \to 891 \to 792 \to 693 \to 594$$

On peut maintenant remonter l'énoncé ci-dessus en 1re case du tableau.

COMMENT CALCULER $\sqrt{2}$ EN FAISANT DU DÉCOUPAGE

Gilles DAMAMME
Maître de conférences, UNIVERSITE DE CAEN-NORMANDIE
LMNO
gilles.damamme@unicaen.fr

Résumé
Le but de cet atelier est de trouver une bonne approximation de $\sqrt{2}$ uniquement avec des découpages et quelques additions, sans utiliser la calculatrice.
Plus précisément, il s'agit de retrouver une démarche inspirée de l'algorithme d'Euclide.

INTRODUCTION

1. But de l'atelier

Le but de l'atelier était de trouver une bonne approximation de $\sqrt{2}$ uniquement avec des découpages et quelques additions, sans utiliser la calculatrice.

Mais il s'agissait aussi de retrouver une démarche inspirée par l'algorithme d'Euclide et qu'ont probablement fait les Grecs durant l'Antiquité (avec autre chose que du papier...).

Cette activité a été expérimentée deux années de suite avec des étudiants de L3 en histoire des mathématiques où elle servait de préliminaire à l'étude du texte d'Euclide sur l'incommensurabilité du côté d'un carré et de sa diagonale mais l'activité proposée peut tout à fait être adaptée pour des élèves de seconde ou troisième.

2. Expérimentation avec des étudiants

J'ai rappelé aux étudiants que le rapport de la longueur d'une feuille de format A3 (resp. A2, A1, A4 etc.) sur sa largeur est $\sqrt{2}$ et leur ai proposé d'effectuer l'algorithme d'Euclide à partir de deux bandes de papier, l'une de la taille de la longueur d'une feuille de format A3 et l'autre de la taille de la largeur, et de former par découpage des bandes de papier de plus en plus petites jusqu'à ce que l'une de ces bandes puisse (à peu près) mesurer la bande précédente et par suite toutes les autres bandes de papier. En appelant « unité » la mesure de cette plus petite bande et en remontant ensuite on peut calculer combien la largeur d'une feuille de format A3 mesure d'unités et combien la longueur de la feuille de format A3 mesure d'unités. En effectuant alors le rapport des deux entiers obtenus, on obtient une approximation de $\sqrt{2}$.

Cette activité a bien fonctionné les 2 années et les étudiants ont souvent trouvé de bonnes approximations de $\sqrt{2}$ (voir annexe) en général différentes selon les groupes de travail (les étudiants travaillaient par deux ou trois). Par contre, il ne leur apparaissait pas en faisant cette activité que $\sqrt{2}$ pouvait être irrationnel (même s'ils connaissaient déjà ce résultat). Néanmoins la 2e année, en confrontant les résultats de chaque

groupe au tableau, certains étudiants ont remarqué une certaine régularité dans le nombre de bandes obtenues par découpages successifs et cela m'a permis quelques semaines plus tard de faire le parallèle avec le développement en fraction continue de $\sqrt{2}$ quand les fractions continues ont été évoquées en cours.

3. L'ATELIER DE TALENCE

1. Présentation

Pour l'atelier de Talence, c'était sensiblement la même activité que pour les étudiants de Licence 3 qui était proposée aux participants de l'atelier, à la différence qu'elle ne servait pas d'introduction à l'étude du texte d'Euclide. Suivaient deux autres activités, l'une de partage, et une autre de réflexion sur la réutilisation de l'activité avec sa propre classe. Voici la feuille qui était distribuée aux participants de l'atelier :

Activité 1 :

Prendre une feuille A3 et plier un côté de la feuille sur un côté perpendiculaire de façon à former un pli représentant la diagonale d'un carré de côté la largeur de la feuille A3.

Mesurer avec une bande de papier cette diagonale et comparer la longueur de la feuille A3 : Que remarque-t-on ?

On note A la longueur de la feuille A3 et B sa largeur : on découpe à l'aide de ciseaux sur deux feuilles A3 une bande de longueur A et une autre de longueur B.

À la bande de longueur A, on retranche autant de fois que possible la longueur B : on obtient ainsi une bande de longueur C et on réitère l'opération, la plus petite bande étant retranchée à chaque fois de la plus grande.

On continue ainsi de suite en notant à chaque fois les étapes jusqu'à ce qu'on obtienne une bande de papier qui mesure (éventuellement approximativement) la bande précédente.

On appelle "unité" le morceau final de bande lorsque qu'on arrête l'itération.

Combien d'unités mesure la longueur A (la diagonale d'un carré de côté B) et combien d'unités mesure la largeur B ?

En déduire une approximation de $\sqrt{2}$.

Remarque : on peut faire aussi l'activité avec une feuille A4, A2 et A1.

Activité 2 :

Partage des résultats et commentaires

A partir du partage précédent, quelles conjectures pouvez-vous faire ?

Peut-on trouver des triplets pythagoriciens où l'on ait deux fois le même entier ?

Activité 3 :

Comment adapter l'activité 1 à sa propre classe ? Préliminaires, notations, prolongement, etc.

2. Déroulement des activités

Comme c'était suggéré, les participants se sont regroupés en groupes de 2 ou 3 pour faire l'activité qui s'est bien déroulée, les participants obtenant des bonnes approximations de $\sqrt{2}$. Là encore, pendant le partage, il n'y a pas eu d'indices relevés aiguillant vers une **conjecture** de l'irrationalité de $\sqrt{2}$. En effet, celle-ci est loin d'être évidente. Néanmoins, quand on fait une confrontation des différents résultats, on aboutit souvent à des approximations par des rationnels différents, ce qui peut laisser penser que $\sqrt{2}$ n'est pas un rationnel précis, sinon on finirait par régulièrement tomber dessus. De plus, si on commence à observer les résultats obtenus par découpage, on s'aperçoit à partir du découpage de B par C (comme sur les deux copies montrées en exemple, mais ce n'était pas le cas sur toutes les copies…), que le découpage en deux morceaux (plus un reste) semble récurent. En fait, plus on fait un découpage précis avec une feuille de plus en plus grande, plus cette régularité va apparaître et laisser conjecturer qu'elle peut se prolonger indéfiniment. Si les Grecs ne connaissaient pas les développements en fraction continue (ils apparaîtront 20 siècles après Euclide…) qui permettent d'aboutir à l'irrationalité de $\sqrt{2}$, ils possédaient des arguments géométriques (voir par exemple l'article de François Boucher cité en biographie, page 67) pour montrer que cet algorithme ne se termine pas et montrer l'irrationalité de $\sqrt{2}$, ou plutôt l'incommensurabilité du coté d'un carré et de sa diagonale. Néanmoins la preuve présentée dans les Eléments ne s'appuie pas sur ce genre d'argument.

Certains participants ont envisagé de faire cette activité avec leur propre classe. Il est à souligner à ce propos que lorsqu'on présente cette activité au collège (par exemple après l'étude du théorème de Pythagore) le fait que les élèves ne connaissent pas l'irrationalité de $\sqrt{2}$ leur donne un regard neuf sur cette question. Par contre il semble utile de faire une activité préliminaire pour montrer que le rapport de la longueur d'une feuille de format A3 sur sa largeur est $\sqrt{2}$. On peut par exemple par pliage faire coïncider la diagonale d'un carré construit à partir de la largeur d'une feuille A3 avec la longueur d'une autre feuille A3 pour « vérifier » que les mesures sont les mêmes et utiliser ensuite le théorème de Pythagore.

3. Conclusion

Le but de l'atelier était de calculer une approximation de $\sqrt{2}$ sans utiliser la calculatrice mais aussi sans utiliser le double décimètre ou un instrument de mesure graduée. À travers cette démarche on aborde une approche différente de $\sqrt{2}$, on introduit une dimension historique et on s'interroge sur la manière dont l'auteur (ou les auteurs) des Eléments pratiquaient le calcul. En effet les Éléments d'Euclide commencent par la géométrie et ensuite seulement on fait de l'arithmétique, et lorsqu'on fait de l'arithmétique, les nombres sont représentés par des lignes, ce qui laisse à penser que les Grecs alliaient probablement la géométrie et la pratique de calcul. Dans cet état d'esprit on peut à l'aide de la même pratique de découpage, calculer le PGCD de deux nombres en utilisant l'algorithme d'Euclide (en définissant au préalable une unité) : cette activité peut servir de préliminaires à celle présentée lors de l'atelier (à condition bien sûr de pouvoir disposer du temps pour faire ces activités).

III - BIBLIOGRAPHIE

Boucher François, Au fil des maths 551. *Petite enquête sur être ou ne pas être un rationnel, p65-70*

Euclide, Eléments. *Proposition 67, Livre X.*

IV - ANNEXE : COPIES ÉTUDIANTS, PHOTO

Exemples de productions d'étudiants :

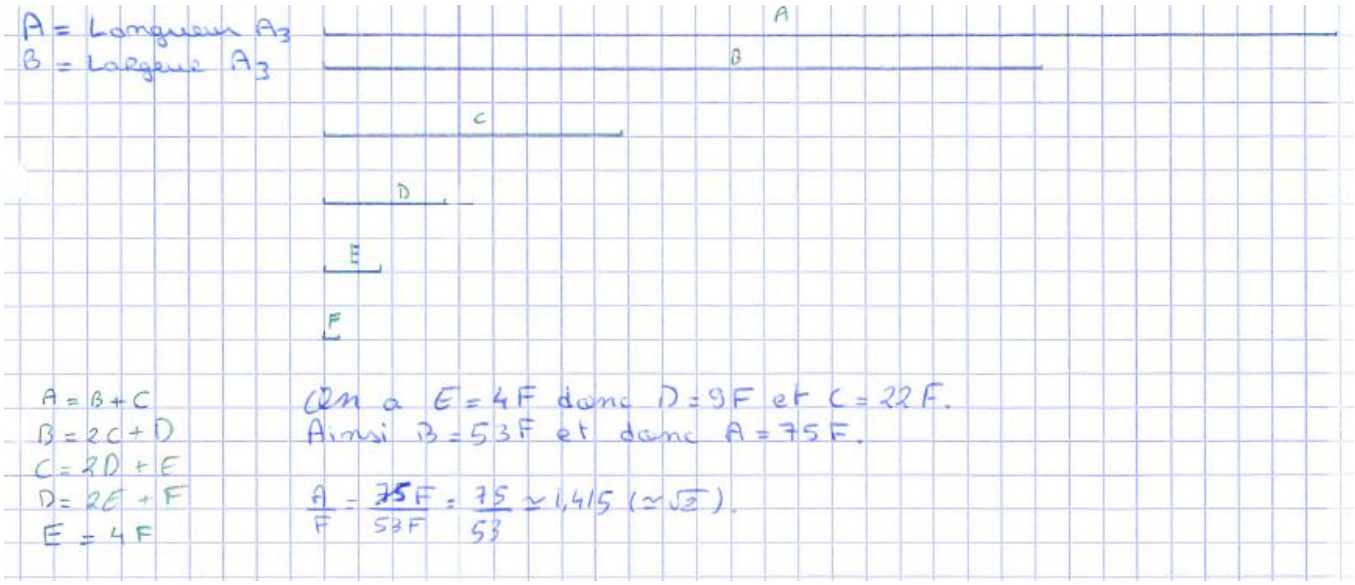


Figure 1. Copie 1

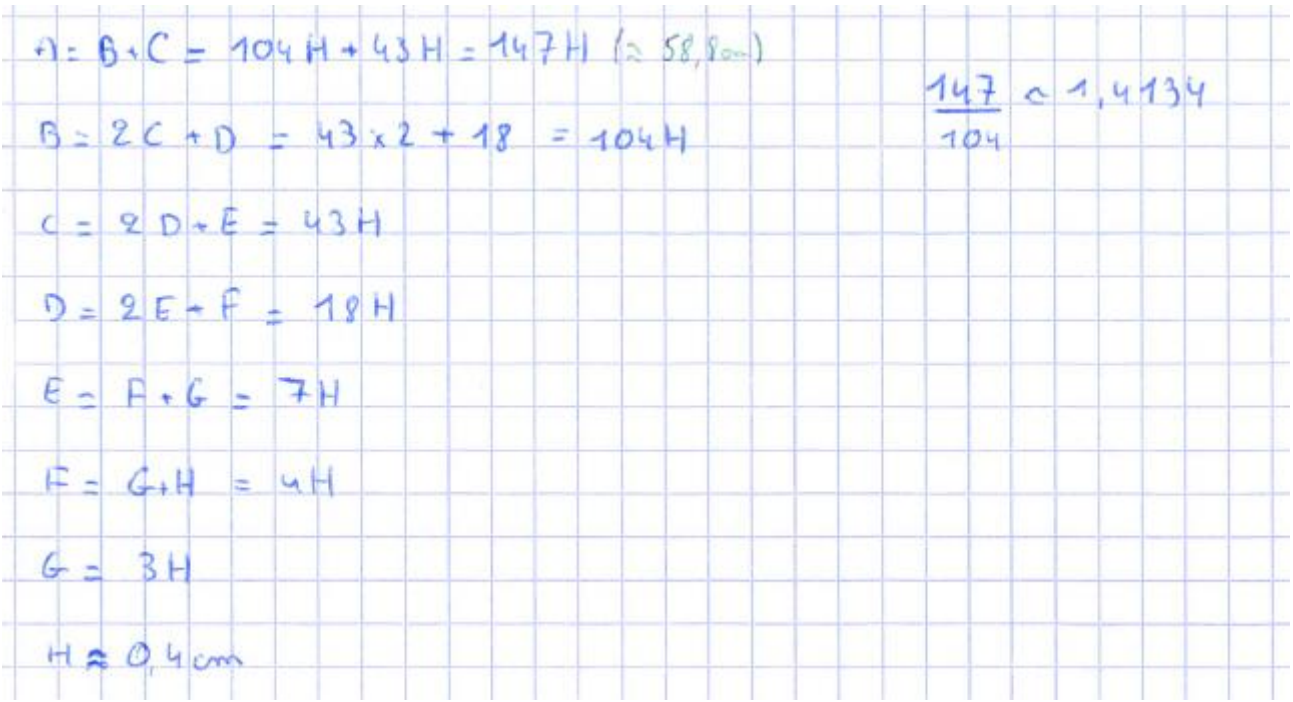


Figure 2. Copie 2

Figure 3. Étudiants lors de l'activité

LE PUZZLE DE LA DIVISION EUCLIDIENNE

Fabrice VANDEBROUCK
Université Paris Cité
IREMS de Paris
vandebro@u-paris.fr

Sylvie ALORY
Lycée Lafontaine
IREMS de Paris
alory.sylvie@free.fr

Benoît MARIOU
Université Paris 8
IREMS de Paris
benoit.mariou@univ-paris8.fr

Résumé
Dans plusieurs classes de terminale et plusieurs TD en L1 d'animateurs de notre groupe IREM, nous avons proposé aux élèves/étudiants de refaire la preuve de l'existence et l'unicité du couple (q, r) d'entiers tel que $a = bq + r$ et $0 \leq r < b$. Cette preuve est difficile. Les élèves/étudiants l'avaient déjà plus ou moins vue en classe selon les cas. Les modalités pour refaire la preuve étaient différentes (en groupe en classe ou bien en autonomie pendant un contrôle) mais il s'agissait toujours de remettre en ordre 15 arguments donnés en vrac. Que ce soit au secondaire ou au supérieur, l'exercice n'a pas été facile et il a mis à jour des difficultés des élèves/étudiants pour raisonner : mélange des arguments de l'existence et de l'unicité, difficultés d'enchainer plus de deux pas successifs du raisonnement, gestion et place de l'introduction des variables… Dans l'atelier, après avoir revu rapidement la preuve et fait une analyse *a priori* des difficultés attendues, on a donné à analyser une sélection de copies des élèves et des étudiants pour mettre à jour ces difficultés effectives à raisonner. Ce sont ces analyses qui sont relatées dans ce texte. Au-delà de cette preuve particulière, la modalité puzzle est une façon de faire raisonner les élèves sur des preuves dans les programmes du secondaire, avec diverses exploitations qui peuvent être faites en classe et des bénéfices pour les élèves. Un autre exemple de puzzle pour la classe de seconde est proposé à la fin de ce texte en ouverture. D'autres modalités sur d'autres preuves d'arithmétique ont été montrées en fin d'atelier – théorème de Bézout notamment - comme des vidéos des élèves eux-mêmes (faites à la maison avec leur smartphone) en train de faire la preuve et de l'expliquer en même temps, ces vidéos pouvant être réinterrogées en classe entière ou pas par le professeur.

Le groupe GLU de l'IREMS de l'université Paris Cité travaille depuis deux ans sur la démonstration à la liaison lycée-université. Nous rappelons le BO (programme de seconde) :

« *Démontrer est une composante fondamentale de l'activité mathématique. Le programme identifie quelques démonstrations exemplaires, que les élèves découvrent selon des modalités variées : présentation par le professeur, élaboration par les élèves sous la direction du professeur, devoirs à la maison, etc.* ».

Le groupe GLU s'est penché sur le « etc. » du BO. Nous avons cherché à proposer d'autres modalités pour travailler la démonstration.

Au cours de ces deux années de travail, nous avons exploré différentes pistes :

- plan de la démonstration dégagé par le groupe classe puis rédaction de la démonstration en groupe ;
- étude d'une démonstration déjà écrite puis analyse de la structure de la démonstration (travail en binôme) ;
- démonstration faite par les élèves/étudiants sous forme de vidéos ;
- puzzle.

C'est cette dernière modalité, que nous avons appelée puzzle, que nous présentons ici. Nous demandons aux élèves de remettre dans l'ordre le texte d'une démonstration présentée par morceaux sous forme d'un puzzle. Nous proposons d'analyser dans cette communication les productions d'élèves de terminale option maths expertes, ainsi que des copies d'étudiants de L1 informatique sur le puzzle de la preuve de la division euclidienne. Dans la partie 1, nous classifions les erreurs de raisonnements observées dans ces copies. Dans la partie 2 nous fournissons une analyse de la structure de la preuve pour comprendre les difficultés observées par les élèves et les étudiants. Dans la dernière partie, nous fournissons quelques ouvertures sur l'intérêt de cette modalité puzzle dans les classes, ainsi qu'un autre exemple du même type réalisé en classe de seconde.

ÉTUDE DE COPIES D'ÉLÈVES ET D'ÉTUDIANTS

Nous avons proposé l'exercice du puzzle à des élèves de Terminale Spé maths dans l'option maths expertes. L'énoncé fourni aux élèves (le même qu'aux étudiants) est en annexe. La correction et la preuve remise en ordre sont données dans la partie 2. Cette preuve a été faite en classe en cours dialogué avec le professeur en classe de maths expertes au cours de l'année 2021/22. Le professeur a demandé aux élèves de réviser spécifiquement la partie sur la division euclidienne pour l'interrogation portant globalement sur de l'arithmétique. Les copies ont donc été recueillies à l'occasion de l'interrogation. Du côté des étudiants de L1, il s'agit d'une preuve qui a été réalisée pendant le cours magistral en amphi. Les étudiants n'ont pas eu de consigne particulière et le puzzle a été donné comme exercice au cours de l'examen de rattrapage de juin 2022. Les étudiants avaient à réviser le chapitre d'arithmétique (qui reprend le programme de maths expertes mais en approfondissant les congruences), mais aussi un chapitre sur les nombres complexes et le début de l'algèbre linéaire. Nous avons là aussi analysé comme matériel les copies des étudiants.

Lors de l'analyse des copies des élèves de terminale, nous avons repéré un certain nombre d'erreurs qui se répétaient. Nous avons ensuite retrouvé ces mêmes erreurs dans les copies des étudiants. Nous avons classé ces erreurs d'abord en trois catégories à partir des copies des élèves de terminales. Nous décrivons et illustrons dans un premier temps ces trois catégories avec les copies des élèves, puis nous les retrouvons sur les copies des étudiants.

1re catégorie : mélanges d'arguments sur l'existence et l'unicité

Les élèves associent assez bien les deux assertions « On montre l'unicité… » et « Soient (q1,r1) et (q2,r2) deux couples qui vérifient… ». Ils sont sans doute bien habitués en classe de terminale à mener des raisonnements d'unicité en introduisant deux objets qui vérifient la condition d'unicité souhaitée. On s'aperçoit qu'il en est de même pour démarrer la preuve d'existence mais dans une moindre mesure. Ces mélanges (ou pas) sont illustrés par les copies d'élèves ci-dessous.

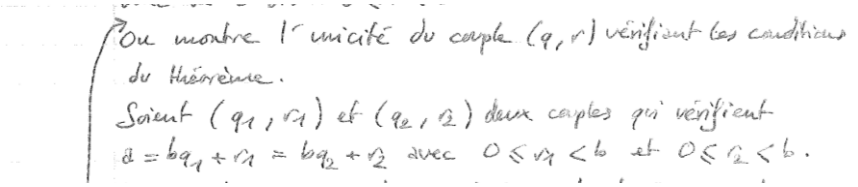

On montre l'unicité du couple (q,r) vérifiant les conditions du théorème.
Soient (q_1,r_1) et (q_2,r_2) deux couples qui vérifient
$a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$.

Figure 1. Extrait de copie d'élève

Dans cette copie (Figure 1), l'unicité est bien introduite.

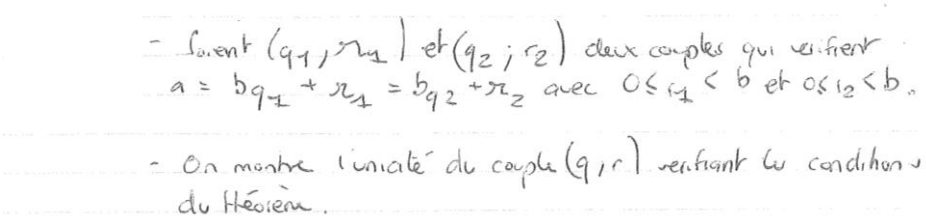

- Soient $(q_1;r_1)$ et $(q_2;r_2)$ deux couples qui vérifient $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$.
- On montre l'unicité du couple (q,r) vérifiant les conditions du théorème.

Figure 2. Extrait de copie d'élève

Dans cette copie (Figure 2), les deux assertions sont inversées mais d'un point de vue sémantique c'est tout à fait acceptable. Il est fréquent dans la vie courante de commencer quelque chose puis aussitôt après (et seulement là) de dire ce qu'on vient d'initier. On trouve la même inversion pour l'existence dans la copie ci-dessous (Figure 3). L'élève a remonté sa phrase « On montre l'existence… », assez haut pour que le lecteur comprenne, mais pas assez haut d'un point de vue de la rédaction usuelle des mathématiques.

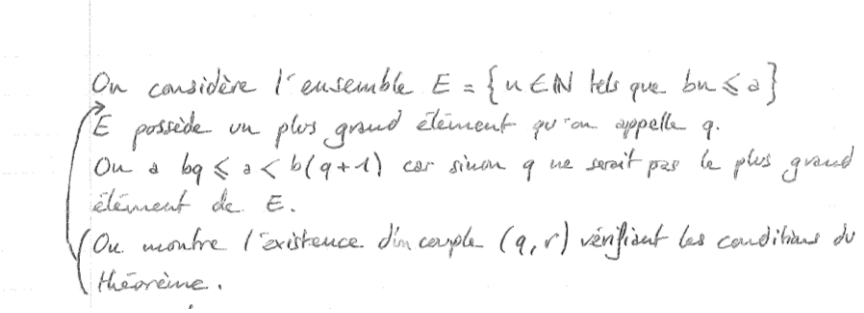

On considère l'ensemble $E = \{n \in \mathbb{N} \text{ tels que } bn \leqslant a\}$
E possède un plus grand élément qu'on appelle q.
On a $bq \leqslant a < b(q+1)$ car sinon q ne serait pas le plus grand élément de E.
On montre l'existence d'un couple (q,r) vérifiant les conditions du théorème.

Figure 3. Extrait de copie d'élève

Dans plusieurs copies on a toutefois des mélanges d'arguments pour l'existence et l'unicité. Soit la preuve de l'unicité est commencée avant que la preuve de l'existence ne soit terminée, soit l'inverse. C'est le cas dans les deux exemples ci-dessous (Figures 4 et 5).

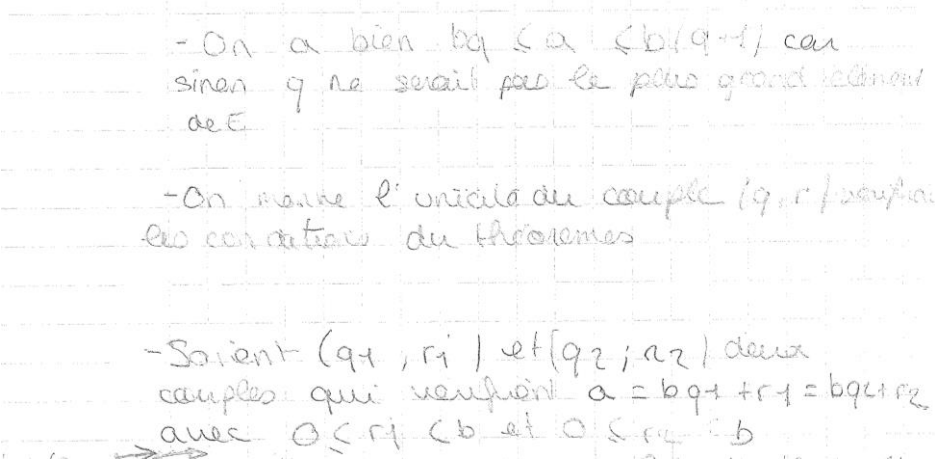


Figure 4. Extrait de copie d'élève

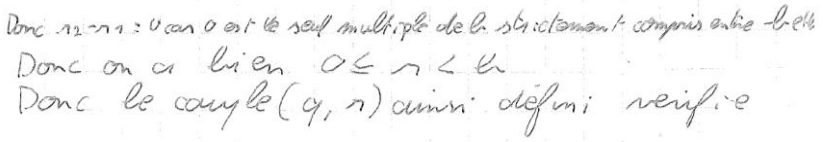


Figure 5. Extrait de copie d'élève

2e catégorie : l'introduction de variables après les avoir utilisées

Dans quelques copies, des objets sont manipulés alors qu'ils ne sont introduits qu'après. C'est faux du point de vue du raisonnement mathématique, mais cette fois cela ne tient pas non plus du point de vue du sens commun. Le lecteur ne peut pas comprendre. On observe surtout cette erreur pour l'introduction de *E*, *q* et *r* dans la preuve de l'existence. En effet, dans la preuve de l'unicité, comme on vient de dire plus haut, les élèves sont sans doute plus habitués à ces types de raisonnement, et les seules variables à introduire sont les deux couples qui sont généralement bien introduits d'emblée.

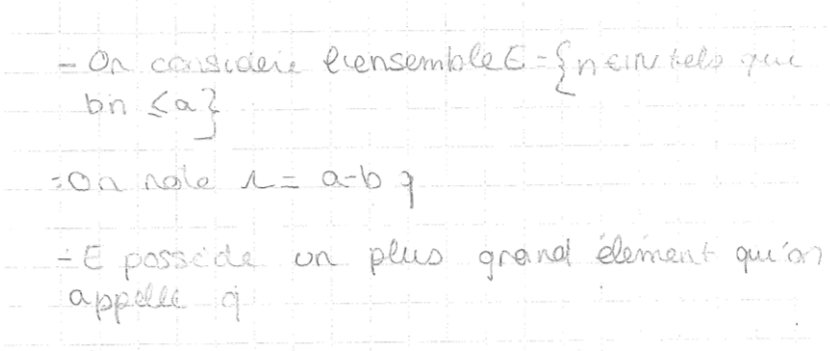


Figure 6. Extrait de copie d'élève

Dans cette copie (Figure 6), l'élève utilise *q* sans l'avoir introduit. On peut penser qu'il ne saisit pas que la phrase « On montre l'existence d'un couple *(q,r)* » n'introduit pas les variables, mais est une simple annonce du raisonnement qui va être développé et dans laquelle les variables sont muettes. Dans la copie suivante (Figure 7), l'élève parle cette fois de *E* sans l'avoir introduit, mais il y a un cumul d'erreurs avec un mélange avec l'unicité (*cf.* catégorie 1).

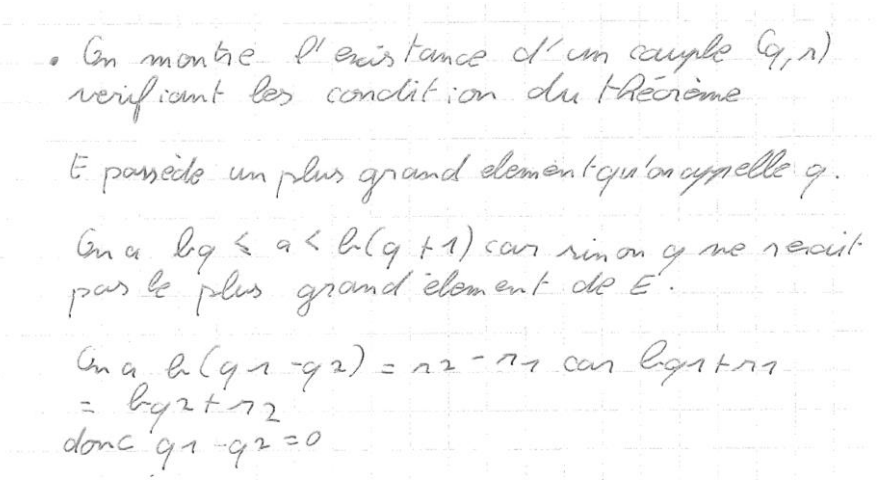


Figure 7. Extrait de copie d'élève ge

3e catégorie : l'enchaînement logique des énoncés

La difficulté est souvent repérée dans l'unicité cette fois. Bien qu'amorcé correctement par beaucoup d'élèves, on voit dans un premier temps que l'enchaînement « $b(q_1-q_2)=r_2-r_1$ » donc « r_2-r_1 est un multiple de b », donc « $r_2-r_1=0$ » est souvent mal fait. On donne trois exemples ci-dessous (Figures 8, 9, 10).

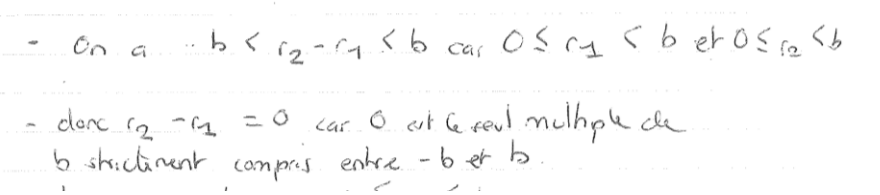


Figure 8. Extrait de copie d'élève

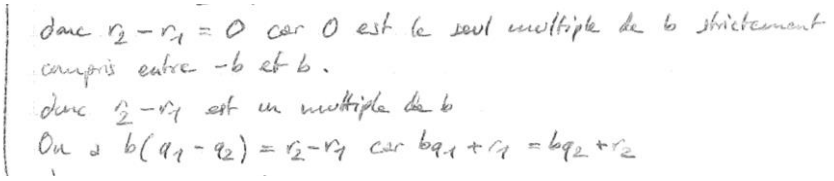


Figure 9. Extrait de copie d'élève

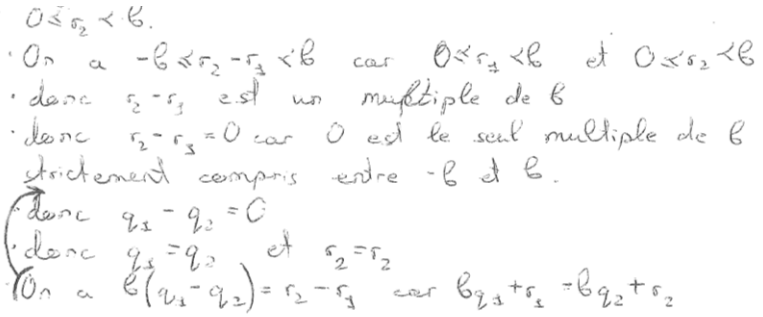


Figure 10. Extrait de copie d'élève

Dans la conclusion de l'unicité, on remarque dans un second temps et très souvent, que les arguments « donc q_1-q_2=0 » et « donc q_1=q_2 et r_1=r_2 » sont inversés. Cette erreur se superpose parfois à la précédente comme dans les deux copies ci-dessous (Figures 11 et 12).

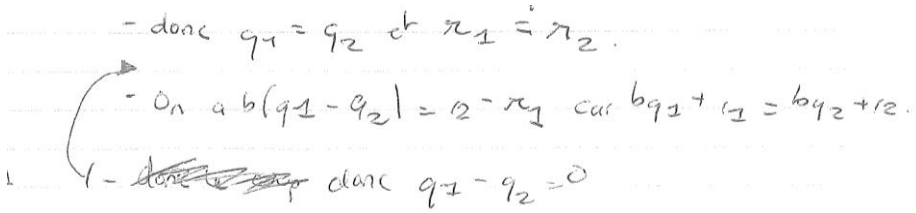


Figure 11. Extrait de copie d'élève

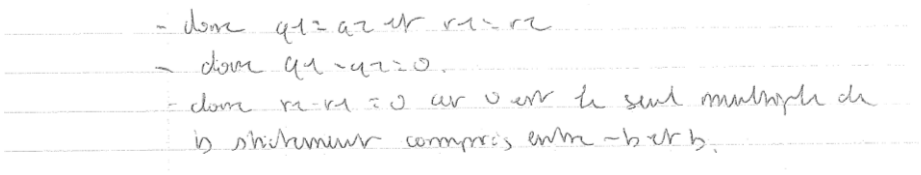


Figure 12. Extrait de copie d'élève

Les mêmes erreurs cumulées et mélangées chez les étudiants

Chez les étudiants (copies A à G), on retrouve les mêmes erreurs, mais souvent cumulées et encore plus mélangées. D'où notre choix initial d'identifier et de catégoriser les erreurs à partir des copies d'élèves qui sont globalement bien meilleures. On propose en exemple deux copies pour illustrer ces erreurs cumulées et mélangées, celle de l'étudiant C (Figure 13) et celle de l'étudiant F (Figure 14).

- Pour la copie de l'étudiant C : entremêlement des preuves d'existence et d'unicité (1re catégorie, inversion entre « donc q_1=q_2 et r_1=r_2 » et « donc q_1=q_2 » et raisonnement pour obtenir « r_2-r_1=0 » incorrect (3e catégorie).
- Pour la copie de l'étudiant F : entremêlement des preuves d'existence et d'unicité (1re catégorie), utilisation de variables q_1, q_2, r_1, r_2 avant de les introduire (2e catégorie et inversion entre « donc q_1=q_2 et r_1=r_2 » et « donc q_1=q_2 » (3e catégorie).

page 4/4

Exercice 1.

1. Soient (q_1, r_1) et (q_2, r_2) deux couples qui vérifient $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$.

2. On considère l'ensemble $E = \{n \in \mathbb{N} \mid bn \leq a\}$

3. E possède un plus grand élément qu'on appelle q.

4. On a $bq \leq a < b(q+1)$ car sinon q ne serait pas le plus grand élément de E.

5. On montre l'unicité du couple (q, r) vérifiant les conditions du théorème.

6. On a $b(q_1 - q_2) = r_2 - r_1$ car $bq_1 + r_1 = bq_2 + r_2$

7. On note $r = a - bq$

8. donc $q_1 = q_2$ et $r_1 = r_2$

9. donc $q_1 - q_2 = 0$

10. On montre l'existence du couple (q, r) vérifiant les conditions du théorème.

11 On a $-b < r_2 - r_1 < b$ car $0 \leq r_1 < b$ et $0 \leq r_2 < b$

12. donc $r_2 - r_1 = 0$ car 0 est le seul multiple de b strictement compris entre $-b$ et b.

13. donc $r_2 - r_1$ est un multiple de b.

14. donc on a bien $0 \leq r < b$

15 donc le couple (q, r) ~~vérifié~~ ainsi défini vérifie $a = bq + r$ et $0 \leq r < b$.

Figure 13. Copie de l'étudiant C

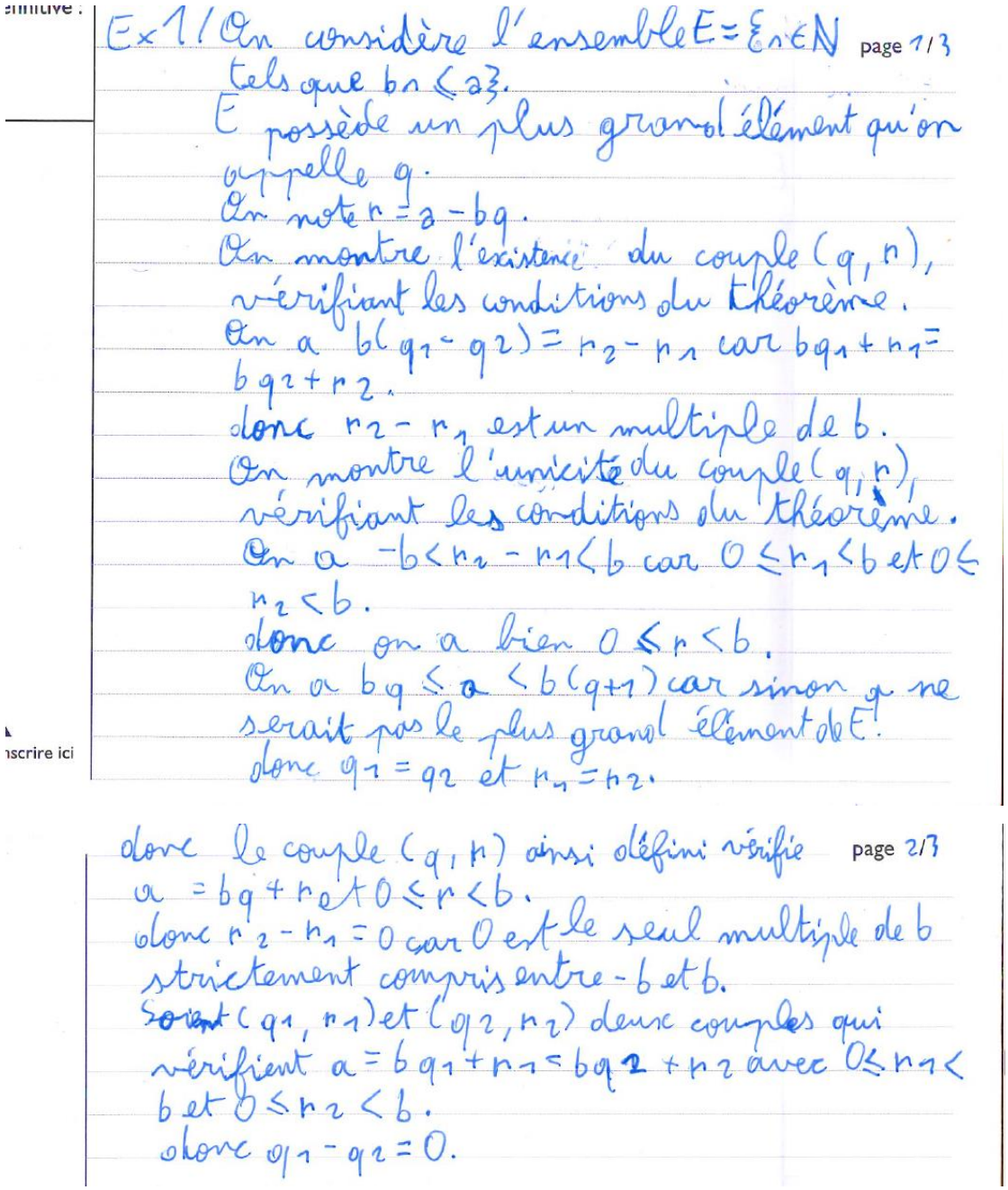


Figure 14. Copie de l'étudiant F

ANALYSE LOGIQUE ET DIDACTIQUE DE LA DÉMONSTRATION

On présente ci-dessous une réponse correcte à l'exercice, afin de pouvoir analyser et commenter la structure de la démonstration qui était à reconstituer. À chaque assertion, on a associé un ou plusieurs commentaires, en respectant le code de style suivant :

- *Italique* : qui relève de l'aide au lecteur et pas, à proprement parler, de l'argumentation.
- Souligné : qui relève des propriétés mathématiques.
- **Gras** : qui relève de l'organisation du raisonnement et des arguments (stratégie de la preuve, introduction des objets, hypothèse temporaire …).

EXISTENCE		
(11)	On montre l'existence d'un couple (q,r) vérifiant les conditions du théorème	*annonce/balise*
(4)	On considère l'ensemble $E = \{ n \in IN \ / bn \leqslant a \}$	**définition/notation**
(13)	E possède un plus grand élément qu'on appelle q.	propriétés de b (non nul), de IN (archimédien) et de E (fini) & **définition/notation**
(14)	On note $r = a - bq$	**définition/notation**
(6)	On a $bq \leqslant a < b(q+1)$ car sinon b ne serait pas le plus grand élément de E	propriété de E
(2)	donc on a bien $0 \leqslant r < b$	calcul
(7)	donc le couple (q,r) ainsi défini vérifie $a = bq + r$ et $0 \leqslant r < b$.	*conclusion/balise*
UNICITÉ		
(10)	On montre l'unicité du couple (q,r)vérifiant les conditions du théorème	*annonce/balise*
(3)	Soient (q_1,r_1) et (q_2,r_2) deux couples qui vérifient $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leqslant r_1, r_2 < b$	**introduction d'éléments génériques & hypothèse temporaire : début de sous-démonstration (indentation)**
(8)	On a $b(q_1 - q_2) = r_2 - r_1$ car $bq_1 + r_1 = bq_2 + r_2$	calcul
(12)	donc $r_2 - r_1$ est un multiple de b	définition de la divisibilité
(1)	On a $-b < r_2 - r_1 < b$ car $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$	calcul
(15)	donc $r_2 - r_1 = 0$ car 0 est le seul multiple de b strictement compris entre $-b$ et b	propriété de la divisibilité
(9)	donc $q_1 - q_2 = 0$	calcul & $b \neq 0$
(5)	donc $q_1 = q_2$ et $r_1 = r_2$	calcul & **fin de la sous-démonstration** & *conclusion/balise*

On a choisi de distinguer les arguments où entrent en jeu les propriétés mathématiques des objets et les assertions qui contribuent à la structure logique et rédactionnelle du texte. Il s'agit d'un découpage qui s'apparente à celui introduit par V. BATTIE, entre dimension opératoire et dimension organisatrice (Battie, 2007 et ce volume d'actes).

Cette distinction est très intéressante dans le cadre de cet exercice de puzzle, qui met l'accent sur l'organisation de la démonstration. Les objets à définir et les calculs à mener sont donnés à l'élève/étudiant, les assertions et les idées sont correctes du point de vue des propriétés mathématiques et pertinentes du point de vue de la démonstration visée. Il n'y a plus qu'à les mettre en ordre !

L'analyse de la structure de la démonstration révèle plusieurs écueils, sources d'erreurs et d'errements compréhensibles dans les réponses des élèves/étudiants. Cela permet de mettre du relief sur les catégories d'erreurs identifiées dans la partie I.

1. La structure globale de la preuve

L'assertion à démontrer est du type *(A et B)*. La démonstration se décompose en deux parties bien distinctes : la preuve de A, la preuve de B.

Dans les copies, les erreurs consistant à mêler des assertions des deux demi-démonstrations pourtant indépendantes, sont assez fréquentes. Ce sont les plus graves dans le sens où, lorsque les démonstrations d'existence et d'unicité sont mélangées, le texte produit est extrêmement difficile à lire et interpréter.

2. La démonstration de l'existence

La démonstration de l'existence ne présente pas de complication, ni arithmétique (exceptée la justification du fait que l'ensemble E est fini – que nous avons occultée), ni stratégique (c'est une démonstration constructive d'existence). La difficulté est d'identifier et d'exhiber les objets appropriés. Dans le cadre de l'exercice, ceux-ci sont donnés.
Cependant, une contrainte de rédaction pèse encore, pas toujours respectée dans les copies : définir et nommer un objet avant de l'utiliser et de le manipuler (4 doit venir avant 13 qui doit précéder 14, par exemple).

On peut penser que le type de l'exercice favorise ce genre d'erreurs : lorsqu'on écrit son propre texte, l'incongruité d'utiliser un objet non défini apparaîtra plus sûrement que lorsqu'on réordonne des phrases déjà écrites par autrui. Comme on l'a déjà signalé plus haut, l'élève peut aussi ne pas comprendre que la phrase 11 est seulement une annonce/balise, donc qu'elle ne fait pas partie à proprement parler du raisonnement, et que les variables citées sont muettes (on aurait pu, du reste, ne pas nommer du tout le couple dans cette assertion). Parler de q et r après cette phrase ne fait donc pas sens, mais pour comprendre cela il faut que l'élève ait bien repéré le statut différent des différentes phrases du puzzle.

3. La démonstration de l'unicité

La démonstration de l'unicité est très différente. L'heuristique est limitée : les objets et les calculs s'imposent d'eux-mêmes (et ils sont donnés dans cet exercice.)

En revanche, l'assertion à prouver, d'une part n'est pas écrite, d'autre part a une forme évoluée. Il s'agit d'une implication, quantifiée universellement sur deux couples.

Il y aurait donc deux sous-démonstrations à ouvrir :

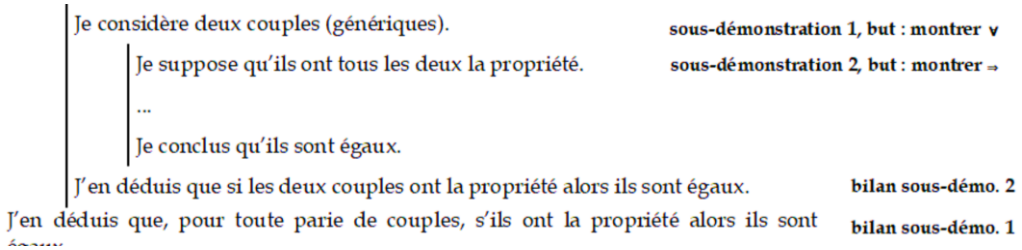


Figure 15. Structure de la preuve de l'unicité

La notion de sous-démonstration souligne qu'on a du matériel supplémentaire (objets génériques, hypothèses) dont on devra se décharger.

Traditionnellement (preuve d'injectivité par exemple), on n'ouvre qu'une sous-démonstration : on se donne des éléments génériques tels que... et on conclut que l'implication est vraie pour tous...

Dans l'exercice, l'assertion 3 correspond à ce début de sous-démonstration, qui se termine par l'assertion 5. Celle-ci ne clôt peut-être pas assez explicitement la démonstration. Notamment, on ne rappelle pas qu'il y avait une implication à prouver et on ne dit pas que le but est atteint ; c'est au lecteur de le remarquer (l'assertion 5 est une balise... implicite !).

Malgré toutes ces difficultés, la structure globale est dans l'ensemble bien restituée dans les copies ; peut-être parce qu'il n'y a pas beaucoup d'alternatives, peut-être parce que ce genre d'assertions est fréquemment traité dans les cours, peut-être aussi parce que cette démonstration a déjà été vue avant l'exercice.

4. Le corps de la preuve de l'unicité

Une dernière difficulté importante est posée par le corps de la preuve d'unicité, les assertions 3-8-12-1-15-9-5. L'assertion 3 pose plusieurs propriétés pour les nombres a, b, q_1, q_2, r_1, r_2. Elles permettent d'obtenir d'une part l'assertion 8 qui donne 12, d'autre part l'assertion 1.
Puis 12 conjointement à 1 permettent d'obtenir 15. Et il faut encore invoquer 8 pour obtenir, avec 15, l'assertion 9. Enfin, 15 et 9 permettent de conclure 5. On a ainsi la structure suivante (Figure 16) :

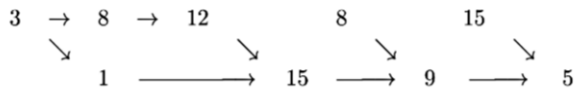


Figure 16. Complexité du raisonnement dans la preuve de l'unicité

Il en résulte une complication sérieuse : aucune des assertions 1, 15, 9, 5 ne découle exclusivement de celle qui la précède immédiatement dans le texte.

Un certain recul sur les propriétés en présence est donc attendu de la part de l'élève/étudiant : ce dernier doit être capable de chercher plus en arrière dans la démonstration les justifications de ces assertions.

L'assertion 8 est particulière : c'est un pas de déduction où on a répété « $bq_1 + r_1 = bq_2 + r_2$ » qui est déjà dans 3 ; initialement pour « aider » les élèves, mais cela a peut-être brouillé leur raisonnement.

Le cas de l'assertion 15 est le plus compliqué : après avoir tiré deux conséquences distinctes de l'hypothèse 3, on doit les considérer conjointement pour utiliser un théorème du type : *si (A et B) alors C*.

Ajoutons que l'assertion 1 pourrait se trouver avant le bloc 8-12 (à quelques majuscules près).

Dans certaines copies, on comprend donc que le paquet 3-8-12-1-15 est agencé de façon malheureuse.

Enfin, une erreur très fréquente consiste à inverser les deux dernières assertions 9 et 5. Le fait, déjà mentionné, que l'assertion 5 n'est pas une conclusion suffisamment explicite entre en jeu. Mais si l'on maîtrise la situation on ne se trompera pas. Et donc, l'erreur peut surtout s'expliquer par le fait que 9 découle directement de 5, tandis que pour conclure 5, 9 doit être associé à 15 (l'assertion 5 est équivalente à la conjonction de 9 et 15). Dans une situation où l'élève/étudiant perd un peu pied, on peut penser qu'il se raccroche à des déductions rassurantes, directes.

III - CONCLUSION ET OUVERTURE

L'exercice proposé en terminale a permis aux élèves de travailler à nouveau cette démonstration assez longue pour eux et qu'ils avaient trouvée difficile en cours. Le format puzzle permet à tous de se mettre à la tâche ce qui n'aurait pas été le cas si nous leur avions demandé de refaire la démonstration. Remettre en ordre les arguments les oblige à porter leur attention sur les articulations logiques. Les erreurs produites ont permis notamment de redire la nécessité d'introduire un objet avant de l'utiliser.

Notre analyse *a posteriori* (partie II) de la structure de la preuve, et plus localement de chacune des phrases, nous a amenés à relativiser la simplicité apparente de l'exercice et à comprendre mieux les erreurs des élèves et étudiants. Dans les prochaines expérimentations de ce puzzle, nous proposerons un autre découpage de sorte à minimiser certaines difficultés observées : par exemple mieux faire identifier aux élèves ce qui relève de balises/annonces et ce qui relève du raisonnement à proprement parler.

À titre d'ouverture nous montrons une modalité de puzzle qui a été proposée à des élèves en classe de seconde. Dans un premier temps, nous avons proposé à un groupe de 16 élèves, sous forme de puzzle, la démonstration de la propriété : *La somme de deux multiples de 7 est un multiple de 7*.

La propriété à démontrer était écrite au tableau sous la forme : « La somme de deux multiples de 7 est un multiple de 7 ».

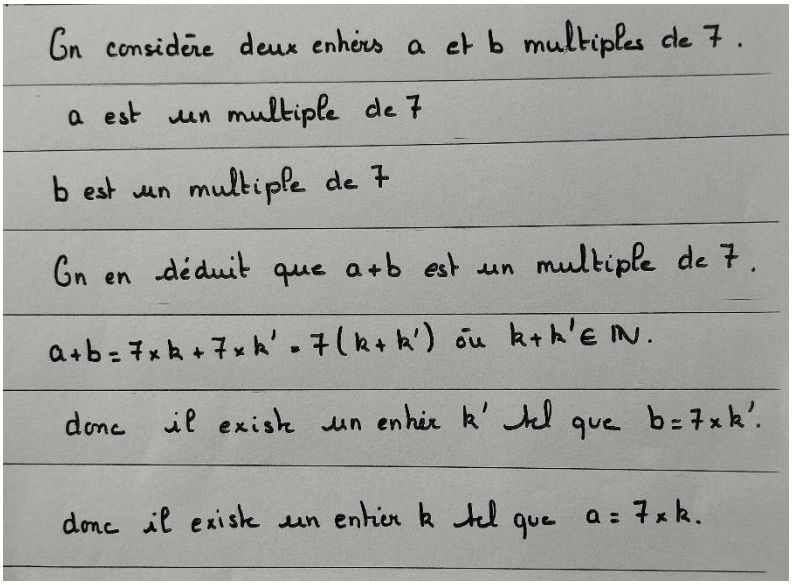


Figure 17. Exemple de puzzle en classe de seconde

Le choix a été fait de distribuer la démonstration dans le désordre et de demander aux élèves de découper les pièces du puzzle et de les remettre dans l'ordre en collant les pièces sur une feuille. Il nous semblait important, pour que les élèves s'impliquent, de ne pas leur demander de recopier dans l'ordre le texte, tâche qui les rebute. Les élèves pouvaient ainsi étaler devant eux les pièces et les bouger facilement jusqu'à ce qu'ils soient satisfaits de l'ordre avant de les coller. Cette modalité (différente de celle proposée en terminale) a permis à tous les élèves de s'impliquer. Le travail des élèves était focalisé sur la tâche principale : remettre en ordre la démonstration. Nous avons veillé à ce que chaque élève relise le texte

qu'il proposait avant de le rendre. Une fois leur puzzle relevé, nous leur avons demandé de faire la démonstration de la propriété : *Soit n un entier naturel. Montrer que la somme de deux multiples de n est un multiple de n.*

D'autres modalités sur d'autres preuves d'arithmétique ont été montrées en fin de notre atelier – théorème de Bézout notamment – comme des vidéos des élèves eux-mêmes (réalisées à la maison avec leur smartphone) en train de faire la preuve et de l'expliquer en même temps ; ces vidéos pouvant être réinterrogées ou non en classe entière par le professeur. Les analyses de ces dispositifs relèveraient d'un autre texte.

BIBLIOGRAPHIE

Battie, V. (2007). Exploitation d'un outil épistémologique pour l'analyse des raisonnements d'élèves confrontés à la résolution de problèmes arithmétiques, *Recherches en didactique des mathématiques*, *27*(1), 9–44

ANNEXE : ÉNONCÉ FOURNI AUX ÉLÈVES ET ÉTUDIANTS

Exercice 1. (4 points)
Dans cet exercice on désire reconstituer la preuve du théorème d'existence et d'unicité de la division euclidienne (voir 1.3 du chapitre d'arithmétique) : Soit a un entier positif et b un entier positif non nul. Alors il existe un couple unique d'entiers (q, r) tel que $a = bq + r$ et $0 \leq r < b$. Reconstituer sur votre copie la preuve en utilisant dans le bon ordre les 15 items suivants (tous doivent être utilisés une seule fois et aucun autre argument n'est nécessaire). On commencera au choix par l'unicité ou par l'existence.

- On a $-b < r_2 - r_1 < b$ car $0 \leq r_1 < b$ et $0 \leq r_2 < b$
- donc on a bien $0 \leq r < b$
- Soient (q_1, r_1) et (q_2, r_2) deux couples qui vérifient $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$.
- On considère l'ensemble $E = \{n \in \mathbb{N} \text{ tels que } bn \leq a\}$
- donc $q_1 = q_2$ et $r_1 = r_2$
- On a $bq \leq a < b(q + 1)$ car sinon q ne serait pas le plus grand élément de E
- donc le couple (q, r) ainsi défini vérifie $a = bq + r$ et $0 \leq r < b$.
- On a $b(q_1 - q_2) = r_2 - r_1$ car $bq_1 + r_1 = bq_2 + r_2$
- donc $q_1 - q_2 = 0$
- On montre l'unicité du couple (q, r) vérifiant les conditions du théorème
- On montre l'existence d'un couple (q, r) vérifiant les conditions du théorème
- donc $r_2 - r_1$ est un multiple de b
- E possède un plus grand élément qu'on appelle q.
- On note $r = a - bq$
- donc $r_2 - r_1 = 0$ car 0 est le seul multiple de b strictement compris entre $-b$ et b

UNE ACTIVITÉ AUTOUR DES NOMBRES DE SOPHIE GERMAIN

Thomas MEYER
Enseignant en lycée, IREM de Grenoble
Thomas.Meyer@ac-grenoble.fr

Résumé
Notre groupe IREM réfléchit à des activités favorisant l'apprentissage de la preuve par les élèves au lycée. Nous présentons ici une expérimentation menée auprès d'élèves de seconde autour d'une situation issue de l'arithmétique.

I - CONTEXTE

1. Notre Groupe IREM

À travers la modélisation et la résolution de problèmes, nous souhaitons permettre aux élèves de construire du sens autour de la notion de preuve en mathématiques. Nous voulons également que les élèves s'interrogent sur la validité de leur(s) solution(s), et donc, sur les arguments donnés pour prouver (Balacheff, 2017). Nous avons également pris le parti de choisir plus particulièrement des problèmes dont la résolution incite à utiliser l'algèbre et pour lesquels l'usage de la technologie est facilitant ou permet de palier à des connaissances qui ne sont pas encore acquises.

1.1. Raisonner, prouver, démontrer, l'apport de la technologie CAS

En mathématiques, la preuve est à la fois un *processus* et un *produit* (Gandit, 2008). C'est un processus qui vise à lever le doute, à valider, à établir la vérité, à convaincre le public concerné (en ce qui nous concerne, la classe), mais aussi à expliquer, tout ceci dans le cadre d'une rationalité propre aux mathématiques. Un travail d'écriture accompagne le processus car la preuve devra être communiquée et devient alors le produit de la résolution du problème. En classe, le processus de preuve a une durée de vie réduite, voire très réduite, et le produit final, la démonstration, est souvent montrée par le professeur (Gandit, 2009). Le programme de seconde (BO spécial n°1 du 22 janvier 2019) donne d'ailleurs une liste de démonstrations et précise que " […] le professeur expose avec précision, présente certaines démonstrations et permet aux élèves d'accéder à l'abstraction." On peut s'interroger sur cette phrase du programme : la présentation d'une démonstration est-elle suffisante pour permettre aux élèves d'accéder à l'abstraction ? On pourrait en effet comprendre qu'il suffirait de présenter la démonstration pour faire comprendre le processus. Ceci s'oppose à de nombreux travaux, comme ceux de Bruner cité par Barth (1985), qui précise : "Il est aussi important d'enseigner à un enfant comment il faut s'y prendre pour résoudre un problème que de lui enseigner le produit de cette résolution." Nous cherchons davantage à faire vivre le processus de preuve plutôt que le produit. En prenant appui sur un logiciel de calcul formel, nous développons ce que Michèle Artigue nomme l'intelligence du calcul (Artigue, 2019), avec ses deux facettes « automatisation et raisonnement. » (ibid.).

Les travaux de ICMI 17 soulignent aussi qu'il existe en général peu de changements dans les pratiques mathématiques par rapport à l'utilisation des systèmes CAS dans des situations papier/crayon, et que les questions liées à l'instrumentation (Rabardel, 1995) sont sous-estimées la plupart du temps. Nous considérons qu'il existe des problèmes que les élèves de seconde peuvent résoudre avec l'aide de la technologie CAS, mais qu'ils ne pourraient pas le faire dans un environnement papier-crayon.

Ainsi pour choisir le problème que nous présentons ci-après, nous avons étudié dans notre analyse a priori l'apport possible de la technologie CAS par rapport à sa résolution. De plus, nous avons pris en considération la genèse instrumentale des artefacts (calculatrices, ordinateurs avec Xcas, *https://www-fourier.univ-grenoble-alpes.fr/~parisse/irem.html*) mis à la disposition des élèves, car nous avons conscience que le processus de transformation d'un artefact en un instrument, c'est-à-dire le processus d'instrumentation, demande du temps.

1.2. Un problème proposé aux élèves

Le théorème selon lequel, pour tout nombre entier naturel a différent de 1, $a^4 + 4$ n'est pas premier, a été énoncé par Sophie Germain[1].

Nous proposons l'énoncé suivant aux élèves de Seconde :

« Pour quelles valeurs de l'entier a, le nombre $a^4 + 4$ est-il premier ? »

Notre analyse a priori est la suivante :

Remarquons que la nature de l'entier a n'est pas précisée. Il est probable que les élèves se restreignent aux entiers naturels. Le questionnement ci-dessous se généralise facilement à tous les entiers relatifs en ajoutant -1 à l'ensemble solution.

Une approche expérimentale possible de cette question consiste à calculer numériquement quelques valeurs de $a^4 + 4$ pour les premiers nombres entiers naturels a. Les résultats de la somme donnent rapidement des nombres supérieurs à 1000, pour lesquels il n'est pas toujours évident de déterminer la primalité (par exemple, $15^4 + 4 = 50629$). L'idée est donc de recourir à l'utilisation de la fonction « isprime » de Xcas ou de rédiger un programme permettant de tester cette primalité. L'utilisation du tableur doit permettre rapidement d'obtenir un très grand nombre de résultats. Ces investigations numériques ne donnant que des nombres qui ne sont pas premiers, on peut en chercher la raison. Il n'est pas évident qu'un élève de seconde pense à faire le lien entre la primalité et sa décomposition en produit de deux facteurs dont un des deux est forcément égal à 1.

Il est également peu probable que les élèves trouvent la factorisation $a^4 + 4 = (a^2 - 2a + 2)(a^2 + 2a + 2)$. Il est important que l'enseignant se demande comment amener les élèves à ce raisonnement.

Nous envisageons les raisonnements suivants :

- Raisonnement par disjonction de cas (a est pair et a est impair)

Cas où ***a* est pair** : certains élèves pourront rédiger une preuve algébrique en écrivant $a = 2p$, p désignant un entier naturel.

[1] *https://hist-math.fr*

$(2p)^4+4 = 4 \times 4\ p^4+4$

$= 4\ (4p^4 + 1)$ sans ou avec l'étape intermédiaire $4 \times 4\ p^4+4 = 16\ p^4 + 4$

Alors, pour tout a pair, il existe un nombre entier naturel p tel qu'on puisse écrire $a^4 + 4$ sous la forme d'un multiple de 4, donc $a^4 + 4$ n'est pas premier.

On peut rencontrer ici une preuve utilisant les résultats connus sur la parité d'une somme ou d'un produit. Il faut alors être vigilant à l'argument « un nombre pair ne peut pas être premier », le contre-exemple à donner étant 2.

Cas où ***a* est impair** : Les élèves vont chercher si $(2p+1)^4+4$ est premier.

Ils pourront vouloir essayer de développer, mais, au-delà de la difficulté d'une telle tâche pour un élève de seconde, il leur sera alors impossible d'arriver à une conclusion en analysant la forme développée, $16p^4+32p^3+24p^2+8p+5$.

Il faudra alors les interroger sur ce qu'ils cherchent à faire. S'ils ont déjà étudié le cas où a est pair, il est envisageable qu'ils répondent que l'objectif est de factoriser, à condition qu'ils aient conjecturé que $a^4 + 4$ n'est pas premier. L'expérimentation numérique, si elle n'a pas encore été faite à ce moment-là, est indispensable pour augmenter le degré de conviction des élèves et leur donner ainsi un but vers lequel diriger leurs calculs. Il convient donc d'engager les élèves dans cette voie plutôt que de leur suggérer immédiatement de factoriser.

Pour la factorisation, il est possible d'utiliser la commande de Xcas qui permet de factoriser. On obtient :

$(2p+1)^4 + 4 = (4p^2+1)\ (4p^2+8p+5)$. Il suffira ensuite d'utiliser que « $4p^2+1 \neq 1$ et $4p^2+8p+5 \neq 1$ » équivaut à

« $(2p+1)^4 + 4$ n'est pas premier ».

Or p désignant un entier naturel, $4p^2+8p+5$ ne peut pas être égal à 1, car c'est forcément un nombre toujours plus grand que 5. Il reste à résoudre, dans l'ensemble des entiers naturels, l'équation $4p^2+1=1$, envisageable dès la classe de Seconde, qui a pour seule solution 0. Ainsi $(2p+1)^4 + 4$ n'est premier que pour $p = 0$, c'est-à-dire que, dans le cas où a est impair, $a^4 + 4$ n'est premier que si $a = 1$.

- Raisonnement à partir du cas général

Cette preuve utilise la factorisation de $a^4 + 4$. Comme mentionné plus haut, cette factorisation passe par l'utilisation du calcul instrumenté au niveau de la classe de Seconde. La façon dont on obtient cette factorisation sans calcul formel n'est d'ailleurs pas à aborder à ce niveau. Comme déjà dit, c'est la reconnaissance de la nécessité de factoriser qui est l'enjeu. Cependant on peut engager les élèves dans la preuve de l'égalité $a^4 + 4 = (a^2 - 2a + 2)\ (a^2 + 2a + 2)$ par développement du second membre.

Concernant la résolution des équations $a^2 - 2a + 2 = 1$ et $a^2 + 2a + 2 = 1$, il peut être envisagé un passage par le registre graphique, la parabole étant un objet connu des élèves de Seconde.

Le nombre a étant positif, le facteur $a^2 + 2a + 2$ est nécessairement différent de 1.

La résolution de l'équation $a^2 - 2a + 2 = 1$ amène 1 comme unique solution, le facteur $a^2 - 2a + 2$ est différent de 1 pour tout nombre a autre que 1.

Ainsi, aucun des deux nombres entiers dont le produit est égal à $a^4 + 4$ n'est égal à 1 pour tout nombre entier naturel a différent de 1. Ceci prouve ce théorème de Sophie Germain.

Une telle preuve n'est pas attendue d'un élève de Seconde, ni même de lycée, s'il ne dispose pas d'un environnement de calcul instrumenté.

Notons qu'il serait également possible d'obtenir la factorisation de $a^4 + 4$ en utilisant l'astuce de deux identités remarquables, en ajoutant et en enlevant $4a^2$, qui correspond à un procédé ad hoc souvent utilisé en mathématiques auquel des élèves de Seconde auront difficilement recours d'eux-mêmes.

- Réflexions complémentaires

Les objectifs poursuivis sont de donner du sens à l'algèbre, en mettant en avant le rôle de celle-ci comme outil de preuve, de travailler le sens du concept de nombre premier (sachant que les nombres premiers jouent un rôle central en cryptologie, mais aussi en calcul exact/formel et dans les codes de correcteurs d'erreurs en communications), de mettre en avant l'aspect expérimental nécessaire à la conjecture et de développer la planification de la preuve en sous-traitant certaines tâches à la machine : calculs numériques avec un tableur ou à l'aide d'un programme, factorisation à l'aide du calcul formel, résolution d'équations avec le calcul formel.

Dans l'énoncé donné aux élèves, le nombre considéré, $a^4 + 4$, est donné dans un registre algébrique. « a » possède le statut de variable dans l'ensemble des entiers.

Les élèves disposent de calculatrices et/ou d'un ordinateur avec un tableur, et une application de calcul formel (Xcas). Nous envisageons le cas où les élèves ne connaissent pas nécessairement le logiciel Xcas. Nous devrons donc leur montrer comment utiliser les commandes utiles, c'est-à-dire « est_premier » (ou « isprime » dans Xcas) et la factorisation, « factoriser » (ou « factor » dans Xcas), en passant par la calculatrice ou l'ordinateur. Nous pensons qu'apprendre à utiliser ces deux commandes, avec une calculatrice ou un ordinateur, peut se faire rapidement dans le cadre d'une séance sans entraver les autres apprentissages visés.

Les élèves sont supposés avoir déjà abordé en classe les nombres premiers et expérimenté un algorithme tel que le crible d'Eratosthène. Ils doivent se rappeler ce que signifie *nombre premier*. Nous nous attendons à ce qu'ils se remémorent qu'un nombre premier est un entier qui n'est divisible que par un et par lui-même. Il faut s'en assurer et si besoin rappeler cette définition. Nous observons que cette définition devrait orienter la pensée des élèves vers les critères de divisibilité et/ou la décomposition d'un nombre en un produit de facteurs. Par ailleurs, les élèves penseront peut-être qu'un nombre pair, hormis deux, n'est pas premier. En revanche, il n'est pas immédiat de savoir si un nombre impair est premier pour de grands nombres, par exemple au-delà de 101. Nous estimons que les élèves devraient pouvoir se souvenir de leurs tables de multiplication de 1 à 10, et qu'ils peuvent connaître les critères de divisibilité jusqu'à onze. Donc, il nous semble intéressant que les élèves puissent utiliser la commande "isprime" ou "est_premier" du logiciel Xcas pour de "grands" nombres afin de pouvoir affirmer qu'un nombre est premier ou non, s'ils ne disposent pas, dans leur calculatrice, d'un programme leur permettant de tester la primalité sans avoir à tâtonner. Mais l'information sur cette commande n'est pas à donner tout de suite aux élèves afin de ne pas influencer leur stratégie et inférer les connaissances qu'ils mettent en œuvre.

Les élèves de Seconde ne savent pas encore résoudre des équations du second degré par la méthode du discriminant, ils doivent se ramener à des équations de type « produit nul », de même pour des équations

de degré supérieur à deux. Ils devront mobiliser des connaissances, comme les identités remarquables, leur permettant de factoriser un polynôme de degré supérieur à un, soit pour résoudre une équation, soit pour donner sa factorisation. La factorisation ne sera pas immédiate car il ne s'agit pas d'une forme usuelle. Pour ce faire, nous envisageons que les élèves se servent de la technologie du calcul formel car la réussite de la factorisation ne fait pas partie de nos objectifs. En revanche, l'identification de la nécessité de la factorisation devrait développer l'intelligence du calcul et contribuer à la construction du sens de la factorisation – bien au-delà du simple travail technique – nécessaire à la résolution du problème et lié au concept de nombre premier, mettant ainsi en évidence les valeurs pragmatique et épistémique de la factorisation.

2. Le stage « MathC2+ » dans l'académie de Grenoble

Conduit dans l'académie depuis plusieurs années, ce stage s'inscrit dans le cadre du programme national MathC2+ porté par la Société Mathématiques de France. Il se déroule au mois de juin, sur trois jours depuis 2022, et est organisé en partenariat avec l'INRIA, l'Université Grenoble Alpes et l'IREM de Grenoble.

Ce stage concerne tous les ans une cinquantaine d'élèves de seconde, venus de toute l'académie, particulièrement motivés par les mathématiques et ayant une appétence pour les sciences. Le fil rouge du stage est la découverte de l'activité de recherche et du métier de chercheur.

II - L'EXPÉRIMENTATION

Dans le cadre du stage MathC2+, quatre problèmes de recherche sont présentés aux stagiaires. Ils ont un premier temps pour s'approprier chacun d'entre eux avant d'en choisir un seul pour lequel ils devront proposer une preuve qui fera l'objet d'une présentation orale devant tous les participants. Il est possible que cette preuve ne soit pas totalement aboutie au moment de la présentation.

Nous restreignons cette présentation au problème présenté plus haut et ne nous étendrons pas sur le rôle des enseignants qui sont intervenus et qui ont eu tout le loisir d'interagir avec les stagiaires.

1. Étude de cas sur des nombres de Sophie Germain

Un tiers des stagiaires ont choisi de travailler sur le problème des nombres de Sophie Germain.

1.1. Organisation de la séquence

La séquence a été partagée en quatre phases. La première a eu lieu le jour de leur arrivée. Après présentation de l'énoncé, les stagiaires ont eu un quart d'heure pour se familiariser avec le problème et clarifier les points qui nécessitaient une reformulation.

Le lendemain, ont eu lieu la deuxième et la troisième phase. Pendant celles-ci, les stagiaires disposaient de quatre heures pour mener leurs recherches et préparer leur présentation orale à l'aide d'un diaporama. Lors de la phase de recherche, les élèves étaient disposés en groupes de trois ou quatre. Le troisième jour, la quatrième phase a eu la forme d'un mini-séminaire durant lequel chaque groupe de stagiaires a présenté le fruit de son travail (recherches et preuves - même partielles) à ses pairs, aux enseignants et aux chercheurs présents.

1.2. Productions d'élèves

- Appropriation et recherche.

Les élèves n'ont pas montré de difficulté pour s'approprier le problème. La recherche a démarré par des essais numériques et la conjecture (C1) « $a^4 + 4$ est premier si et seulement si $a = 1$ » est sortie en quelques minutes (Fig. 1 et Fig. 2).

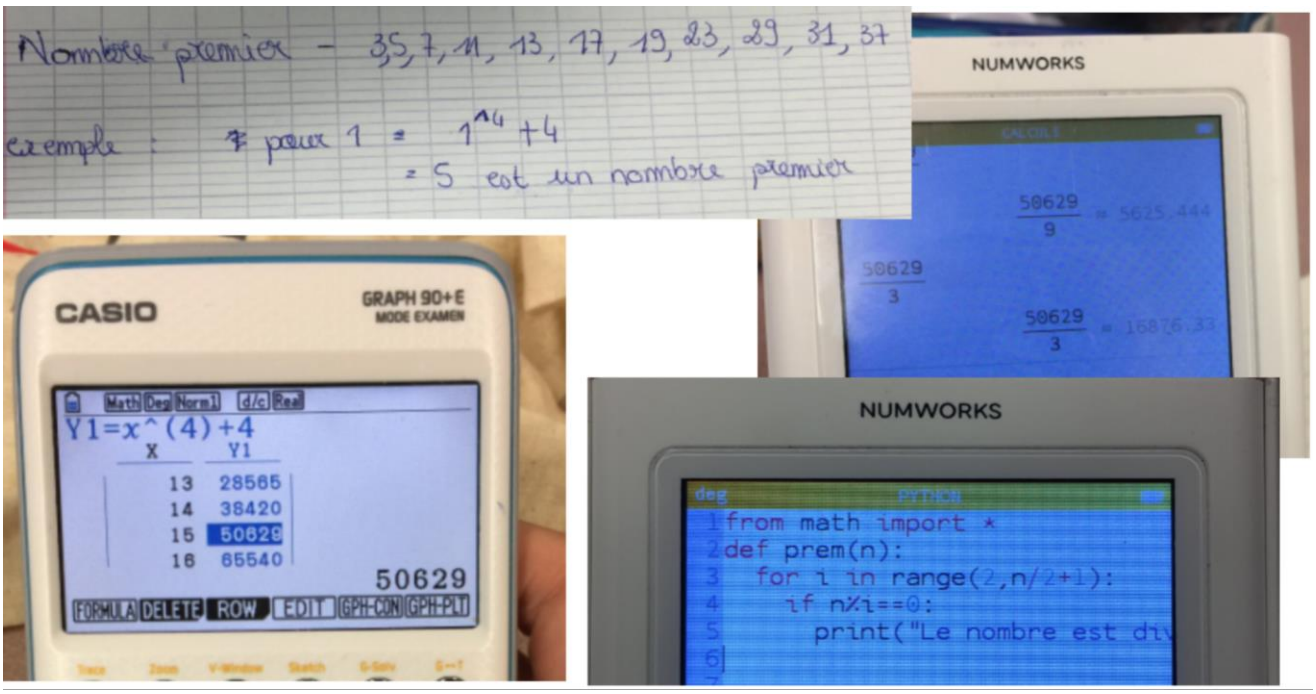


Figure 1. Productions de stagiaires lors de MathC2+

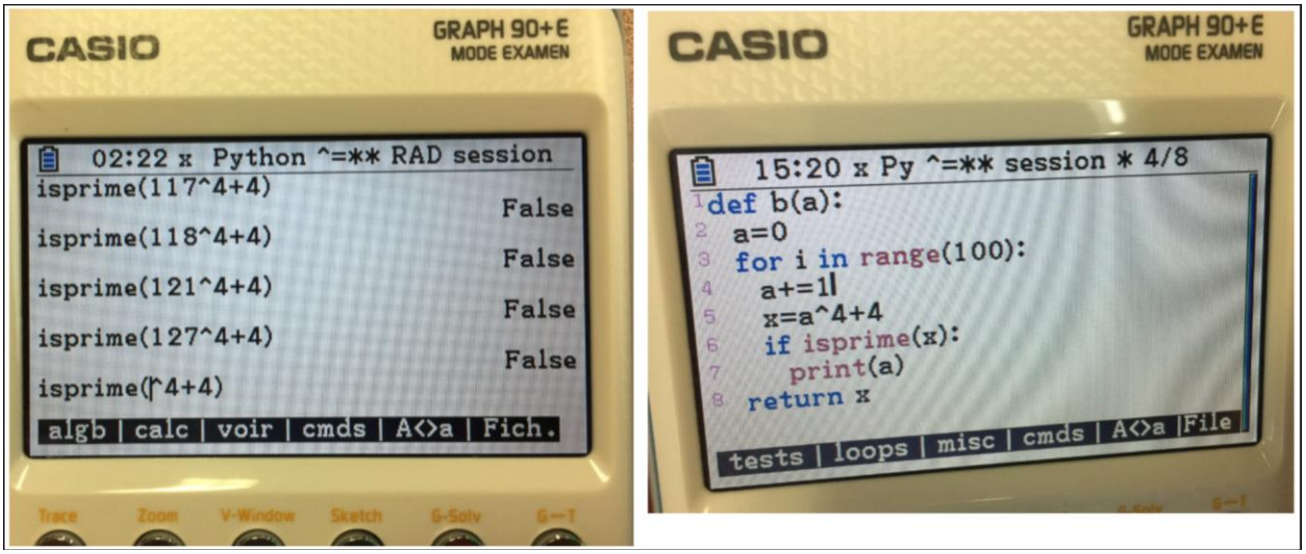


Figure 2. Tests de primalité instrumentés

- Preuves proposées

Le raisonnement par disjonction de cas a émergé rapidement. La preuve du cas « a pair » a été produite rapidement conformément à nos attentes dans l'analyse a priori.

En essayant de traiter le cas « a impair », deux nouvelles conjectures sont apparues : (C2) « Lorsque le chiffre des unités de a est 5, celui de $a^4 + 4$ est 9 » et (C3) « Lorsque le chiffre des unités de a est 1, 3, 7 ou 9, celui de $a^4 + 4$ est 5 ».

Notons que la démonstration de la conjecture (C3) permet d'affirmer que lorsque a est différent de 1, est impair et que son chiffre des unités est 1, 3, 7 ou 9, le nombre $a^4 + 4$ n'est pas premier (car divisible par 5 et supérieur à 5) mais que la démonstration de la conjecture (C2) ne permet pas de déterminer la primalité de $a^4 + 4$ lorsque le chiffre des unités de a est 5.

Les élèves n'ont pas réussi à aller plus loin dans l'élaboration de leur preuve. Le raisonnement à partir du cas général n'a pas été envisagé par les élèves. Par conséquent, les enseignants encadrant l'activité ont décidé d'orienter la recherche de la preuve vers le recours à Xcas afin d'obtenir la factorisation :

$a^4 + 4 = (a^2 - 2a + 2)(a^2 + 2a + 2)$ présentée. Une partie des stagiaires a su s'approprier ce résultat pour aboutir à la preuve algébrique exposée plus haut. D'autres stagiaires ont utilisé Xcas pour factoriser $a^4 + 4$ lorsque a est impair et ont réussi à achever leur preuve par disjonction de cas (Fig.3).

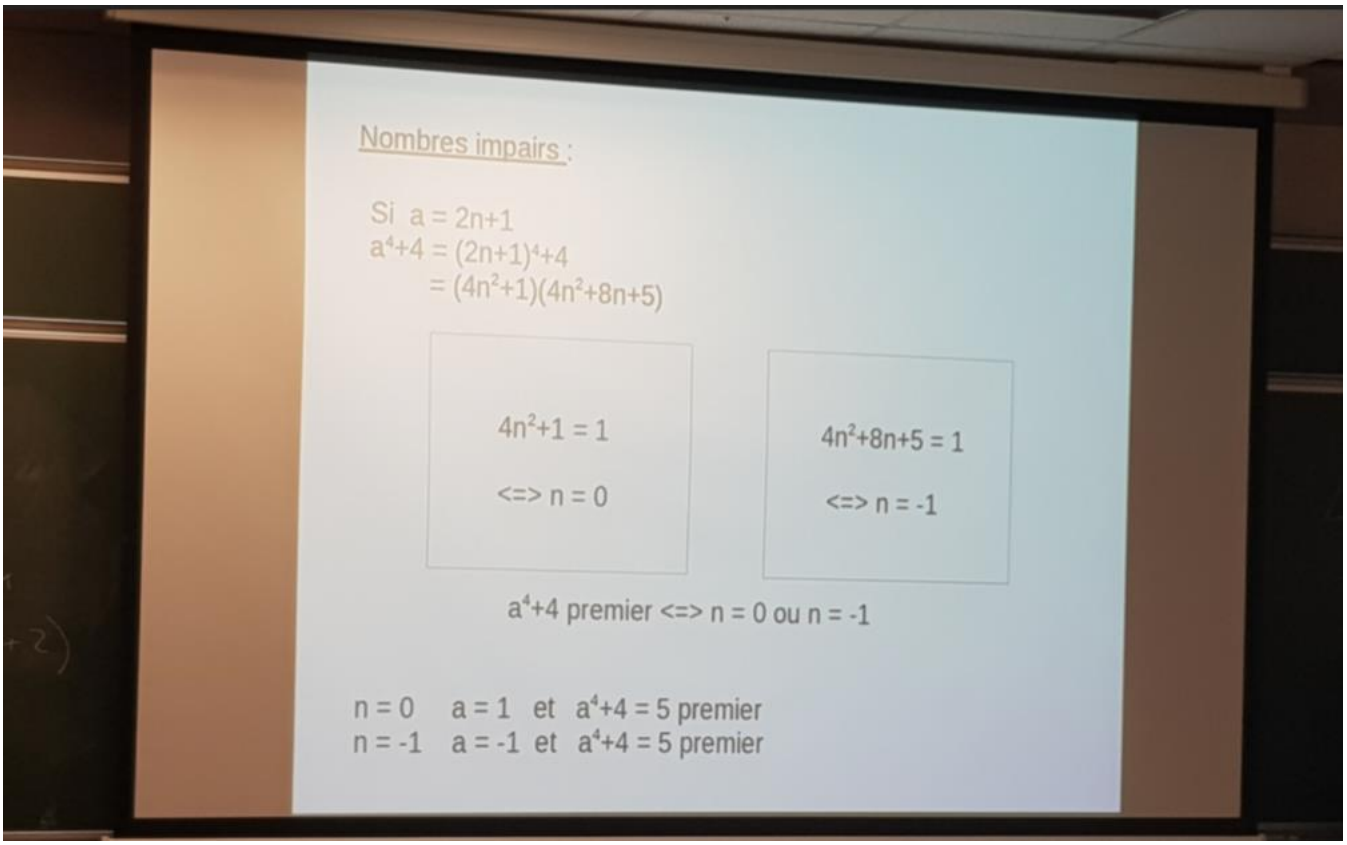


Figure 3. Preuve proposée par un stagiaire pour a impair.

Une fois la preuve rédigée, certains stagiaires ont souhaité se pencher sur la preuve des conjectures (C2) et (C3). Cela a poussé un des enseignants présents à les questionner sur l'écriture générique d'un nombre dont le chiffre des unités est 5 pour essayer de lever le blocage constaté plus haut. Ils ont finalement réussi à démontrer les conjectures (C2) et (C3) (Fig 4.).

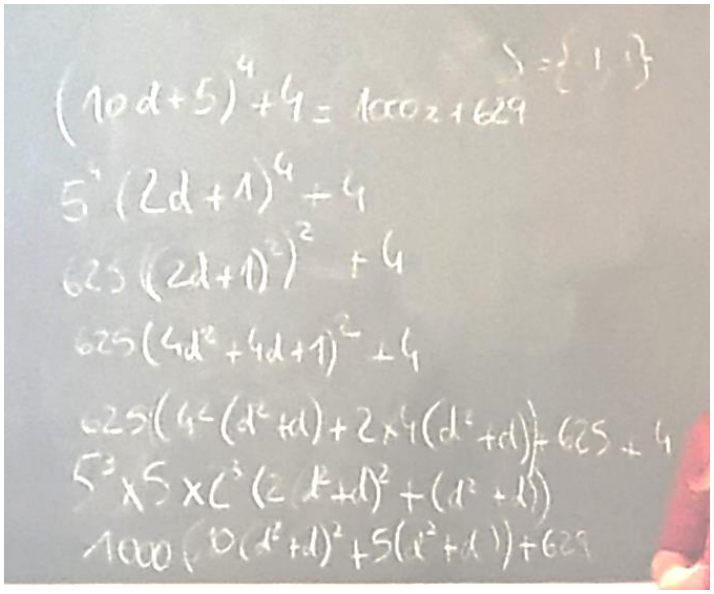


Figure 4. Preuve de la conjecture (C2) proposée par un stagiaire.

2. Analyse

Comme pressenti dans l'analyse a priori, les élèves ont commencé par des essais en utilisant leur calculatrice et ont rapidement formulé une conjecture pertinente pour résoudre le problème proposé. Ils se sont tous lancés dans une preuve pour le cas pair, qu'ils ont su rédiger correctement, puis se sont retrouvés en difficulté pour prouver le cas impair, qui a été un réel blocage. Les enseignants présents ont choisi d'intervenir pour relancer l'activité en repartant sur le cas général avec l'idée d'exploiter la factorisation pour justifier qu'un nombre est premier (Fig. 5). Cette idée n'est pas apparue chez les élèves (ce qui n'est pas surprenant en seconde). La factorisation n'a été utilisée que pour justifier que, lorsque a est pair, $a^4 + 4$ n'est pas premier car il est plus grand que 2 et divisible par 2.

$$p \geqslant 2 \text{ est premier}$$
$$\Longleftrightarrow$$
$$\forall (a,b) \in \mathbb{N}^2, p = ab \Rightarrow (a = 1 \text{ ou } b = 1)$$

Figure 5. Caractérisation de la primalité d'un entier naturel p.

L'intervention des enseignants a permis aux stagiaires de rédiger une preuve, soit en traitant le cas général, soit en se réappropriant la méthode pour traiter le cas « a impair ». Nous supposons que la connaissance des stagiaires sur la notion de primalité a été consolidée. Néanmoins, le contexte du stage n'ayant pas permis la mise en place d'une institutionnalisation des connaissances d'ordre I et II (Sackur et al., 2005), il n'est pas certain que les stagiaires puissent transposer la méthodologie mise en œuvre dans cette preuve (utilisation de la traduction en langage algébrique d'une définition pour effectuer une preuve) dans un autre contexte.

De plus les tâches de développement et de factorisation prennent ici tout leur sens.

III - CONCLUSION

Nous sommes conscients que cette expérimentation a pu être menée dans un contexte très favorable avec un public ayant une image positive des mathématiques et une envie de découvrir le monde de la recherche. Ils étaient de fait motivés pour résoudre le problème (indépendamment de celui-ci). Il nous semble néanmoins que cet énoncé peut être proposé en classe ordinaire de seconde en fin d'année scolaire. En effet, la notion de primalité, abordée dès le collège et retravaillée en seconde, permet aux élèves de s'approprier aisément l'énoncé. De plus, les premiers essais ne posent pas de difficulté majeure et conduisent rapidement à une conjecture pertinente.

Nous avons pu observer une activité mathématique des stagiaires très riche durant les 4 heures d'atelier. Ils ont cherché, conjecturé, prouvé, et ont été amenés à changer de stratégie pour arriver au résultat final. Il est donc nécessaire qu'un enseignant qui souhaiterait proposer cet énoncé à ses élèves prévoit un temps suffisamment long, quitte à envisager d'autres modalités, en demandant par exemple aux élèves de finaliser la rédaction de la preuve dans le cadre d'un devoir en temps libre.

IV - BIBLIOGRAPHIE

Artigue, M. (2019). Intelligence du calcul, Diaporama présenté à la CII-Université, 18 janvier 2019, http://www.univ-irem.fr/IMG/pdf/dijon-artigue.pdf, consulté le 24/08/2020.

Balacheff, N. (2017). Contrôle, preuve et démonstration. Trois régimes de la validation. Séminaire national de didactique des mathématiques, Association pour la recherche en didactique des mathématiques (ARDM), Paris, France, pp.423-456. ⟨hal-02333720⟩

Barth, B.M. (1985). Jérôme Bruner et l'innovation pédagogique. *Communication & langages*, 66(1), 46-58. DOI : https://doi.org/10.3406/colan.1985.3656

Gandit, M. (2009). Il est urgent de repenser l'enseignement de la preuve. In Actes du colloque Espace Mathématique Francophone (EMF) 2009, Groupe de Travail n°3 : Rôle et place de l'arithmétique et de la géométrie dans la formation des élèves et des professeurs. Dakar, 6-10 avril 2009. http://fastef.ucad.sn/EMF2009/Groupes%20de%20travail/GT3/Gandit.pdf

Gandit, M. (2008). *Étude épistémologique et didactique de la preuve en mathématiques et de son enseignement : une ingénierie en formation.* (Doctoral dissertation, Grenoble 1).

Rabardel, P. (1995). *Les hommes et les technologies ; approche cognitive des instruments contemporains*.

Sackur, C., Drouhard, J.-P., Assude, T., Paquelier, Y. et Maurel, M. (2005). L'expérience de la nécessité épistémique. *Recherches en didactique des mathématiques*, 25(1), 57–90.

ENTRÉE DANS LA PREUVE EN ARITHMÉTIQUE : UN EXEMPLE D'USAGE DE LA SITUATION DU PLUS GRAND PRODUIT

Laurianne FOULQUIER
Formatrice en mathématiques, INSPE BORDEAUX
CII Collège, Irem d'Aquitaine
laurianne.foulquier@u-bordeaux.fr

Aurélie ROUX
Formatrice en mathématiques, INSPE CLERMONT AUVERGNE
CII Collège, Irem de Clermont-Ferrand
aurelie.roux@uca.fr

Résumé
En didactique des mathématiques, des recherches variées se sont intéressées aux processus de preuves. Le rôle de l'enseignant dans la mise en œuvre de situations mobilisant la preuve y apparaît toujours comme fondamental. Toutefois, les leviers dont disposent les enseignants pour agir en classe ordinaire sont peu décrits.
Nous nous intéressons aux pratiques de classe favorisant l'émergence de premières preuves dans les activités des élèves. La géométrie pourrait apparaitre comme le domaine privilégié pour mener ce travail, cependant, de nombreux articles montrent les difficultés que peuvent avoir les élèves dans ce domaine, en particulier celle à entrer dans la géométrie théorique liée à la résistance à se détacher des formes et propriétés visuellement reconnues (Duval, 1995). Ainsi, nous nous sommes naturellement tournées vers l'arithmétique que nous jugeons loin d'être incongrue pour développer des activités de preuve.
À travers cet atelier, nous cherchons à présenter des travaux que nous avons conduits dans le cadre d'un master en didactique questionnant les façons d'aménager une entrée progressive des élèves dans les activités de preuve au collège. Pour ce faire, nous proposons un exemple d'exploitation d'une activité qui a déjà fait l'objet de plusieurs publications : le problème du *Plus grand produit* (Artigue (2004), Argaud et al. (2005), Douaire (1999)).
Les participants ont résolu le problème avant d'envisager les procédures possibles d'élèves de cycle 4. Après un échange sur les définitions associées à la notion de preuve, nous avons exposé les travaux de Balacheff proposant une typologie générale des types de preuves. Nous présentons ensuite une séquence d'apprentissage imbriquant des situations d'action, formulation, validation, issues de la *Théorie des Situations Didactiques* (Brousseau, 1998), en appui sur le problème du *Plus grand produit* visant à favoriser l'entrée dans la preuve. Cette séquence a été expérimentée dans plusieurs classes.
Enfin, les participants ont pu analyser des productions d'élèves issues de la situation de validation à l'aide de la typologie présentée.
L'objectif de notre atelier est d'outiller les enseignants afin qu'ils portent un autre regard sur les processus de preuve de leurs élèves.
Dans cet article, nous présentons les différentes parties de l'atelier et nous concluons avec quelques réactions de participants.

I - PRÉSENTATION DU PROBLÈME

1. Choix des énoncés

Le problème choisi est un problème ouvert qui demande un bagage mathématique modeste. Il s'agit, parmi les décompositions additives d'un entier donné, de trouver celle qui a le plus grand produit. Cette situation a fait l'objet de plusieurs publications qui en proposent une analyse *a priori* (Artigue (2004), Argaud et al. (2005), Douaire (1999)).

Voici la suite d'énoncés soumise aux participants :

> **Premier énoncé :**
>
> Je vous donne le nombre 7. Décomposer 7 sous forme d'une somme, effectuer le produit des termes de la somme.
>
> Le nombre 7 peut s'écrire de plusieurs façons comme somme d'entiers, trouver parmi ces sommes celle(s) dont le produit est maximum.
>
> **Deuxième énoncé :**
>
> Trouver la décomposition en somme du nombre 23 correspondant au plus grand produit.
>
> **Énoncé général :**
>
> Parmi les décompositions additives d'un entier donné, trouver celle qui donne le plus grand produit.

Le premier énoncé vise l'appropriation du problème. Le nombre 7 est un petit nombre entier, il permet éventuellement de prouver que le plus grand produit a bien été trouvé puisqu'il est aisé de dresser la liste exhaustive de toutes les décompositions additives de 7. Ce premier exemple peut permettre de constater que la commutativité joue un rôle pour économiser le nombre de décompositions, que les décompositions comprenant des termes 1 ou 0 ne permettent pas de « gagner ».

Dans le deuxième énoncé, le nombre 23 est proposé de façon à ce que certaines observations faites sur le premier exemple puissent être mises à l'épreuve. Le nombre 23 reste encore un petit nombre entier mais suffisamment grand pour ne plus permettre de réaliser rapidement la liste des décompositions additives possibles. 7 est congru à 1 modulo 3 alors que 23 est congru à 2 modulo 3 ; ce qui conduit, comme nous allons le voir plus loin, à des décompositions gagnantes différentes.

2. Résolution mathématique

Intéressons-nous à la résolution mathématique du problème et aux procédures possibles de résolution des élèves.

Soit $n \in \mathbb{N}$ le nombre choisi :

- $si\ n \equiv 0[3], i.e. \exists k \in \mathbb{N}\ tel\ que\ n = 3k\ alors\ la\ décomposition\ cherchée\ est\ 3^k \times 2^0$.
- $si\ n \equiv 1[3], i.e. \exists k \in \mathbb{N}\ tel\ que\ n = 3k + 1\ alors\ la\ décomposition\ cherchée\ est\ 3^{k-1} \times 2^2$ $ou\ encore\ 3^{k-1} \times 4$.
- $si\ n \equiv 2[3], i.e. \exists k \in \mathbb{N}\ tel\ que\ n = 3k + 2\ alors\ la\ décomposition\ cherchée\ est\ 3^k \times 2^1$.

En effet,

- la décomposition additive optimale ne peut pas contenir de zéro car le produit des termes serait nul,
- la décomposition additive optimale ne peut pas contenir de 1 car si l'on ajoute ce 1 à l'un des autres termes, le produit devient supérieur. Pour tout couple d'entiers $(n_1 ; n_2)$, $n_1 \times n_2 \times 1 < n_1 \times (n_2+1)$.
- nous allons maintenant montrer la propriété suivante : tout nombre supérieur ou égal à 5 peut se décomposer en deux termes supérieurs à 1 dont le produit est supérieur à ce nombre.

  Soit n un nombre entier, $n \geq 5, n = (n-2) + 2$, or $2 \times (n-2) = 2n - 4 = n + (n-4)$.
  Or, $(n-4) \geq 0$, donc $n + (n-4) \geq n$.
  De cette propriété, il découle que seuls des termes égaux à 2 ou 3 subsistent. En effet, $4 = 2 + 2$ et $2 \times 2 = 4$.
  Dès que l'on a plus de deux facteurs égaux à 2, comme $2 \times 2 \times 2 = 8$ que $2 + 2 + 2 = 3 + 3$ et que $3 \times 3 = 9 > 8$; chaque trinôme de termes égaux à deux doit être remplacé par un binôme de termes égaux à 3.

La résolution mathématique du problème demande elle aussi un bagage mathématique modeste et accessible des élèves de cycle 4.

3. Procédures de résolution des élèves

Lorsque nous les avons questionnés, les participants ont proposé plusieurs procédures de résolution, nous complétons cette liste avec nos observations dans les classes. Il est naturel de verbaliser une stratégie en prenant appui sur des exemples numériques. On peut donc faire l'hypothèse que les élèves vont faire émerger des stratégies de leurs premiers tests numériques.

- Procédure 1 : faire la liste exhaustive de toutes les décompositions additives possibles. Cette stratégie est rapidement vouée à l'échec car trop coûteuse. En effet, même pour des « petits » nombres entiers, le nombre de décompositions additives possibles est rapidement important.
- Procédure 2 : décomposer le nombre en deux termes. Dans ce cas, la parité du nombre joue un rôle dans la conclusion portée. Si le nombre est pair, le produit obtenu avec deux termes correspond au carré de la moitié du nombre de départ. Si le nombre est impair, le produit obtenu avec deux termes correspond au produit du nombre entier égal à la partie entière de la moitié du nombre et du nombre entier suivant. Cette procédure n'est plus valide pour les entiers supérieurs à 8.
- Procédure 3 : prendre des nombres proches de la moitié pour des décompositions en deux termes, ou du tiers pour des décompositions en 3 termes...
- Procédure 4 : décomposer le nombre en le plus de termes possibles. Cette procédure permet de comprendre qu'il faut exclure la présence de termes égaux à 1 puisque 1 est élément neutre de la multiplication.
- Procédure 5 : décomposer le nombre avec des 2, 3 et 4 sans chercher à rendre maximal le nombre de termes égaux à 3.
- Procédure 6 : décomposer avec le plus de termes égaux à 3 sans terme égal à 1.

II - COMMENT ANALYSER LES PREUVES PRODUITES PAR LES ÉLÈVES ?

1. Qu'appelle-t-on preuve ?

Un échange autour des conceptions des participants a montré la nécessité de s'accorder sur une définition du terme « preuve » et de le distinguer de « démonstration » et « raisonnement ». Il n'y a pas eu consensus au sein des participants. Par ailleurs, des points de vue différents existent également dans les travaux de recherche en didactique des mathématiques. Nous faisons le choix de considérer comme définition celle de Balacheff, à savoir « une explication acceptée par une communauté donnée à un moment donné » conduisant à un débat permettant de définir un système de validation commun aux différents interlocuteurs.
Depuis 2008, les documents officiels distinguent bien deux activités différentes, celles de preuve et de démonstration sans les définir. La question suivante a naturellement émergé parmi les enseignants présents : « Dans nos classes, prend-on encore le temps de travailler de manière explicite la preuve ? ».

2. La typologie de Balacheff

Les travaux de recherche de Balacheff s'intéressent aux processus de preuves et proposent une typologie de celles-ci. Il distingue deux grandes catégories, les preuves pragmatiques qui se situent dans l'action et se manifestent généralement par des théorèmes élèves non prouvés et les preuves intellectuelles nécessitant un changement de posture, exprimant la volonté de considérer les connaissances comme objets de débat et nécessitant une certaine décontextualisation. Le tableau ci-dessous reprend les différents types de preuve issus des travaux de Balacheff :

Preuves pragmatiques	Empirisme naïf	Vérification sur quelques exemples, conjecture possible mais sans remise en question. La question de la validité n'est pas posée.
	Expérience cruciale	Exemples permettant une conjecture sur la relation entre les objets. La question de la généralisation est posée et mise à l'épreuve.
Exemple générique		« Explication des raisons de la validité d'une assertion par la réalisation d'opérations ou de transformations sur un objet présent non pour lui-même mais en tant que représentant caractéristique d'une classe d'individus. »
Preuves intellectuelles	Expérience mentale	Utilisation d'un représentant considéré comme quelconque. La preuve montre une décontextualisation et l'analyse des relations entre les objets.
	Calcul sur les énoncés	Manifestation d'une construction intellectuelle fondée sur des théories. La preuve ne s'appuie pas sur l'expérience.

Pour Balacheff, la transition des preuves pragmatiques vers les preuves intellectuelles se caractérise par une évolution de la manière dont les exemples sont considérés, par la prise de conscience de la nécessité de les manipuler non pas pour eux-mêmes mais comme des représentants génériques d'une classe d'objets. La transition vers une preuve intellectuelle nécessite donc de ne plus rendre compte des actions sur des énoncés isolés mais de pratiquer un calcul sur des énoncés globaux de manière décontextualisée. La typologie proposée n'a pas pour objectif de classer les élèves en fonction des types de preuves qu'ils invoquent mais de chercher à caractériser les activités de ces derniers, les processus de preuve qu'ils mettent en œuvre et d'envisager des pistes possibles pour l'enseignant permettant d'accompagner les élèves pour une autonomie plus grande dans le cadre de la résolution de problèmes. Nous nous intéressons donc naturellement à ces leviers possibles pour l'enseignant.

III - COMMENT ENGAGER LES ÉLÉVES DANS LA PREUVE ? LE CHOIX DU TYPE DE SITUATION D'ENSEIGNEMENT

Afin d'engager les élèves dans des processus de preuve, le choix de la situation d'apprentissage est un élément essentiel. Les travaux de Balacheff s'inscrivent plus globalement dans une théorie socio-constructiviste des apprentissages, la théorie des situations didactiques de Guy Brousseau (1998).

Dans cette théorie, les situations d'action désignent les situations qui permettent aux élèves d'élaborer de nouvelles stratégies et visent à les engager dans la construction de nouvelles « connaissances en actes ». Elles ne rendent pas nécessaire la formulation du modèle utilisé pour résoudre le problème posé.

Les situations de formulation sont des situations dans lesquelles l'action directe est empêchée et cet empêchement engendre la nécessité pour l'élève d'expliciter le modèle implicite de ses actions pour réussir. Cette formulation du modèle peut être de formes différentes : verbale (orale ou écrite), graphique, à destination d'autrui ou pour soi-même, ... Elles visent la construction progressive d'un langage compris de tous, qui « prenne en compte les objets et les relations pertinentes de la situation adéquate » et rend possible l'explicitation des actions et des modèles d'action. Les moyens d'emporter la conviction existent mais restent encore implicites.

Les situations de validation quant à elles s'inscrivent dans une perspective de preuve intellectuelle, elles doivent conduire les élèves à « réviser » leur opinion, remplacer leur théorie fausse par une théorie vraie. Le processus de validation est fondé sur la prise en charge de contradictions potentielles. Les situations de validation comprennent elles-mêmes des phases d'action ou de formulation puisque les élèves doivent encore agir ou formuler de nouvelles stratégies.

Balacheff s'intéresse à la question de la validation des énoncés, non pas du point de vue de leur logique mais de la façon dont les élèves questionnent ce qu'ils sont en train de faire.

Il distingue trois types preuves :

- preuves pour décider (du côté de l'action) ;
- preuves pour convaincre (aspects théoriques : je me suis déjà décidé, je cherche des arguments pour convaincre) ;
- preuves pour comprendre, savoir (du côté de l'axiomatique).

Dans la suite de l'atelier, nous nous intéressons donc à l'effet potentiel de l'articulation de situations d'action, de formulation et de validation sur les processus de preuves conduits par les élèves. Pour cela, nous présentons une séquence conçue en appui sur les travaux de Balacheff et ancrée en *Théorie des situations didactiques*, mise en place en classe de quatrième et exploitant le problème du *Plus grand produit*.

IV - UNE PROPOSITION DE SÉQUENCE

1. Descriptif

Ci-dessous un tableau récapitulant les différentes phases de cette séquence et leur articulation. Durant l'atelier, nous avons échangé avec les participants sur les raisons qui ont motivé nos choix.

<table>
<tr><th colspan="3">Séance 1</th></tr>
<tr><td>Action</td><td>- Dévolution : Présentation du problème pour 7.
- Relance avec le nombre 23.</td><td></td></tr>
<tr><td>Formulation</td><td>En groupe :
« Déterminer la méthode qui permet de trouver le plus grand produit pour n'importe quel nombre de départ. »
« Un membre de votre groupe sera choisi au hasard. Il sera opposé à un autre élève et devra appliquer votre méthode sur un nombre que je choisirai. Le gagnant sera celui qui obtiendra le plus grand produit. »
Duel puis retour en groupe.</td><td>Trois étapes :
- Étape 1, En groupe : se mettre d'accord « Vous devez trouver une méthode qui permet de déterminer pour n'importe quel nombre la ou les sommes qui correspondent au plus grand produit. Tout à l'heure, un membre de votre groupe sera choisi au hasard. Il sera opposé à un autre élève et devra appliquer votre méthode sur un nombre que je vous donnerai. Le gagnant sera celui qui obtiendra le plus grand produit. »
- Étape 2, duels : Un membre de chaque groupe affronte un membre d'un autre groupe.
Le professeur donne à chaque binôme une feuille sur laquelle est inscrit un nombre.
- Étape 3, retour en groupe : suite au duel, retour du représentant du groupe, révision de la procédure si besoin.</td></tr>
<tr><th colspan="3">Séance 2</th></tr>
<tr><td colspan="2">Rappel du problème, distribution de 3 propositions de stratégies.</td><td></td></tr>
<tr><td rowspan="2">Validation</td><td>En groupe : « Pour chacune des stratégies, dire si elle est gagnante à tous les coups. Prouvez votre réponse. »</td><td>« Laisser toutes les pistes que vous avez tentées même si elles n'ont pas abouti. »
Chaque élève reçoit une feuille avec les trois productions à analyser.
Chaque groupe reçoit une seule feuille, collective, de travail.</td></tr>
<tr><td>Débat collectif sur les différents types de preuve.
Institutionnalisation : elle porte sur ce qu'est « prouver en mathématiques ».</td><td></td></tr>
</table>

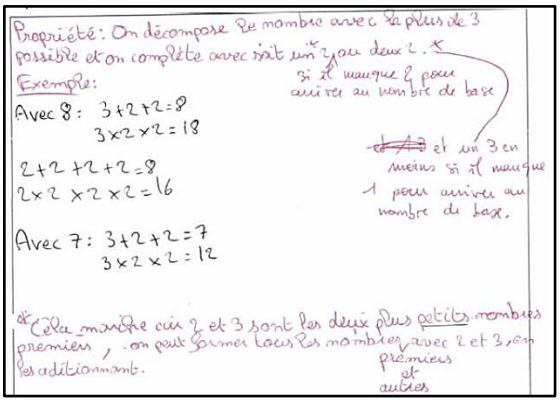
Pour faire progresser les groupes dans la formulation d'une stratégie gagnante, l'enseignant peut jouer sur deux leviers, le choix des binômes constituant les duels (représentants de deux groupes qui ont envisagé des stratégies différentes) et le choix des nombres proposés dans les duels (choix d'un nombre congru à 0, 1 ou 2 modulo 3 selon les stratégies envisagées dans les groupes, de façon à pouvoir réfuter certaines d'entre elles).

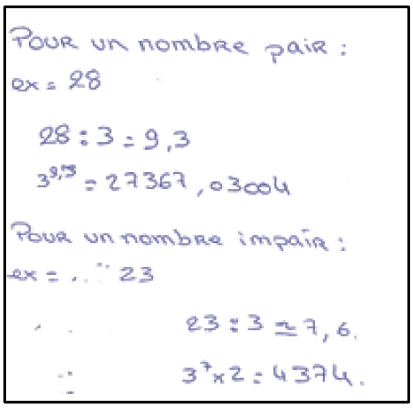
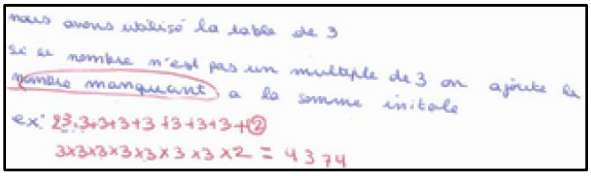
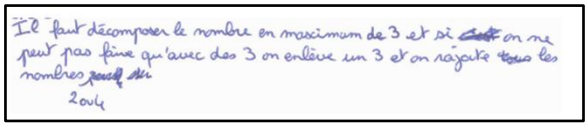
À l'issue de la situation de formulation, l'enseignant analyse les productions de façon à conduire en séance 2 la situation de validation, s'appuyant sur la recherche des méthodes permettant de gagner à coup sûr. La situation de validation inclut une situation de formulation mais également une situation d'action puisqu'on peut jouer de nouveau pour éprouver la validité de la méthode ou pour l'invalider. On vise ici les preuves pour savoir, mais les preuves pour décider et pour convaincre continuent de vivre.

Le débat collectif conduit à l'issue du travail de groupe s'inscrit dans la continuité du travail sur la preuve. Durant la situation de validation, les élèves sont certes amenés à se poser la question de la validité mathématique. Cependant, on n'attend pas d'eux qu'ils soient tous capables d'accéder à cette validation.

2. Comment choisir les productions dont on cherche à assurer la validité ? Exemples

Nous avons soumis aux participants des productions issues de la situation de formulation et avons échangé sur les raisons pour lesquelles nous avons choisi ces productions en particulier. Notre objectif ici est d'éclairer les enseignants sur la façon de sélectionner les stratégies des élèves dont on veut prouver la validité en phase 2. Certains arguments sont retranscrits dans le tableau ci-dessous.

 *Figure 1. Stratégie 1*	Production aboutie : la stratégie est la bonne. Il y a clairement une tentative de preuve, les arguments convoqués, même s'ils sont mathématiques, ne sont pas appropriés, nous la classons dans expérience mentale.

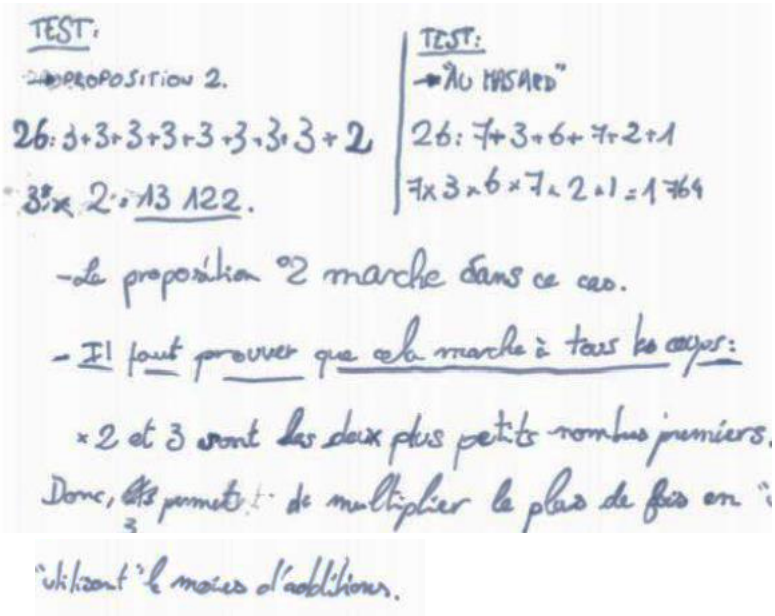
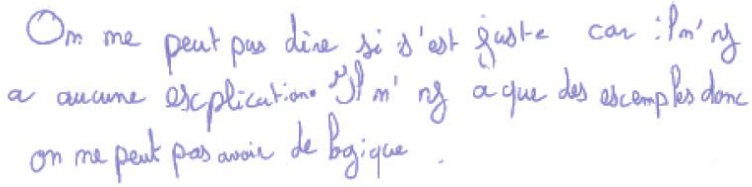
 *Figure 2. Stratégie 2*	Stratégie erronée : les élèves choisissent deux nombres, l'un pair et l'autre impair et proposent deux stratégies différentes selon la parité des nombres. Certes le critère de parité est cité mais aucune transformation des nombres ne montre la généricité des exemples. Les méthodes sont implicites. Les lecteurs doivent analyser les transformations faites sur les nombres de départ pour comprendre la stratégie. Nous considérons que cette preuve est de type empirisme naïf.
 *Figure 3. Stratégie 3*  *Figure 4. Stratégie 4*	Stratégie non aboutie, valide dans certains cas seulement : cette méthode ne fonctionne pas pour les nombres congrus à 1 modulo 3. On note une absence de tentative de preuve par les auteurs de ces formulations.

Bien que ce ne soit pas l'enjeu de la phase de formulation, nous remarquons déjà la présence de premiers types de preuves.

Les stratégies 1 à 4 ont été discutées dans les groupes d'élèves pendant la phase de validation, nous avons alors proposé aux participants d'identifier les types de preuves produits lors de cette situation de validation à l'aide de la typologie présentée. Nous faisons l'hypothèse que ce travail peut faire évoluer le regard porté par les enseignants sur les productions de leurs élèves et leur faire prendre conscience de la nécessité d'analyser les processus de preuve dans la classe.

Voici la consigne donnée aux participants : « Vous trouverez ci-dessous quelques productions d'élèves réalisées dans la situation de validation. Pour chacune de ces productions d'élèves, analysez le type de preuve engagé en appui sur la typologie proposée par Balacheff. »

Nous présentons dans ce tableau les types de preuve que nous associons à ces productions :

Concernant la stratégie 1  *Figure 5. Production 1*	La production 1 montre une réelle volonté de décontextualisation après avoir testé la stratégie sur un exemple dont il est dit qu'il est choisi au hasard. Nous considérons qu'il s'agit d'une preuve de type expérience mentale.
Concernant la stratégie 2  *Figure 6. Production 2*	La production 2 comporte un discours « méta » sur la preuve, évoquant le statut des exemples dans la recherche d'une preuve. Nous envisageons cette preuve comme une preuve de type expérience mentale.
Concernant la stratégie 3	La production 3-A comporte un argument lié à la propriété de la multiplication (existence d'un élément neutre égal à 1). La présence du nombre 26 644 semble montrer une référence implicite à un contre-exemple permettant de réfuter la stratégie 3.

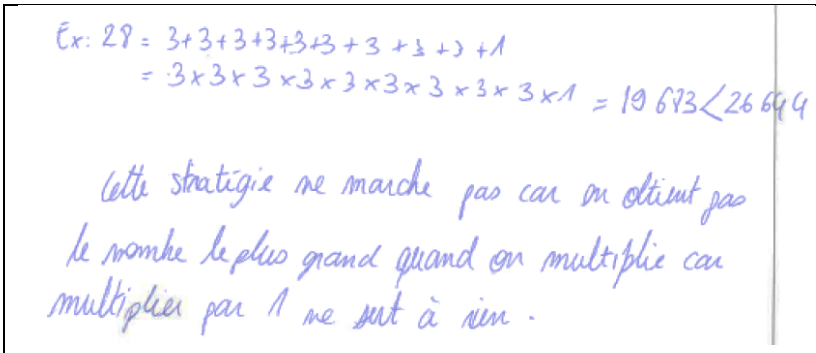


Figure 7. Production 3-A

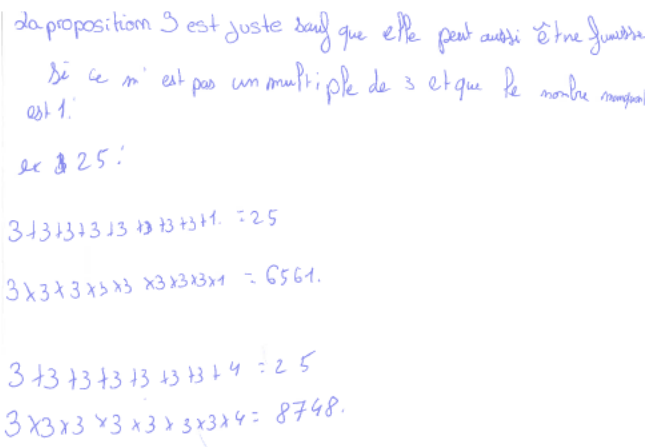


Figure 8. Production 3-B

Cette preuve nous semble relever d'une expérience mentale.

La production 8 met en exergue un contre-exemple bien choisi. Par ailleurs, elle fait référence à une propriété arithmétique des nombres (multiples de 3). Nous l'identifions comme une preuve intellectuelle de type expérience mentale.

Concernant la stratégie 4

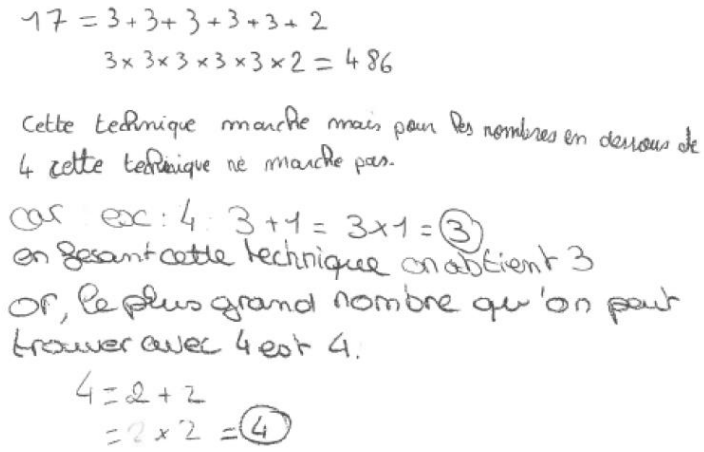


Figure 9. Production 4

La première partie de la production 4 relève davantage d'une preuve empirique de type empirisme naïf. Un seul exemple sur lequel la stratégie 4 est mise en fonctionnement est proposé.

La seconde partie de la production fait référence à un contre-exemple pour des nombres inférieurs à 4. Nous la considérons du type expérience mentale car aucun argument mathématique n'est avancé pour prouver que 4 est bien le plus grand produit pour le nombre 4 choisi au départ.

3. Importance de l'explicitation des connaissances en jeu

À l'issue de cette situation, il est improbable que l'enseignant rencontre la résolution présentée dans le premier paragraphe de cet article mais ce n'est pas l'enjeu. Dans cette séquence, l'institutionnalisation ne porte pas sur la résolution du problème. Elle s'appuie sur les productions d'élèves et les échanges collectifs pour faire émerger des règles de débat et de preuve en mathématiques. Par exemple, elle fait référence à la possibilité d'utiliser un contre-exemple pour prouver qu'une affirmation est fausse, à la nécessité de faire appel à des « propriétés » mathématiques pour prouver qu'une affirmation est vraie, aux différents statuts des exemples dans une preuve. Ce bilan pourra prendre la forme d'une affiche avec une première partie contextualisée prenant en compte les différentes preuves produites par les élèves et une seconde partie décontextualisée mettant en avant quelques règles déjà évoquées plus haut.

Nous avons proposé une trace écrite qui a pu être améliorée grâce aux échanges avec les participants :

Il semble qu'une stratégie permettant de gagner à tous les coups consiste à décomposer en une somme comprenant le maximum de termes égaux à 3 et sans terme égal à 1. Cette stratégie semble fonctionner pour tous les nombres plus grands que 4.

Des arguments pour justifier cette stratégie :

Le nombre 1 ne permet pas d'augmenter le produit obtenu (multiplier un nombre par 1 ne change pas ce nombre).

Si la somme comprend un terme égal à 5, ce nombre 5 peut se décomposer en 3+2. Or, 3 x 2 = 6 et multiplier par 6 donne un résultat plus grand que de multiplier par 5.

Si la somme comprend un terme égal à 6, ce nombre 6 peut se décomposer en 3+3. Or, 3 x 3 = 9 et multiplier par 9 donne un résultat plus grand que de multiplier par 2 x 4 = 8

On peut ainsi répéter ce procédé…

Comment prouver en mathématique ?

Pour montrer qu'une affirmation mathématique est fausse, on peut parfois trouver un contre-exemple.

Pour montrer qu'une affirmation mathématique est vraie, il ne suffit pas de trouver plusieurs exemples qui « fonctionnent bien » c'est-à-dire pour lesquels l'affirmation mathématique est vérifiée.

Pour montrer qu'une affirmation mathématique est vraie, il faut articuler entre elles des propriétés générales et construire un raisonnement valable pour tous les nombres.

V - CONCLUSION

Dans ce travail, nous proposions d'analyser les processus de preuve en utilisant la typologie de Balacheff comme un modèle. Cette dernière a été plus ou moins opérationnelle pour nous car l'analyse des productions montre de fréquentes imbrications entre les types de preuve. Il nous a été nécessaire de prendre des décisions pour classer le travail global de chaque groupe dans un type de preuve. De plus, nous n'avons travaillé qu'avec des productions recueillies en fin de séquence sans noter les évolutions dans le processus de preuve des élèves au cours des séances. Une autre étude aurait pu s'attarder à analyser ces évolutions au fur et à mesure des débats dans les groupes. Cependant, notre travail permet de prendre conscience qu'il existe dans les activités des élèves d'autres preuves que les preuves intellectuelles qui méritent l'attention de l'enseignant. Apprendre à prouver est un travail de longue haleine, il faut donc que les élèves soient placés dès la sixième dans des situations d'apprentissage dont l'objectif est le travail sur la preuve et non celui sur la démonstration.

L'attitude de preuve n'est pas innée, elle s'entretient et se développe. **Un travail plus ambitieux depuis le cycle 3 nous paraît indispensable dans cet objectif.**

BIBLIOGRAPHIE

Argaud, H., Boët, J., & Bouculat, N. (2005). *Apprentissages numériques et résolution de problèmes cours moyen (première année)* (ERMEL). Paris (France) : Hatier.

Artigue, M. (2004). L'enseignement du calcul aujourd'hui : problèmes, défis et perspectives. *Repères IREM*, n° 54, 23-39.

Balacheff, N. (1987b). Processus de preuve et situations de validation. *Educational Studies in Mathematics*, 18(2), 147–176. https://hal.archives-ouvertes.fr/hal-01619264/document

Brousseau, G. (1998). Théorie des situations didactiques. *Didactique des mathématiques* (1970-1990). Grenoble : La Pensée Sauvage

Douaire, J., & Hubert, C. (1999). Vrai ? faux ? on en débat ! de l'argumentation vers la preuve en mathématiques au cycle 3. *Didactiques des disciplines*. Paris (France) : INRP, Institut national de recherche pédagogique.

Margolinas, C. (2003). Un point de vue didactique sur la place du langagier dans les pratiques d'enseignement des mathématiques. *Construction des connaissances et langage dans les disciplines d'enseignement*. Bordeaux (France),1-17.

VI - ANNEXE : DOCUMENT DISTRIBUÉ AUX PARTICIPANTS

Aux pages suivantes, se trouve le document papier distribué à chaque participant de l'atelier.

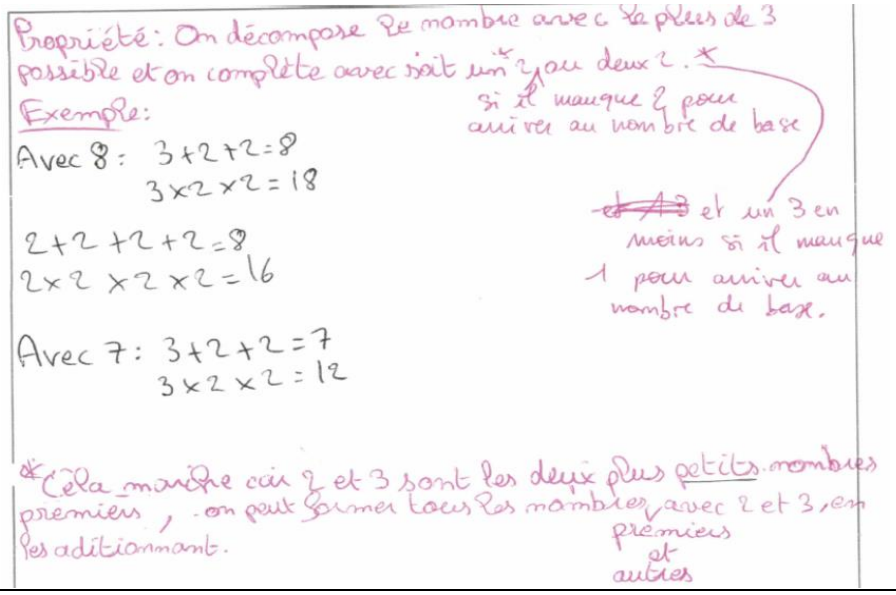
Atelier « Entrée dans la preuve en arithmétique : un exemple d'usage de la situation du plus grand produit »

Rappel : Les élèves sont en groupe. Chaque groupe a rédigé une méthode censée permettre de trouver le plus grand produit pour n'importe quel nombre de départ entier. L'enseignant a récupéré les productions et en a choisi certaines pour construire l'énoncé distribué aux élèves dans la situation de validation.

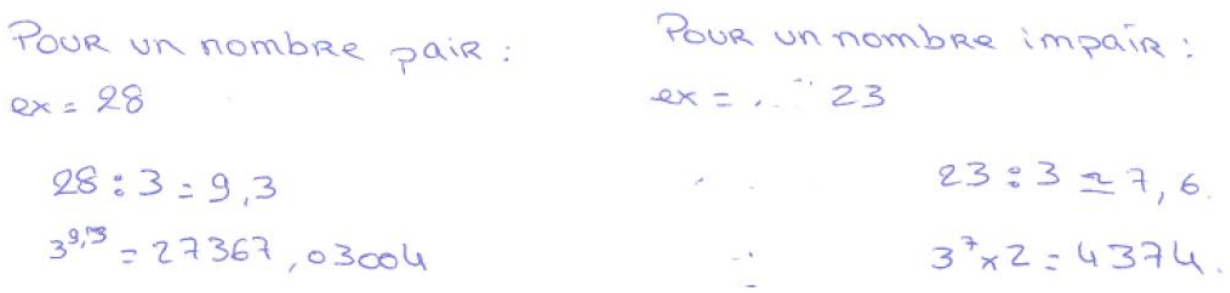
Consigne distribuée aux élèves dans la situation de validation :

« Pour chacune de ces propositions de stratégies gagnantes faites dans la classe, dire si elle est gagnante à tous les coups. Prouver votre réponse. Laisser toutes les pistes que vous avez tentées même si elles n'ont pas abouti. »

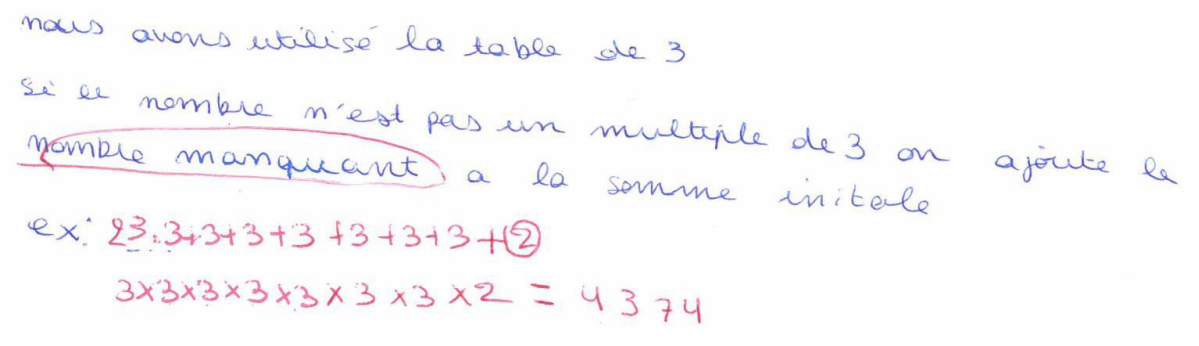
Stratégie 1



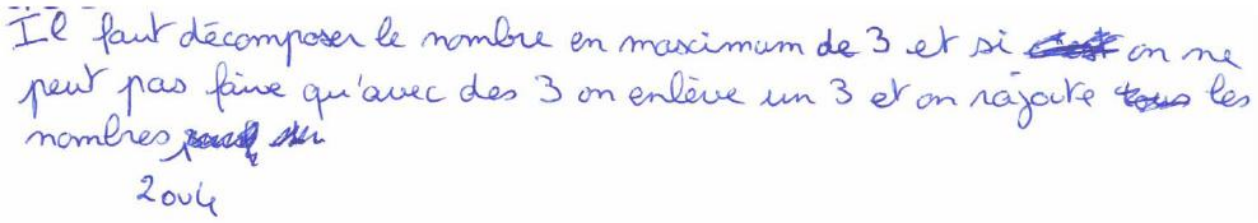
Stratégie 2



Stratégie 3



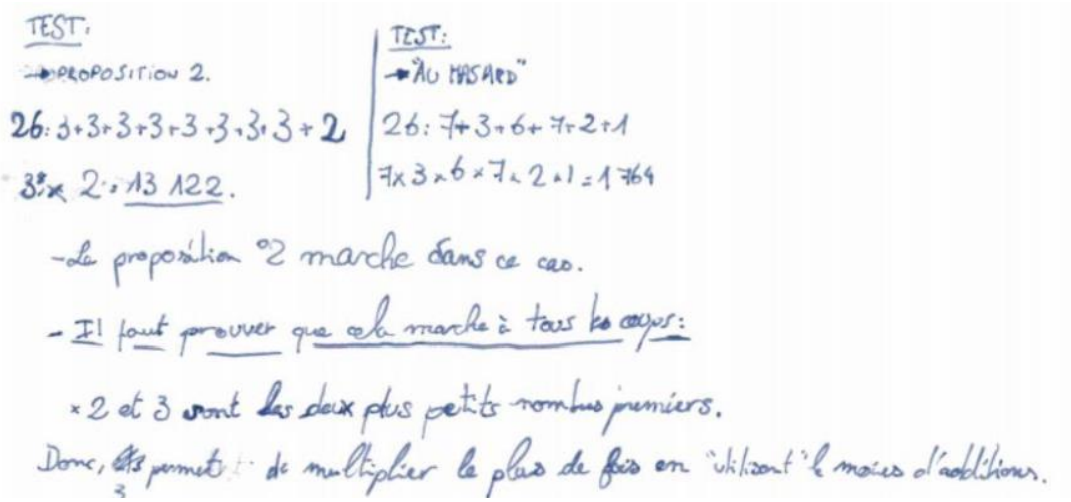
Stratégie 4



Vous trouverez ci-dessous quelques productions d'élèves réalisées dans la situation de validation.

Consigne : Pour chacune de ces productions d'élève, analyser le type de preuve engagé en appui sur la typologie proposée par Balacheff.

Concernant la stratégie 1



Concernant la stratégie 2

On ne peut pas dire si c'est juste car : On n'y a aucune explication. Il n'y a que des exemples donc on ne peut pas avoir de logique.

Concernant la stratégie 3

Production 3-A

Ex: 29 = 3+3+3+3+3+3+3+3+3+1
= 3×3×3×3×3×3×3×3×3×1 = 19 683 < 26 644

Cette stratégie ne marche pas car on obtient pas le nombre le plus grand quand on multiplie car multiplier par 1 ne sert à rien.

Production 3-B

La proposition 3 est juste sauf que elle peut aussi être fausse. Si ce n'est pas un multiple de 3 et que le nombre manquant est 1.

ex : 25 :

3+3+3+3+3+3+3+3+1. = 25

3×3×3×3×3×3×3×3×1 = 6561.

3+3+3+3+3+3+3+4 = 25

3×3×3×3×3×3×3×4 = 8748.

Concernant la stratégie 4

$17 = 3+3+3+3+3+2$

$3\times3\times3\times3\times3\times2 = 486$

Cette technique marche mais pour les nombres en dessous de 4 cette technique ne marche pas.

car exc : 4 $3+1 = 3\times1 = 3$

en faisant cette technique on obtient 3

or, le plus grand nombre qu'on peut trouver avec 4 est 4.

$4 = 2+2$

$= 2\times2 = 4$

PIÈCES DE MONNAIE : DIOPS À TOUT PRIX ?

Thierry CHEVALARIAS
Enseignant, Collège saint Exupéry
CII Collège, IREM&S Poitiers
thierry.chevalarias@ac-poitiers.fr

Stéphanie DEWYSPELAERE
Enseignante, Collège du Mont des Princes
CII Collège, IREM de Grenoble
Stephanie.dewyspelaere@ac-grenoble.fr

Jérôme HERISSET
Enseignant, Collège La Fontaine Margot Keranroux
CII Collège, IREM de Brest
jerome.herisset@ac-rennes.fr

Résumé
Lors de cet atelier, les membres de la CII-Collège ont présenté une activité expérimentée dans des classes afin de permettre un travail sur la notion de preuve en mathématiques. Cette activité portait sur la validité d'un système de monnaie basé sur seulement deux types de pièces de valeurs différentes.

A partir de la résolution du problème et de l'analyse de productions d'élèves, les participants ont listé les connaissances mathématiques en jeu en lien avec les programmes du collège.

L'analyse de ces productions a également permis de catégoriser plusieurs types de raisonnements et de justifications chez les élèves, à partir desquels les participants ont pu travailler, en utilisant les travaux de N. Balacheff concernant les types de preuves. Ainsi ils ont pu envisager comment gérer la phase d'institutionnalisation en regard d'apports théoriques relatifs à la preuve en mathématiques.

I - PRÉSENTATION DE LA SITUATION D'APPRENTISSAGE

Dans le cadre de travaux de la commission CII-Collège sur la preuve en arithmétique, les membres ont proposé une activité inspirée de l'exercice proposé dans les évaluations PISA 2009 ci-dessous :

PIÈCES DE MONNAIE – *QUESTION 1*

Serait-il concevable de mettre en place un système de pièces de monnaie en n'utilisant que les valeurs 3 et 5 ? Plus spécifiquement, quels sont les montants qui pourraient être obtenus sur cette base ? Un tel système serait-il souhaitable ?

Figure 1. Énoncé extrait des évaluations PISA 2009

Il s'agissait alors de l'énoncé d'un exercice à prise d'initiative. Plusieurs démarches de raisonnement étaient envisagées.

La Commission Inter-IREM Collège propose une adaptation de cet énoncé, exploitable à tous les niveaux de classe du collège. Un article à paraitre explicitera davantage les choix pédagogiques et didactiques de mise en œuvre de cette situation d'apprentissage. Voici l'énoncé du problème retenu :

L'île de Diophée a un système de monnaie particulier: les habitants n'utilisent que des pièces de 9 diops et 11 diops. Ce système de monnaie permet-il de vendre ou d'acheter des objets à n'importe quel prix ?

Dans un premier temps, les participants ont résolu le problème puis se sont interrogés sur les démarches possibles des élèves et sur les objectifs d'enseignement visés.

Il s'agit de faire travailler les élèves sur la notion de preuve. Les connaissances mathématiques mises en jeu sont des notions d'arithmétique telles que la notion de multiple, de diviseur et de nombres premiers entre eux.
La CII a proposé le déroulé suivant à ses classes :
- une phase de travail individuel
- une phase de travail de groupe avec production d'un compte-rendu commun
- une mise en commun visant à analyser avec la classe les arguments avancés par chacun des groupes. Celle-ci aboutit à une trace écrite portant sur « ce qu'est prouver ».
- Un prolongement possible : « Quelles valeurs entières peut-on choisir pour les deux pièces pour pouvoir vendre ou acheter des objets à n'importe quel prix ? »

Les élèves ne disposent pas de la connaissance mathématique permettant la résolution experte du problème. L'objectif de cet atelier est de sensibiliser les enseignants sur le fait que les élèves peuvent tout de même produire des preuves variées en analysant des productions d'élèves issues de nos expérimentations.

II - ANALYSE DES PRODUCTIONS D'ÉLÈVES

La preuve chez Balacheff

Les participants ont analysé une sélection de productions d'élèves et les ont catégorisés en lien avec la typologie des preuves de Nicolas Balacheff (1987), présentée au préalable.

Voici un tableau récapitulatif de ces types de preuve.

Preuves pragmatiques	Empirisme naïf	Vérification sur quelques exemples, une conjecture possible mais sans remise en question. La question de la validité n'est pas posée.
	Expérience cruciale	Exemples permettant une conjecture sur la relation entre les objets. La question de la généralisation est posée et mise à l'épreuve.
Exemple générique		"Explication des raisons de la validité d'une assertion par la réalisation d'opérations ou de transformations sur un objet présent non pour lui-même mais en tant que représentant caractéristique d'une classe d'individus"[1].
Preuves intellectuelles	Expérience mentale	Utilisation d'un représentant considéré comme quelconque. La preuve montre une décontextualisation et l'analyse des relations entre les objets.
	Calcul sur les énoncés	Manifestation d'une construction intellectuelle fondée sur des théories. La preuve ne s'appuie pas sur l'expérience.

Figure 2. Typologie des preuves selon N. Balacheff (1987)

Productions d'élèves

Nous avons retenu et analysé quelques productions d'élèves afin de les catégoriser. Nous résumons ci-dessous ces éléments d'analyse. L'ordre des productions dépend du type de preuve convoqué.

L'élève fait des hypothèses sur des prix envisageables , il écarte des valeurs trop grandes. Il n'y a pas de raisonnement apparent.

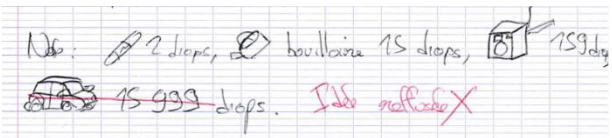


Figure 3. Production 1

Par une suite d'essais, il tente de trouver comment fabriquer différents prix. Il n'y a pas de conclusion apportée par les élèves.

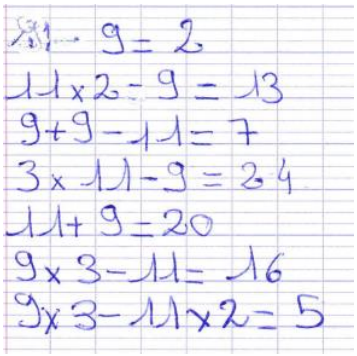


Figure 4. Production 2

Cette production semble témoigner d'une volonté de partitionner l'ensemble des entiers (multiples de 9, de 11 et certaines combinaisons linéaires de ces deux nombres).

Nous considérons qu'il s'agit d'une preuve de type exemple générique dans la mesure où 9 et 11, dans leur production, engendrent un ensemble de nombres.

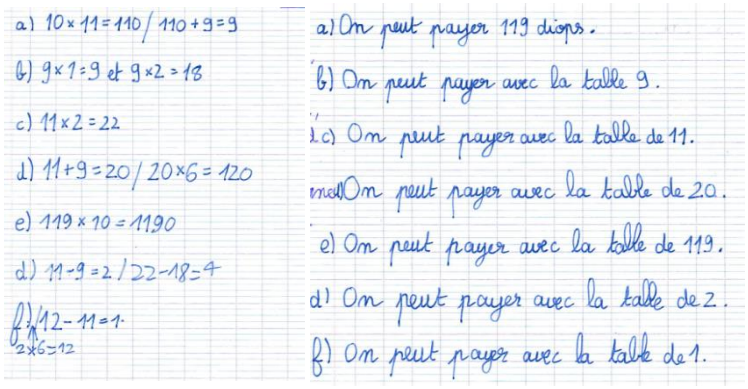


Figure 5. Production 5

L'élève tente de produire l'ensemble des nombres impairs supérieurs à 11 puis inférieurs à 9. Il réussit à produire une combinaison linéaire égale à 1. Mais il n'envisage pas de construire tous les nombres à l'aide de cette dernière composition .

Nous la qualifierions cette production d'exemple générique, nous repérons une référence aux nombres impairs et une structure commune dans les combinaisons linéaires (il ajoute 1 aux coefficients multiplicateurs des nombres 11 et 9 à chaque étape).

Nous constatons que l'élève ne cherche pas à produire les nombres pairs une fois déterminée une combinaison égale à 1. On peut faire l'hypothèse qu'il n'envisage pas des nombres pairs en partant des nombres impairs. Il semble nécessaire de faire verbaliser à l'élève les raisons pour lesquels il s'est arrêté là.

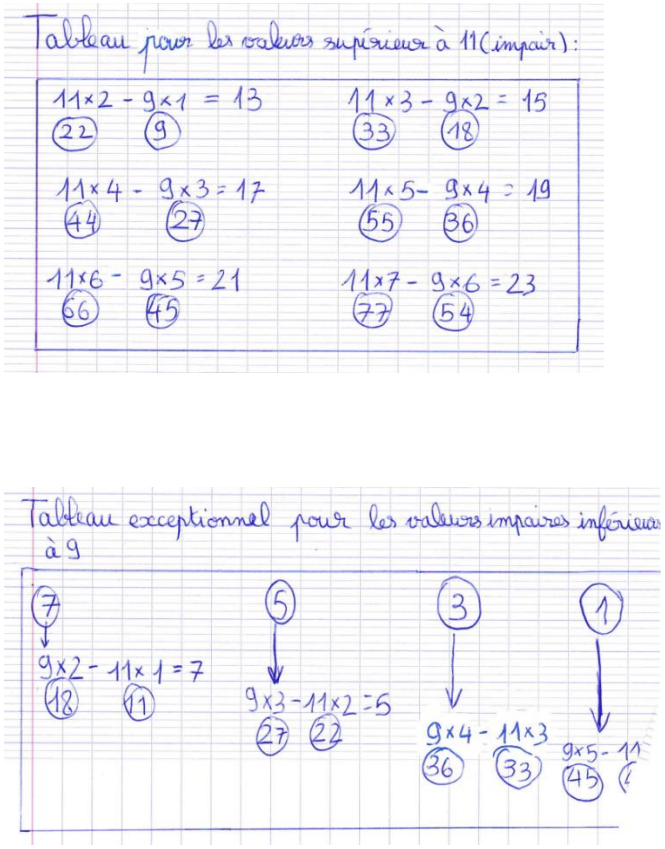


Figure 6. Production 7

L'élève détermine une combinaison égale à 1, il conclut que tous les prix sont possibles. Nous ne trouvons pas de justification de cette affirmation.

Nous choisissons de qualifier cette production d'expérience cruciale.

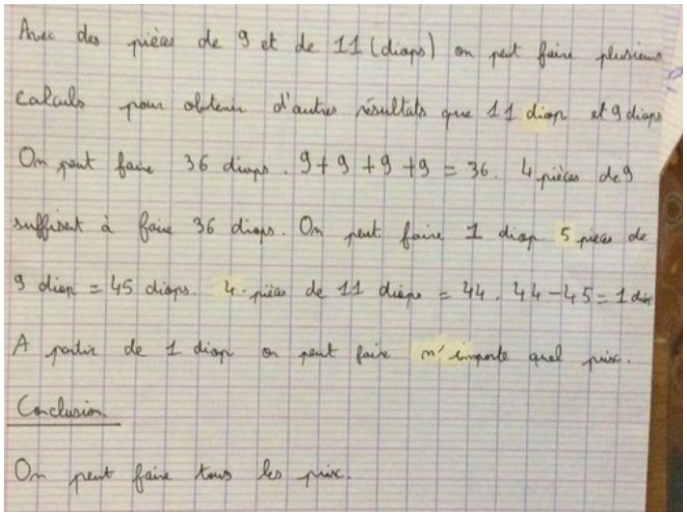
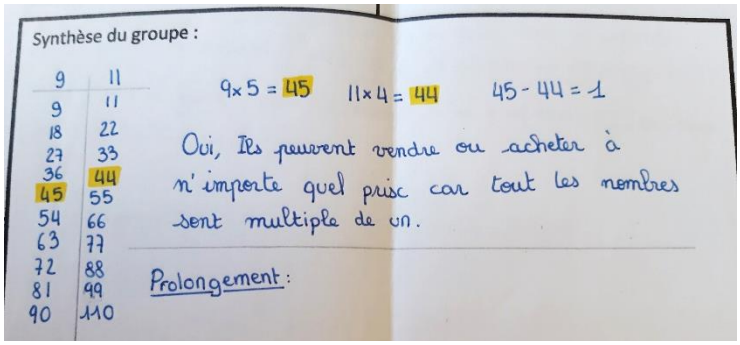

Avec des pièces de 9 et de 11 (diops) on peut faire plusieurs calculs pour obtenir d'autres résultats que 11 diops et 9 diops
On peut faire 36 diops. 9+9+9+9 = 36. 4 pièces de 9 suffisent à faire 36 diops. On peut faire 1 diops 5 pièces de 9 diops = 45 diops. 4 pièces de 11 diops = 44. 44−45 = 1 dio
A partir de 1 diops on peut faire n'importe quel prix.
Conclusion
On peut faire tous les prix.

Figure 7. Production 17

L'élève fait la liste des multiples successifs de 9 et 11 pour repérer deux nombres dont l'écart est égal à 1. Il a identifié l'importance du nombre 1 et formule le fait que tous les autres se construisent comme le produit de « 1 » et de n'importe quel nombre. Il s'agit ici d'une preuve intellectuelle de type expérience mentale.


Synthèse du groupe :

9	11
9	11
18	22
27	33
36	44
45	55
54	66
63	77
72	88
81	99
90	110

9×5 = 45 11×4 = 44 45 - 44 = 1

Oui, Ils peuvent vendre ou acheter à n'importe quel prix car tout les nombres sont multiple de un.

Prolongement :

Figure 8. Production 9

L'élève rend compte d'une combinaison linéaire égale à 1 puis explique dans un langage naturel et non algébrique comment produire n'importe quel prix à partir de cette combinaison linéaire. Il s'agit selon nous d'une preuve intellectuelle de type expérience mentale.

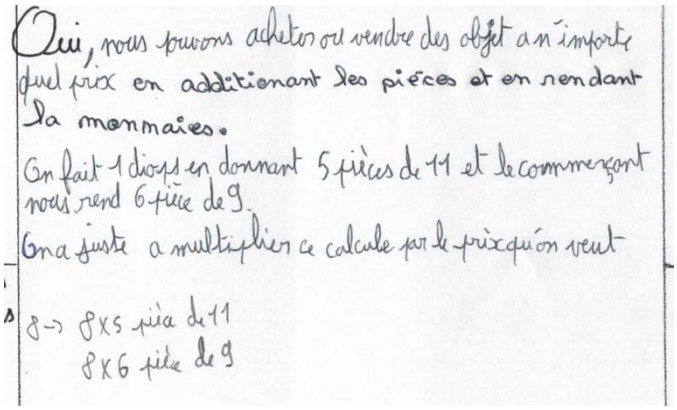

Oui, nous pouvons acheter ou vendre des objet a n'importe quel prix en additionant des pièces et en rendant la monnaies.
On fait 1 diops en donnant 5 pièces de 11 et le commerçant nous rend 6 pièce de 9.
On a juste a multiplier ce calcule par le prix qu'on veut
8 → 8x5 pièce de 11
8x6 pièce de 9

Figure 9. Production 18

Les participants se sont impliqués dans l'analyse des productions élèves, ils ont constaté que délimiter les caractéristiques pour chaque type de preuve est parfois difficile. Les éléments de contexte sont souvent déterminants pour choisir d'associer une production d'élèves à un type de preuve. Ils ont pu constater la grande variété des productions d'élèves.

Institutionnalisation

L'institutionnalisation dépend du niveau d'enseignement et des éléments observés avec les élèves.
La question posée est alors de déterminer quelques critères pour produire une preuve.
Une institutionnalisation pourrait être, en regard avec les productions précédentes :

Bilan :

- Pour montrer qu'une conjecture est fausse, on peut produire un contre-exemple.
- Plusieurs exemples vérifiant la conjecture ne suffisent pas pour montrer qu'une conjecture est vraie.

CONCLUSION

Analyser les productions des élèves en fonction des types de preuve permet à l'enseignant de prendre conscience de la diversité des types de preuve existants au sein d'une même classe. Il peut ainsi confronter les élèves aux différentes productions afin de les sensibiliser aux différentes façons de prouver. Il est nécessaire de prendre en compte les preuves non intellectuelles pour accompagner l'évolution des processus de preuve des élèves. Il semble important de proposer ce type de problèmes ouverts à tout niveau de classe pour développer les capacités des élèves à prouver. C'est aussi l'occasion de construire des bilans dont l'objectif est de sensibiliser à la preuve en mathématiques.

BIBLIOGRAPHIE

Balacheff, N. (1987). Processus de preuve et situations de validation (Proving Processes and Situations for Validation). *Educational Studies in Mathematics*, *18*(2), 147–176. http://www.jstor.org/stable/3482413

ANNEXES

Enoncé et son prolongement

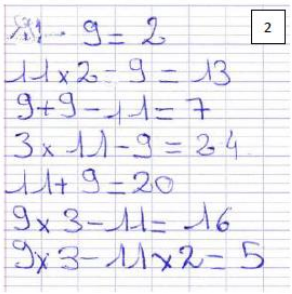
L'île de Diophée a un système de monnaie particulier : les habitants n'utilisent que des pièces de 9 Diops et des pièces de 11 Diops.

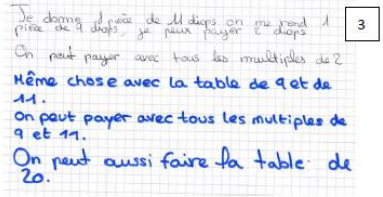
Ce système de monnaie permet-il de vendre ou d'acheter des objets à n'importe quel prix ?

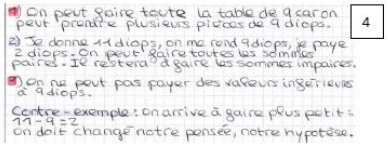
Prolongement : Quelles valeurs entières peut-on choisir pour les deux pièces pour vendre ou acheter des objets à n'importe quel prix ?

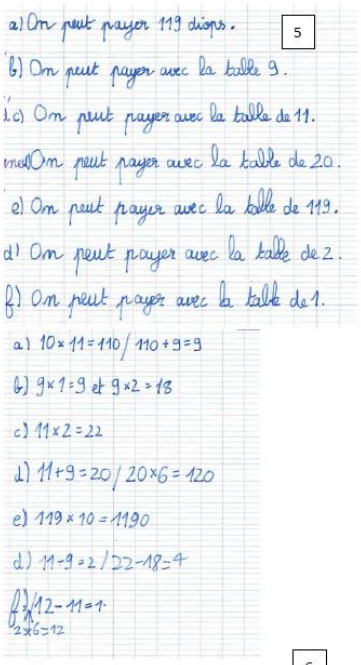
Productions d'élèves analysées au cours de l'atelier

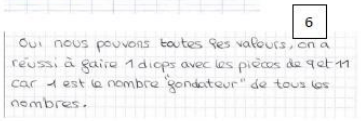

1

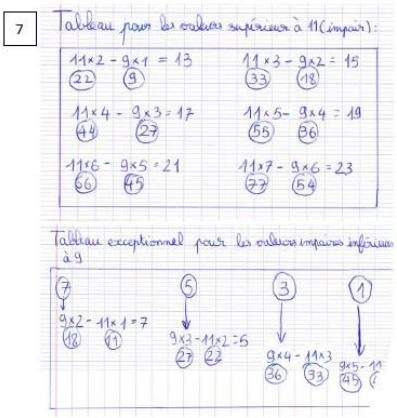

2


3

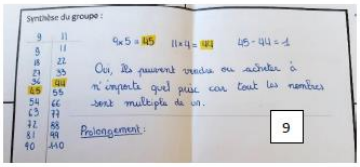

4

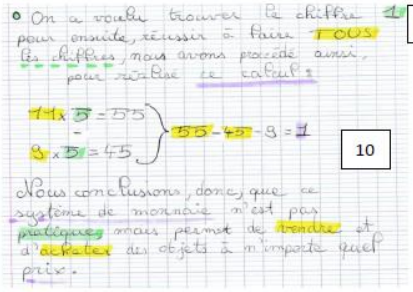

5


6


7

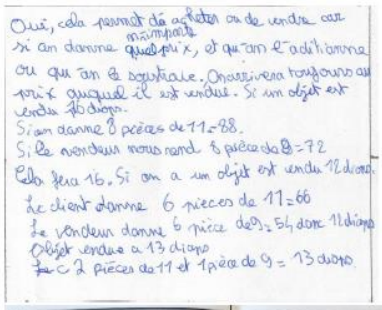

8


9

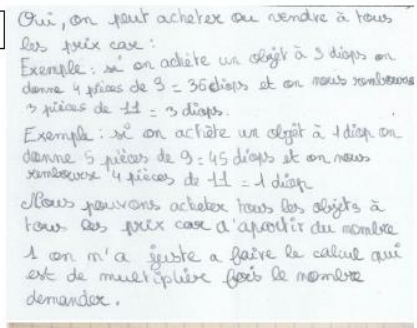


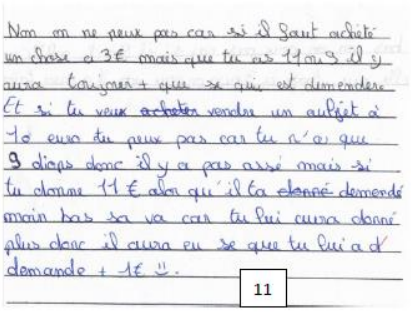
13

10

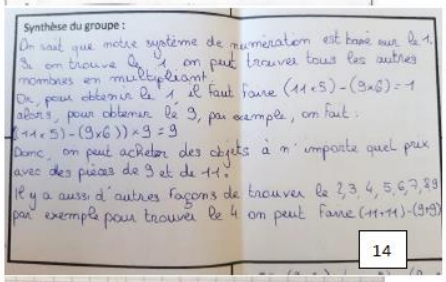


16

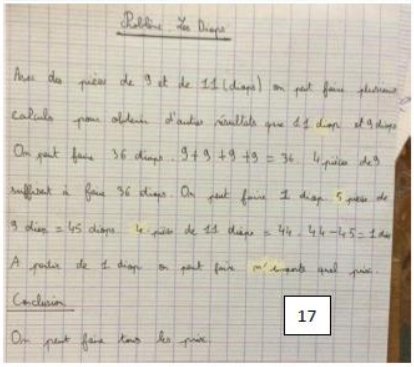




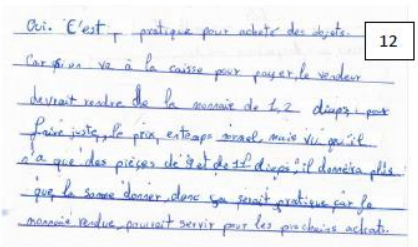
11



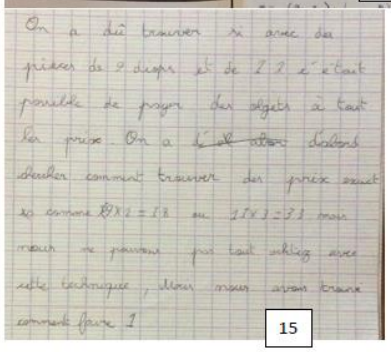
14



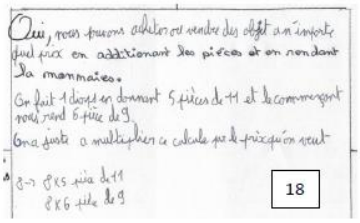
17



12



15



18

LE TOUR DE MAGIE DE GERGONNE

Anne CORTELLA
Maîtresse de Conférences
Groupe jeux, IRES de Montpellier
anne.cortella@u.montpellier.fr

Résumé
Gergonne, professeur de mathématiques puis recteur à Montpellier au début du 19ème siècle publie en 1814 dans le premier journal de recherche en mathématiques (qu'il a créé) ses « Recherches sur un tour de cartes », maintenant appelé tour des « des piles de Gergonne », décrit initialement en 1769 par Guyot dans ses Nouvelles récréations physiques et mathématiques. La version traditionnelle de ce tour est basée sur l'écriture des nombres en base 3, qui permet de numéroter chacune des cartes entre 0 et 26 par une écriture à 3 chiffres.

L'atelier a consisté en une appropriation du tour « de magie », une recherche des participants sur le fonctionnement de ce tour, et une mise en lumière des propriétés mathématiques permettant de le modéliser. Les expérimentations ont utilisé des jeux de 27 ou de 100 cartes, reparties respectivement en 3 ou 10 tas, ce qui a conduit à une généralisation à un jeu d'une puissance quelconque n d'un nombre a de cartes, réparties en n tas.

Des éléments sur ce qui peut être traité avec/produit par les élèves en classe ont finalement été proposés. Ces éléments sont issus des expérimentations effectuées à divers niveaux du collège à la terminale ainsi qu'en formation des enseignants du premier ou second degré, en grands comme en petits groupes, par le groupe jeux de l'IRES de Montpellier.

Ce groupe est composé de

- professeurs de collège : Alix Boissière, Clémence Bargniol, Audrey Burel, Carole Duffet, Driss Foufa, Saïd Mounime ;

- un professeur des écoles : Thomas Haye ;

- des enseignants-chercheurs : Anne Cortella, Nicolas Saby, David Théret.

Le lecteur est d'ailleurs invité à se munir d'un jeu de 27 cartes, voire d'un jeu de 100 cartes (par exemple les 100 premières d'un jeu de *6 qui prend*) pour expérimenter les actions au fur et à mesure et ainsi avoir une idée de ce qui se passe, puis suivre les calculs proposés. On pourra mettre, pour démarrer, les 100 cartes dans l'ordre croissant, en commençant par le dessus du paquet, faces cachées.

I - PRÉSENTATION DU TOUR DE MAGIE

1. La version classique

L'atelier a débuté par plusieurs démonstrations effectives du tour, par une "mauvaise magicienne" (pour que l'on puisse entrapercevoir que "Y'a un trrruc").

On va ici tout d'abord expliquer le fonctionnement du tour de magie de Gergonne.

On dispose d'un jeu de 27 cartes toutes différentes. La magicienne propose à une personne du public, que l'on nommera le cobaye, de choisir une des cartes, de bien la mémoriser en ne la montrant qu'au public et pas à la magicienne. Elle tient alors le paquet de cartes faces cachées, et distribue les cartes une par une, en les retournant, en 3 colonnes. Elle demande au cobaye de lui indiquer celle dans laquelle est positionnée sa carte, puis regroupe les colonnes en 3 paquets qu'elle entasse avant de redistribuer suivant la même méthode. Elle répète ceci plusieurs fois, puis retourne les cartes une à une et s'arrête miraculeusement à la carte choisie par le cobaye.

La présentation de ce tour peut être répétée plusieurs fois, en changeant de cobaye, en laissant de plus en plus apparentes les manipulations, afin que le public puisse remarquer *in fine* que :

- le jeu comporte 27 cartes ;

- on a distribué et regroupé 3 fois ;

- on a toujours mis le paquet contenant la carte visée au milieu du paquet reconstitué ;

- on a ensuite compté jusqu'à 14, et ainsi la carte choisie s'est retrouvée au bout des 3 manipulations au milieu du paquet.

La démonstration faite avec le jeu de 100 cartes, pas forcément triées au départ, permet de constater qu'en distribuant et regroupant 2 fois les 100 cartes en 10 tas, et en mettant chaque fois le tas contenant la carte en cinquième position, à partir du haut faces cachées, la carte choisie se retrouve en 50-ième position. Pour le faire apparaître plus visuellement, on peut distribuer à partir de la fin le tas en 10 colonnes et on s'arrête donc quand on a rempli les 5 premières lignes de toutes les colonnes. La carte est la dernière posée.

2. Plus de magie

Puisque les participants pensent maintenant avoir tout compris, on peut leur montrer qu'on peut faire beaucoup mieux : le cobaye est alors amené à proposer un nombre entre 1 et 27 (pour le jeu de 27 cartes). La magicienne, après un moment d'intense concentration, après avoir distribué et regroupé à nouveau trois fois, compte les cartes à partir du haut du paquet. La carte choisie se trouve (si elle ne s'est pas trompée), à la place choisie par le cobaye.

S'il est laborieux de le faire également pour le jeu de 100 cartes, on peut plutôt proposer d'observer précisément les manipulations qui conduisent la carte choisie tout en haut ou tout en bas du tas de 27 cartes (en 1ère ou en 27-ième position).

Le rôle de l'observation de ces manipulations est d'éclairer sur la manière dont la carte « remonte » dans les premières positions, ou « redescend » dans les dernières, suivant les positions choisies par la magicienne. Ce sont ces observations qui conduisent aux premières constatations sur le comportement des cartes au fur-et-à-mesure des manipulations pour conduire la carte en une position quelconque pour 27 cartes : si on met toujours le tas contenant la carte au-dessus du paquet (faces cachées), la carte arrive en une fois dans les 9 premières, en deux fois dans les 3 premières, en trois fois en premier (et symétriquement quand on met le paquet contenant la carte en dessous).

De la même manière quand on place le paquet contenant la carte au milieu du paquet, la carte se situe entre la 10-ième et la 18-ième place dans le paquet reconstitué.

L'utilisation des 100 cartes peut alors être renouvelée mais seulement (à cause du caractère fastidieux de l'opération) pour mettre la carte en deux fois à l'une des extrémités du paquet. On pourra ainsi infirmer ou confirmer certaines des conjectures émises précédemment.

3. Le cas général

Le travail effectué dans l'atelier tend à généraliser les deux cas observés précédemment en modélisant les actions et leurs effets pour un paquet de a^n cartes, pour un entier positif a quelconque.

On désire alors choisir un nombre b entre 1 et a^n, et en distribuant n fois le paquet en a colonnes et en les regroupant suivant un ordre bien choisi, on amène la carte en position b du paquet recomposé, sans toutefois connaître la carte, mais sur les seules indications à chaque distribution de la colonne dans laquelle elle se trouve.

C'est ce travail qui a été proposé dans une réflexion guidée par petits groupes disposant de jeux de 27 cartes et avec un jeu de 100 cartes commun pour tous les groupes.

II - MODÉLISATION DES MANIPULATIONS DES CARTES

1. Observation et modélisation de la distribution

Les petits groupes ont reçu la consigne suivante : essayez de réaliser le tour. Puis regardez plus précisément la répartition de cartes, par exemple en supposant qu'elles sont numérotées dans l'ordre dans le paquet à distribuer. Plus précisément :

- Avec un jeu de 100 cartes distribuées en 10 tas : comment sont réparties les cartes ?Caractériser la colonne et le rang dans cette colonne de la carte b.
- Et avec un jeu de 27 cartes ? Comment caractériser les cartes de chaque tas ? En quelle position de quelle colonne arrive la carte b ?
- Généraliser pour a^n cartes.

Voici ce que l'on peut observer.
Tout d'abord si on distribue 100 cartes numérotées de 1 à 100 en 10 colonnes, observons la place de la 46-ième carte dans les lignes et colonnes

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	11	12	13	14	15	16	17	18	19	20
3	21	22	23	24	25	26	27	28	29	30
4	31	32	33	34	35	36	37	38	39	40
4 + 1	41	42	43	44	45	46	47	48	49	50
6	51	52	53	54	55	56	57	58	59	60
7	61	62	63	64	65	66	67	68	69	70
8	71	72	73	74	75	76	77	78	79	80
9	81	82	83	84	85	86	87	88	89	90
10	91	92	93	94	95	96	97	98	99	100

Figure 1. Distribution pour 100 cartes

La carte 46 = 45 + 1 est placée en position 4 + 1 de la colonne 5 + 1.

Autrement dit, la première colonne contient les cartes dont le numéro se termine par 1, la deuxième celles terminant par 2, etc…, mais la dixième et dernière celles terminant par 0. La première ligne contient celles dont le numéro n'a qu'un chiffre et le numéro 10, c'est-à-dire dont le numéro moins 1, écrit avec deux chiffres, commence par 0 ; la deuxième celles dont le numéro moins un commence par 1, etc…Ainsi la carte numérotée $b = a_1a_0 + 1$, l'écriture en base 10 de $b-1$ étant notée a_1a_0, est placée par la distribution en $(a_1 + 1)$-ième place dans la colonne $(a_0 + 1)$.

Cela peut encore s'écrire : la carte b avec $b - 1 = 10 \times q + r$ se trouve en position $q + 1$ dela colonne $r + 1$.

Effectuons maintenant la distribution pour 27 cartes numérotées de 1 à 27 distribuées en 3 colonnes de 9, et repérons la 17-ième carte :

	1	$1+1$	3	
1-ière position	1	2	3	
2-ième position	4	5	6	
3-ième position	7	8	9	
4-ième position	10	11	12	
5-ième position	13	14	15	
position $5+1$	16	17	18	$17 = 3 \times 5 + 1 + 1$
7-ième position	19	20	21	
8-ième position	22	23	24	
9-ième position	25	26	27	

Figure 2. Distribution pour 27 cartes

Ainsi la carte b telle que $b - 1 = 3 \times q + r$ se trouve en position $q + 1$ dans la colonne $r + 1$.

On peut extrapoler facilement :

Résultat 1. Pour a^n cartes distribuées en a tas (a entier non nul fixé) : si la division euclidienne de b- 1 par a s'écrit $b - 1 = qa + r$, alors la b-ième carte se trouve à la $(q + 1)$-ième place dans la $(r + 1)$-ième colonne.

Remarque : À ce stade, il peut paraître plus simple de tout numéroter entre 0 et a^n-1 ou $a-1$ ou encore $a^{n-1} - 1$. C'est effectivement ce qu'un enseignant peut décider. Ce n'est pas le choix qui a été fait ici bien que cela puisse simplifier les écritures. En effet, cela ne correspond pas aux observations que font naturellement des élèves de collège qui comptent bien sûr les cartes à partir de 1, ni aux constatations préalables qui ont été faites pendant la phase d'observation.On retrouve néanmoins partout cette correspondance puisqu'on considère toujours la division du rang $b - 1$ par a qui se trouverait en q-ième position de la r-ième colonne si on numérotait partout à partir de zéro.

2. Modélisation du rassemblement des colonnes en tas

On regroupe maintenant les colonnes en un seul tas, en mettant la colonne contenant la carte b en $(k + 1)$-ième position à partir du dessus, toujours face cachée.

On peut par exemple mettre pour le jeu de 100 cartes distribuées précédemment la colonne 5 + 1 contenant la carte $b = 46 = 45 + 1$ en 3-ième position. On choisit donc dans cet exemple $k = 2$. On place

ainsi 2 paquets de 10 cartes avant la colonne sélectionnée. La carte choisie, qui était en position 4 + 1 dans sa colonne, est ainsi placée, après distribution et recomposition, en position $b' = 2 \times 10 + 4 + 1$.

De même, on peut mettre pour le jeu de $3^3 = 27$ cartes distribuées précédemment la colonne 1+1 contenant la carte $b = 17 = 5 \times 3 + 1 + 1$ en 2-ième position. On choisit donc dans cet exemple $k = 1$. On place ainsi 1 paquet de 9 cartes avant la colonne sélectionnée. La carte choisie, qui était en position 5 + 1 dans sa colonne, est ainsi placée, après distribution et recomposition, en position $b' = 1 \times 9 + 5 + 1$.

Résultat 2. Pour a^n cartes distribuées en a colonnes : supposons que la carte choisie se trouve en $(q + 1)$-ième position de sa colonne.

a. En mettant cette colonne sur le dessus, la carte reste en $(q + 1)$-ème position du tas reconstitué.
b. Pour la colonne en deuxième position, on a alors ajouté au-dessus autant de cartes qu'il y a de cartes dans une colonne, c'est-à-dire a^{n-1}. Elle se retrouve alors en $(a^{n-1} + q + 1)$-ième position.

De manière générale, si on met la colonne contenant la carte b en $(k + 1)$-ième position à partir du dessus face cachée, la carte est maintenant placée en position $k.a^{n-1} + q + 1$ dans le tas reconstitué.

Quelques cas particuliers intéressants :

c. Pour 100 cartes, si la carte est en 10-ième position de sa colonne ($q = 9$), et que l'on met cette colonne en 5-ième place en partant du dessus dans le tas ($k = 4$), la carte se retrouve en position $4 \times 10 + 9 + 1 = 50$ dans le tas reconstitué.
d. Si elle était en première position de sa colonne ($q = 0$) et qu'on met cette colonne en 6-ième place ($k = 5$), alors elle se retrouve en position $5 \times 10 + 0 + 1 = 51$ dans le tas.
e. Pour 27 cartes, si la carte était au milieu de sa colonne (i.e. pour $q = 4$), et que l'on met cette colonne au milieu du tas ($k = 1$), elle se retrouve en $9 + 4 + 1 = 14$-ième position donc au milieu du paquet.

3. Combinaison des deux actions pour 100 ou 27 cartes

Les membres de l'atelier ont alors été amenés à répondre aux questions suivantes :

- Avec 100 cartes, si on met la colonne $r + 1$ de la carte $b = aq + r + 1$ en $(k + 1)$-ème position à partir du haut (faces cachées), en quelle nouvelle position se trouve la carte ?
- Avec 27 cartes, si la carte b était en deuxième colonne et qu'on met cette colonne au milieu, quelle est la nouvelle position de la carte ?
- Avec 27 cartes, donner un encadrement de la position de la carte b valable pour b quelconque.

Pour mieux comprendre, reprenons le paquet de 100 cartes et observons la position b' de la carte $b = 46$ après la recomposition décrite ci-dessus ($k = 2$) : $b' = 2 \times 10 + 4 + 1$. Ainsi, pour trouver l'écriture en base 10 de $b'-1$, on a décalé dans celle de $b - 1$ le 4 d'un cran vers la droite, et on a mis en premier chiffre le rang de recomposition choisi moins 1 (soit k).

Reprenons le paquet de 27 cartes. Observons tout d'abord des recompositions particulières.

- Si on met la 2-ième colonne au milieu (en position 1 + 1), on ramène toutes les cartes de rang b avec $b = 3q + r + 1$ pour $r = 1$ en position $9 \times 1 + q + 1$, soit entre la 10-ième et la 18-ième position, puisque

$0 \leq q < 9$.

C'était le cas dans le paragraphe ci-dessus pour la carte $b = 17$, qui est conduite en $b' = 15$.

- De même pour les cartes telles que $r = 0$ (1ère colonne) ou $r = 2$ (troisième colonne), si on met leur colonne au milieu (en $1 + 1$) : la dépendance en r disparaît.
- Si maintenant on considère une carte de rang b compris entre 10 et 18. Écrivons $b = 9 \times 1 + 3b_1 + b_0 + 1$ avec $0 \leq b_0 = r < 3$ et $0 \leq b_1 < 3$. Ainsi $q = 3 + b_1$. Elle arrive par distribution en position $3 + b_1 + 1$ de la $(b_0 + 1)$-ième colonne. Donc si on met cette colonne au milieu, elle se retrouve en position $9 + 3 + b_1 + 1$, donc entre la 13-ième et la 15-ième position.
  - Si de plus $b_1 = 1$, donc si $b = 12 + b_0 + 1$ est entre 13 et 15, alors la carte arrive en $9 + 3 + 1 + 1 = 14$-ième position, soit au milieu du paquet de 27 cartes.

On est ainsi amené à décrire la position b par l'écriture de b-1 en base 3. Comme $0 < b \leq 27$, $b - 1$ décrit les nombres qui ont 3 chiffres en base 3. Nous pouvons donc écrire $b = 9b_2 + 3b_1 + b_0 + 1$ avec les chiffres b_i en base 3 valant 0, 1 ou 2.

On observe alors qu'après distribution et en remettant la colonne de la carte en $(k + 1)$-ième position, la carte choisie se retrouve en position $b' = 9k + 3b_2 + b_1 + 1$.

Comme pour le cas d'un jeu de 100 cartes, la dépendance $r = b_0$ a disparu et l'avant dernier 3-chiffre b_1 de $b - 1$ est devenu le dernier chiffre de $b' - 1$, et le premier chiffre est devenu k. Mais ici le chiffre précédent b_2 de $b - 1$ a glissé en deuxième chiffre.

C'est ce glissement-remplacement que l'on va observer dans le cas général.

4. Cas général

On distribue les a^n cartes en a paquets, nous allons choisir d'écrire la position d'une carte dans les paquets en base a. Si b est la position d'une carte, alors $b - 1 \leq a^n - 1$ donc il s'écrit avec n chiffres en base a (on les appellera ses a-chiffres). On notera donc :

$$b = \sum_{i=0}^{n-1} b_i a^i + 1, \text{ avec pour chaque } i,\ b_i \in \{0, \dots, a - 1\}.$$

Ainsi dans le tour classique $b = 9b_2 + 3b_1 + b_0 + 1$, avec $b_i \in \{0, 1, 2\}$ comme ci-dessus, et s'il y a 100 cartes, alors $b = 10b_1 + b_0 + 1$ avec b_i les chiffres usuels.

Alors $b - 1 = qa + r$ avec $q = \sum_{i=1}^{n-1} b_i a^{i-1}$ et $r = b_0$.

Ainsi, lors de la distribution, la carte b arrive en $(q + 1)$-ième place dans la $(b_0 + 1)$-ième colonne. Si on place cette colonne en $(k + 1)$-ième place au-dessus face cachée dans le tas, la carte se retrouve en position $b' = k.a^{n-1} + q + 1$ dans le tas reconstitué.

Résultat 3. La nouvelle place est donc

$$b' = \sum_{i=0}^{n-1} b'_i a^i + 1, \text{ avec } b'_{n-1} = k \text{ et pour } i = 0 \text{ à } n - 2,\ b'_i = b'_{i+1}$$

Les a-chiffres ont glissé d'un rang vers la droite, le premier étant remplacé par k. Le dernier chiffre initial b_0 n'apparaît plus.

III AMENER UNE CARTE CHOISIE EN UNE POSITION CHOISIE

1. Amener la carte au milieu du paquet pour un nombre impair de cartes

On a pu observer pour un paquet de 27 cartes que :

- En mettant la colonne de la carte souhaitée au milieu du tas ($k = 1$) après distribution, la carte se trouvait alors en position b' tel que $10 \leq b' \leq 18$, c'est-à-dire avec $b'_2 = k = 1$.
- Si on redistribue et que l'on met la colonne souhaitée (la colonne $b'_0 + 1 = b_1 + 1$) au milieu, la carte arrive en position b'' comprise entre 13 et 15 : $b''_2 = 1$ et $b''_1 = 1$.
- On recommence en mettant à nouveau la colonne souhaitée (la colonne $b''_0 + 1 = b_2 + 1$) au milieu, et la carte se trouve maintenant en $14 = 9 \times 1 + 3 \times 1 + 1 + 1$-ième position, donc au milieu du paquet.

Considérons maintenant un paquet de a^n cartes pour un entier a impair. La position centrale est la position cible M définie par

$$M - 1 = \frac{a^n - 1}{2} = \frac{a-1}{2}(a^{n-1} + a^{n-2} + \ldots + a + 1),$$

dont tous les chiffres en base a sont $m = \frac{a-1}{2}$. L'entier $m + 1$ est alors également la position de la colonne centrale. Ainsi dans l'exemple précédent $m = 1$ et $M = 14$.

Pour amener la carte petit à petit au milieu du tas, on commence par mettre sa colonne ($b_0 + 1$) au milieu du paquet (en position $m + 1$) : cela conduit la carte dans le tas recomposé en position $b' = ma^{n-1} + b_{n-1}a^{n-2} + \cdots + b_2 a + b_1 + 1$.

On a décalé à les $n - 1$ derniers a-chiffres d'une place vers la droite, et mis m en premier a-chiffre.

On recommence : la colonne $b_1 + 1$ est mise au milieu, puis $b_2 + 1$, etc…

Résultat 4. La carte se retrouve en i étapes, par une récurrence immédiate, en position

$$ma^{n-1} + ma^{n-2} + \cdots + ma^{n-i} + b_{n-1}a^{n-i-1} + \cdots + b_i + 1.$$

Ainsi à partir de $i = n$, la carte est stabilisée en position centrale dans le paquet.

Remarque : On peut remarquer que pour que le tour fonctionne à coup sûr, il faut distribuer et recomposer au moins n fois !!!

2. Amener la carte en haut ou en bas du paquet

On a vu qu'en mettant la colonne contenant la carte en haut du paquet ($k = 0$), la carte se retrouve en position $q + 1$ du paquet. Ainsi

- Pour 100 cartes : $b = 10b_1 + b_0 + 1$, arrive ainsi en $b' = 0 \times 10 + b_1 + 1$. On recommence, elle est

distribuée en 1ère position de sa colonne, puis arrive en $b'' = 0 \times 10 + 0 + 1 = 1$, donc en haut !

- Pour 27 cartes, $b = 9b_2 + 3b_1 + b_0 + 1$ est conduite la première fois en $b' = 9 \times 0 + 3b_2 + b_1 + 1$, puis en b'' = 9 x 0+3 x 0+b_2+1 et à la troisième manipulation en $b''' = 9 \times 0 + 3 \times 0 + 0 + 1 = 1$, donc en haut.
- En général : cette manipulation effectuée n fois fait glisser progressivement les a-chiffres vers la droite en plaçant 0 en premier chiffre. Ça marche encore !
- Symétriquement, mettre à chaque fois la colonne de la carte en bas du paquet (position a donc $k = a - 1$) face cachée amène en n fois la carte en bas du paquet, en position $(a-1)a^{n-1} + \cdots + (a-1)a + (a-1) + 1 = a^n$.

3. Choisir la position pour 100 cartes

Si la cible est la position $c = 10c_1 + c_0 + 1$ (donnés par l'écriture décimale de $c - 1$)

- Après une première distribution, on recompose en positionnant la colonne $b_0 + 1$ en $(c_0 + 1)$-ième place au-dessus face cachée. La carte se trouve en position $b' = 10c_0 + b_1 + 1$;
- Après redistribution on amène la colonne $b_1 + 1$ en $c_1 + 1$. La carte se trouve en c. C'est facile !! Même pas de calcul à faire...

4. Choisir la position dans le cas général

Si la cible est la position $c = \sum_{i=0}^{n-1} c_i + 1$, on place successivement la colonne de la carte (colonne $b_0 + 1$ puis $b_1 + 1$…) en $c_0 + 1$ puis en $c_1 + 1$, $c_2 + 1$,…. Les a-chiffres de la position sont décalés progressivement vers la droite tandis que les premiers chiffres sont remplacés par les c_i pour i allant de 0 à n.

Il " suffit "donc de calculer les a-chiffres de c pour effectuer le tour ! Le magicien a besoin d'un peu de temps et de concentration pour cela. On peut remarquer que comme précédemment, pour que le tour fonctionne, il faut faire n manipulations.

Faute de temps, les participants n'ont pas pu tenter d'effectuer le tour. Mais ils auraient pu constater que cet exercice de calcul mental, sous la pression du public, n'est pas toujours si simple.

C'est pourquoi la magicienne disposait dans la première phase de l'atelier d'une « antisèche » décrivant les 3 actions à produire dans l'ordre pour amener la carte en position cible donnée par le public. Un assistant pourra détourner l'attention du public pendant cette « triche » du magicien. Gergonne, en référence à Guyot, recommande également l'utilisation d'un tel stratagème :

> Si donc on a sous les yeux un tableau qui présente la correspondance entre les vingt-sept manières dont on a pu relever les paquets trois fois consécutivement, et le rang que chaque système de relèvement assigne à la carte pensée, rien ne sera plus facile que de trouver cette carte. L'ouvrage cité prescrit de faire construire une lunette mystérieuse, telle qu'en y regardant on n'y aperçoive que ce tableau, qui s'y trouvera caché intérieurement. A chaque opération, on feindra de regarder les paquets avec cette lunette, comme pour tâcher de discerner la carte pensée ; et on en prendra occasion de contempler le tableau, et d'y lire ce qu'on a à faire, pour que cette carte se trouve à la fin dans le jeu à la place qu'on lui aura assignée à l'avance. (Gergonne, p 277-278)

IV- QUELQUES EXPÉRIMENTATIONS DE LA 4IÈME À LA 1ÈRE

1. Faits généraux

L'atelier s'est terminé par des retours d'expérimentation menés par les membres du groupe IREM jeux de Montpellier.

1. Premier constat : ils ont envie de savoir faire !… mais pas vraiment forcément de comprendre. Nous, on veut qu'ils comprennent ce qu'on utilise :
   - reste, quotient, écriture en base 10 et en base 3,
   - raisonnement,
   - modélisation et représentation du paquet, des actions.

   Donc on veut qu'ils découvrent par eux-mêmes "le truc".
2. Deuxième constat : ils sont incapables (pour beaucoup) de distribuer des cartes...
3. Des difficultés à décrire sont inhérentes aux actions : nécessité de se mettre d'accord. On retourne les cartes, faces cachées, haut, bas...
4. Certains chemins pris par les cartes sont plus visibles que d'autres : ce seront les points d'appui pour commencer à modéliser.
5. À partir de la 3ième, la présence de cartes à jouer induit souvent pour les élèves un modèle probabiliste... C'est difficile de penser à autre chose.

2. Des difficultés de modélisation

Deux choix de numérotation sont possibles qui ont tous les deux des avantages et des inconvénients :

- Le choix fait ici : les numérotations se font à partir de 1.
  - C'est beaucoup plus naturel et proche du tour de magie initial : on compte jusqu'à 14.
  - On peut utiliser le « 6 qui prend » pour la base 10.
  - Les décompositions utilisées sont toujours celles de b - 1, on rajoute 1 partout, il y a des décalages. Mais ils sont toujours les mêmes.
  - Les élèves doivent repérer ces décalages.
  - Le choix de travailler avec 100 cartes est très porteur.
- On peut numéroter les cartes à partir de 0, et compter toujours à partir de 0.
  - Ce n'est pas naturel,
  - Aucun jeu avec cette numérotation n'existe.
  - On peut utiliser des cartes blanches (vendues dans le commerce et qui seront alors effaçables) et les marquer en base 3 (ou 10) à partir de 0.
  - On peut ainsi travailler avec des cartes codées par une écriture à 3 chiffres 000, 001, 002, 010, 011, 012 . . . 222.

- Les actions sont plus faciles à coder,
- C'est difficile de leur faire coder les cartes eux-mêmes.

C'est le choix qui a été fait le plus souvent dans nos expérimentations, sans utiliser de paquet de 100 cartes, quand il y avait des petits groupes d'élèves (stages MathC2+ par exemple, ou avec des classes de première et deux encadrants).

3. Quelques productions d'élèves

Les participants ont pu alors chercher la logique de quelques productions d'élèves de 4ième auxquels on avait demandé d'expliquer pourquoi la carte choisie se trouvait à la fin en 14-ième position après avoir mis la colonne choisie trois fois de suite au milieu du paquet reconstitué.

L'interprétation n'est pas simple si l'on ne s'est pas attaché non seulement à la position des cartes en base 3 mais aussi à des encadrements de cette position au fur et à mesure du tour.

Des tentatives de représentations :

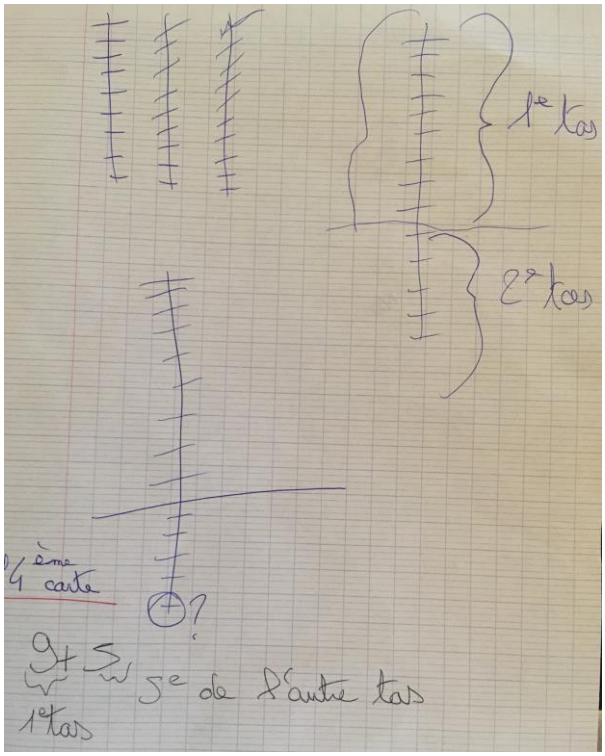


Figure 3. Représentation 1

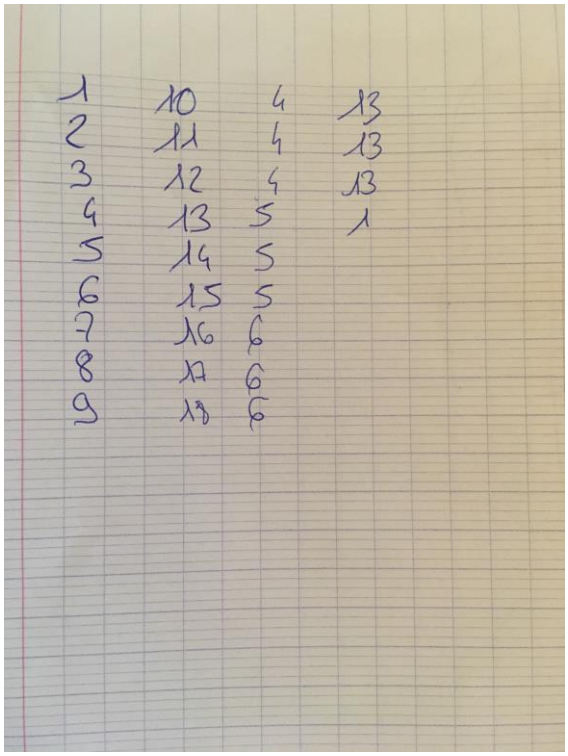


Figure 4. Représentation 2

La première représentation montre que les élèves ont compris comment la position de la carte évolue par recomposition du paquet. Les trois colonnes sont représentées contenant chacune 9 cartes, puis un exemple de position de carte est donné : pour la cinquième d'un paquet.

Il se trouve que ce choix n'est pas anodin puisque la carte arrive donc en 14-ième position dès la première reconstitution, puis se stabilise à cette 14-ième position. La représentation après redistribution puis rassemblement la place encore en 9+5 = 14-ième position.

La deuxième représentation énumère dans la première colonne les positions possibles d'une carte dans sa colonne, et dans la deuxième la position correspondante dans le tas reconstitué (position dans la colonne +9). Dans la troisième colonne, on trouve la position de la même carte dans sa colonne après redistribution, et dans la quatrième (non achevée), la position dans le tas recomposé. Il manquerait une cinquième et une sixième colonne pour obtenir une représentation complète. Il se peut que les élèves aient remarqué que l'on retournait à la première colonne et que ce n'était pas la peine de continuer : les trois premières colonnes suffisent à pister la position d'une carte donnée.

Des descriptions factuelles :

La première description proposée ci-dessous commence plutôt par un fait numérique : distribuer revient à une division du nombre de cartes. Malgré un premier constat d'encadrement du rang de la carte dans sa colonne, les élèves ne poursuivent pas par des encadrements qu'ils n'ont sans doute pas vraiment les moyens de traiter logiquement. Ils considèrent à la fois le cas particulier de la première carte d'une colonne, qui devient 10-ième du paquet puis 4-ième de sa colonne dans la distribution suivante, mais aussi les deux suivantes qui arrivent également en 4-ième position, ainsi que celles d'après qui sont annoncées comme arrivant en 5-ième position quand on redistribue.

Dans leur optique de ne considérer que le chemin de la dixième carte, les élèves n'ont pas remarqué que seules les cartes entre les rangs 13 et 15 sont distribuées en cinquième position de leur colonne. Ils pistent correctement les positions de la première carte d'une colonne.

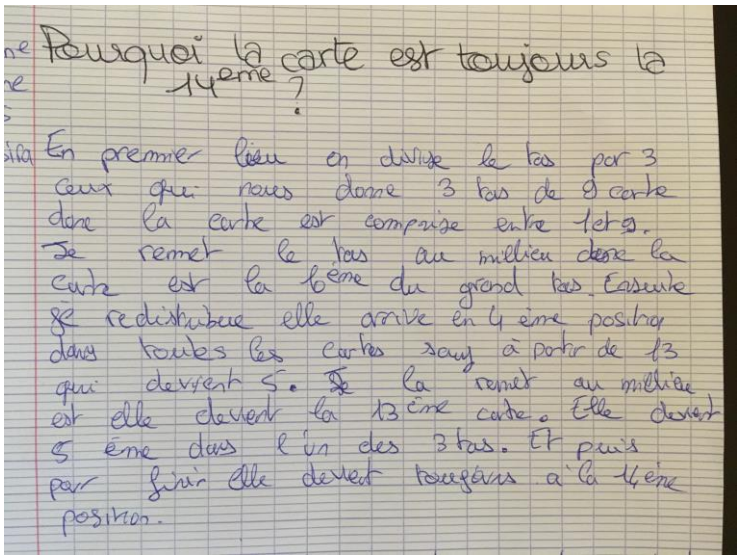


Figure 5. Description 1

Dans la dernière description, le choix de prendre un exemple, qui se veut peut-être générique, est plus conscient. Là encore, les élèves ont bien compris ce qui se passe en distribuant et rassemblant les cartes.

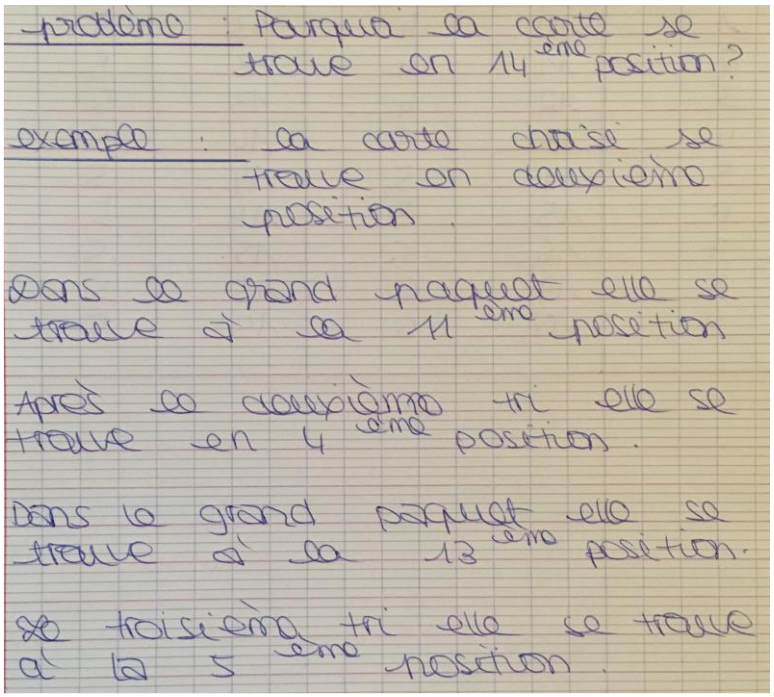


Figure 6. Description 2

V- CONCLUSION DE L'ATELIER

L'atelier était construit pour donner de réels éléments mathématiques permettant de comprendre le tour dans une assez grande généralité, ce qui en a fait un atelier relativement exigeant du point de vue de l'attention aux mathématiques et au raisonnement.

Cela n'a sans doute pas permis complètement aux participants de se projeter dans l'analyse avec des élèves d'un tel tour de magie. Néanmoins il a donné les bases d'une activité originale pour travailler l'arithmétique, et éventuellement l'écriture en bases, avec les élèves. Le groupe jeux de l'IRES de Montpellier travaille encore actuellement sur la mise en place en classe avec divers formats et devra également tenter ce travail avec des élèves de terminale en mathématiques expertes.

Une brochure est en préparation, ainsi qu'un article plus complet élargissant le problème à d'autres nombres de cartes.

VI- BIBLIOGRAPHIE

Guyot, Edme-Gilles (1769). *Nouvelles récréations physiques et mathématiques*, tome III, Gueffierpage 267.

Gergonne, Joseph-Diez (1813-1814).Récréations mathématiques – Recherches sur un tour decartes, *Annales de Mathématiques pures et appliquées*, tome 4, p. 276-283.
http://www.numdam.org/item?id=AMPA_1813-1814__4__276_1

Quintero, Roy, Guérini, Christian (2010). Le "tour de cartes de Gergonne" ; d'un article datant de près de deux cents ans à une généralisation en plusieurs étapes, *Quadrature* n^0 78, p. 8-17.

UNE RÉSOLUTION COLLABORATIVE DE PROBLÈMES : LES VITRES

Julien LAVOLE
Professeur de mathématiques, physique et chimie au LYCEE PROFESSIONNEL PAUL LANGEVIN À BEAUCAIRE
Groupe ResCo de l'IRES de Montpellier
julien.lavole@ac-montpellier.fr

Mireille SAUTER
Professeur de mathématiques, retraitée
Groupe ResCo de l'IRES de Montpellier
mireille.sauter@orange.fr

Sébastien DURAND
Professeur de mathématiques au COLLEGE JEAN MOULIN À PERPIGNAN
Groupe ResCo de l'IRES de Montpellier
Sebastien.Durand@ac-montpellier.fr

Résumé
Lors de cet atelier-TP, les membres du groupe ResCo ont présenté leurs activités, les objectifs qu'ils se fixent et l'organisation générale du dispositif de résolution collaboratif de problèmes auquel participent chaque année entre 80 et 100 classes de la Sixième à la Terminale.
Dans un second temps, les participants ont vécu en accéléré les trois premières semaines du dispositif ResCo.
Durant cette mise en activité, des moments de mises en commun et de discussions ont eu lieu.
Puis, des résolutions d'élèves sur l'énoncé proposé ont été présentées notamment celles faisant appel à l'arithmétique.
Pour conclure, quelques aspects théoriques relatifs au dispositif ResCo ont été abordés.

I - PRESENTATION DE RESCO ET DE SON DISPOSITIF

1. Présentation du groupe

L'acronyme ResCo a pour signification Résolution Collaborative de problèmes.

Le groupe ResCo est un groupe de travail de l'IRES (Institut de Recherche pour l'Enseignement des Sciences) de Montpellier composé de trois professeurs de mathématiques des collèges (Boris Brodin – collège Bellevue à Alès, Damien Clementz – collège Salagou à Clermont l'Hérault, Sébastien Durand – collège Jean Moulin à Perpignan), d'une professeure de mathématiques au collège à la retraite (Mireille Sauter), d'un professeur de mathématiques, physique et chimie au lycée professionnel (Julien Lavolé – LP Paul Langevin à Beaucaire) et de deux enseignants-chercheurs (Simon Modeste – Institut Montpelliérain Alexander Grothendieck, Sonia Yvain-Prébiski – LDAR-INSPE Cergy).

Chaque année, le groupe met en œuvre des formations de deux journées inscrites au Plan Académique de Formation de Montpellier en inscription individuelle dans les locaux de l'IRES de Montpellier et en Formation d'Initiative Locale (à Béziers en 2021, à Carcassonne en 2022). Ces formations s'articulent sur la résolution de problèmes. De plus, le groupe a présenté ces dernières années des ateliers-TP aux journées nationales de l'APMEP, aux séminaires des Commissions Inter-IREM, au colloque de la CIEAEM.

Enfin, dans le cadre du colloque des commissions Inter-IREM Collège et Lycée, le groupe a présenté le dispositif de résolution collaborative de problèmes qu'il organise chaque année.

2. Participation au dispositif

Le dispositif ResCo s'adresse à des classes de collège et lycée général, technologique et professionnel.

Le tableau ci-dessous récapitule le nombre de participations depuis 2015 :

Année	2015	2016	2017	2018	2019	2020	2021	2022	2023
Nombre de classes	74	60	52	63	128	97	81	81	91
Nombre d'enseignants				46	81	60	49	50	50

2.1. Les objectifs du groupe ResCo de l'IRES de Montpellier

Tout d'abord le groupe cherche à développer chez les élèves les compétences mathématiques (la modélisation en particulier), par une activité de résolution de problèmes issus de la vie courante ou d'autres disciplines.

Ensuite, le groupe veut proposer à des enseignants un dispositif favorisant l'autonomie, la créativité et la communication dans la résolution de problèmes mathématiques en classe et entre classes.

Pour ce faire, le groupe réfléchit aux problèmes et aux modalités de travail pertinentes pour ces objectifs.

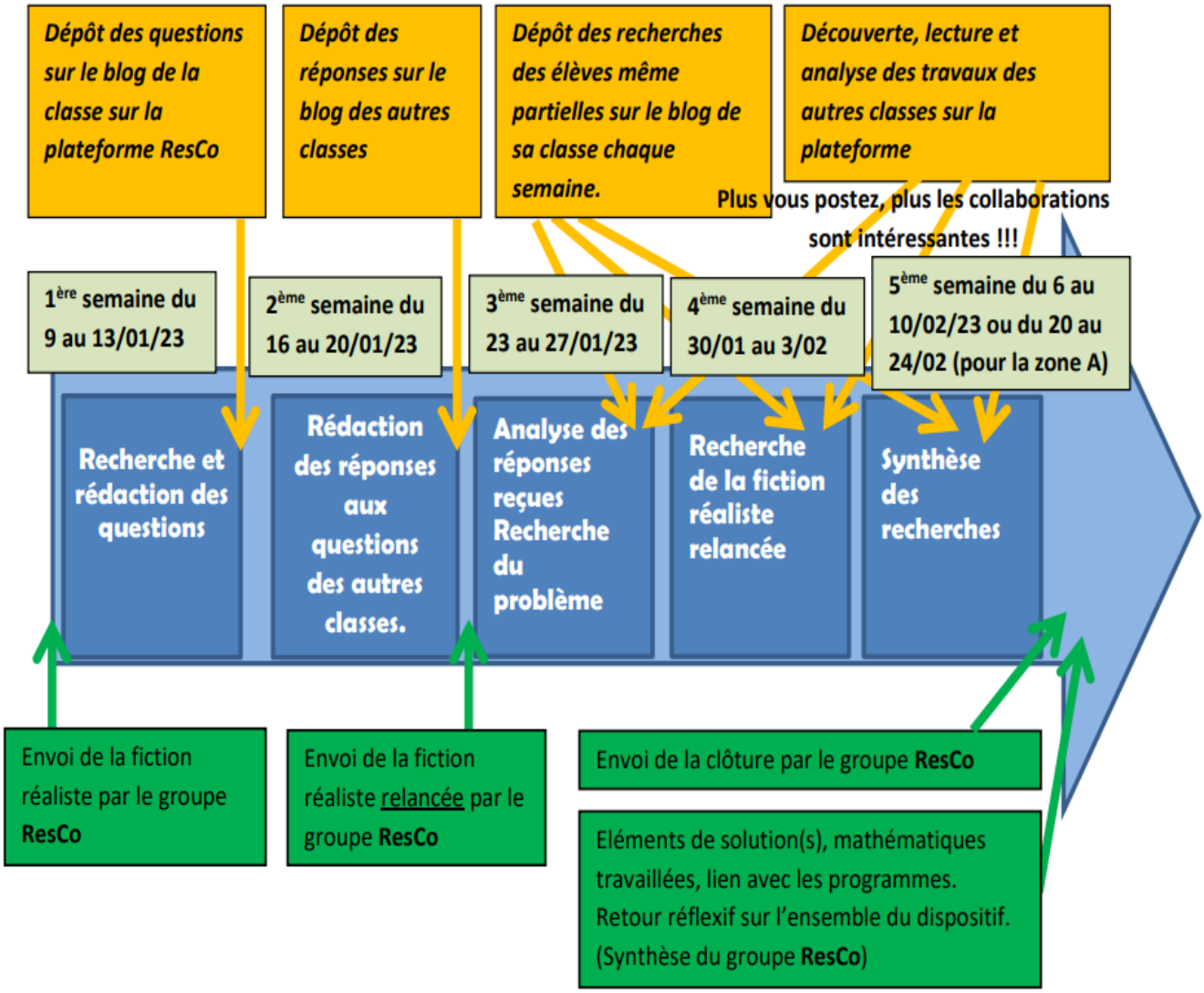
2.2. Présentation générale du dispositif ResCo

Chaque année, le groupe ResCo élabore un énoncé de problème conçu comme une adaptation d'une problématique professionnelle de modélisation depuis 2016.

Les classes inscrites sont réparties en groupes de trois classes de niveaux proches.

Les classes communiquent entre elles via un forum géré par l'enseignant et dont voici le lien : http://forum.math.univ-montp2.fr (nous contacter pour vous y inscrire).

Le dispositif est programmé entre les vacances de Noël et celles d'Hiver (janvier - février) et débute lors de la deuxième semaine après la reprise. Il se déroule pendant cinq semaines au minimum. Le groupe ResCo conseille à chaque classe d'investir au minimum une séance par semaine. Le dispositif s'organise tel qu'indiqué sur la flèche schématisée ci-dessous :



• 1re semaine : recherche et envoi des questions :

Chaque classe prend connaissance de l'énoncé du problème. Les élèves, en groupes, rédigent des questions mathématiques et hors mathématiques pour s'approprier la situation. En fin de séance, une mise en commun est effectuée, puis les questions de la classe sont envoyées aux autres classes du groupe.

• 2e semaine : recherche sur les questions des autres classes et envoi des réponses :

Les élèves, en groupes, répondent aux questions des autres classes. Les groupes les plus avancés émettent les premières conjectures. En fin de séance, une mise en commun est effectuée, puis les réponses et réflexions sont envoyées aux autres classes du groupe.

• 3e semaine : découverte des réponses et poursuite de la recherche avec la fiction relancée adressée à l'ensemble des classes par l'équipe ResCo pour recentrer les pistes de recherche autour d'une problématique commune :

Les élèves, en groupes, découvrent les réponses des autres classes, débattent éventuellement sur ces réponses. Découverte de la fiction relancée et recherche. Les professeurs sont invités à faire prendre conscience aux élèves de la nécessité de faire des choix dans une activité de modélisation mathématique et à échanger sur l'expérience vécue en classe via le forum.

• 4e semaine : poursuite de la recherche :

Les élèves, en groupes, poursuivent la recherche. Chaque groupe d'élèves rédige un bilan des recherches. Le professeur rédige et envoie une synthèse de ces bilans aux autres classes.

• 5e semaine : fin de la recherche :

Le professeur organise un débat scientifique, alimenté par les synthèses des groupes de la classe, celles des groupes des autres classes, renforcé par les synthèses individuelles. Chaque professeur devra ensuite établir avec sa classe un bilan des solutions partielles, des mathématiques travaillées et de l'apport de cette recherche. Des documents élaborés par ResCo seront envoyés.

II - PLAN DE L'ATELIER

Lors de l'atelier, les participants ont, dans un premier temps, pris connaissance du groupe ResCo et de ses travaux tels que présentés dans la partie I.

Ensuite, ils ont vécu les 1e, 2e et 3e semaines du dispositif ResCo en accéléré.

Puis, ils ont débriefé avec les membres du groupe ResCo à propos du dispositif et de l'expérience qu'ils venaient de vivre.

Enfin, ils ont pu voir ce qu'il se passait durant le dispositif dans les classes et comment le groupe ResCo accompagne les enseignants dans la clôture du projet.

III - FICTION RÉALISTE, FICTION RELANCÉE, CLÔTURE

1. Fiction réaliste

Une fiction réaliste est une adaptation d'une problématique professionnelle de modélisation qui se caractérise par six critères (Yvain-Prébiski 2018) :

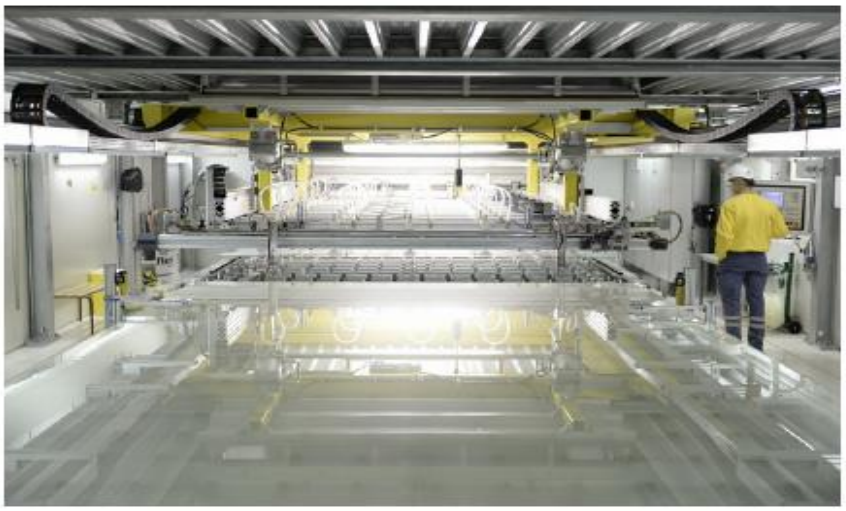
- Une situation a priori non mathématique.
- Un contexte fictif mais réaliste.
- La nécessité d'une phase de modélisation pour une prise en charge efficace de la situation.
- La phase de modélisation peut renvoyer à plusieurs problèmes mathématiques selon les choix qui sont faits.
- La fiction réaliste est conçue comme une adaptation d'une problématique de modélisation issue des pratiques scientifiques professionnelles.
- Les variables didactiques sont choisies de manière à favoriser l'entrée dans la mathématisation.

Simon Modeste
simon.modeste@umontpellier.fr

IREM de Montpellier – 2018-2019
Résolution Collaborative de Problème

Reso

Les vitres



Une entreprise découpe des vitres rectangulaires de 4 dimensions différentes :

210 cm x 215 cm
100 cm x 215 cm
100 cm x 125 cm
60 cm x 215 cm.

Ces vitres sont découpées dans des grandes plaques rectangulaires de verre de 600 cm x 320 cm.

L'entreprise cherche une méthode pour réaliser les découpes selon les commandes en limitant les chutes.

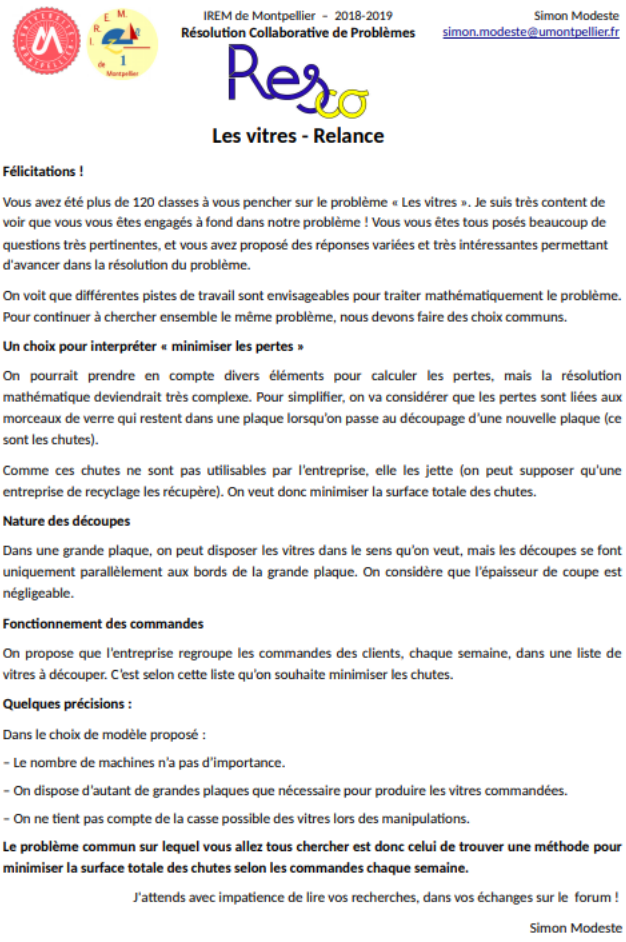
Pour aider l'entreprise, pouvez-vous proposer une méthode qui réalise les découpes et minimise les pertes ?

Fiction réaliste présentée durant l'atelier

2. Fiction relancée

Sur la base de l'analyse a priori des mathématisations possibles, et des spécificités mathématiques, le groupe ResCo prend en compte les questions et réponses des classes et propose un nouveau texte qui fixe des choix de modélisation, selon certaines contraintes du dispositif :

- Le problème mathématique est accessible, au moins en partie, à tous les niveaux scolaires impliqués
- Les choix de mathématisation effectués conservent une cohérence avec les choix proposés par les classes.
- Le problème mathématisé permet un travail de recherche mathématique consistant



IREM de Montpellier - 2018-2019
Résolution Collaborative de Problèmes

Simon Modeste
simon.modeste@umontpellier.fr

Resco

Les vitres - Relance

Félicitations !

Vous avez été plus de 120 classes à vous pencher sur le problème « Les vitres ». Je suis très content de voir que vous vous êtes engagés à fond dans notre problème ! Vous vous êtes tous posés beaucoup de questions très pertinentes, et vous avez proposé des réponses variées et très intéressantes permettant d'avancer dans la résolution du problème.

On voit que différentes pistes de travail sont envisageables pour traiter mathématiquement le problème. Pour continuer à chercher ensemble le même problème, nous devons faire des choix communs.

Un choix pour interpréter « minimiser les pertes »

On pourrait prendre en compte divers éléments pour calculer les pertes, mais la résolution mathématique deviendrait très complexe. Pour simplifier, on va considérer que les pertes sont liées aux morceaux de verre qui restent dans une plaque lorsqu'on passe au découpage d'une nouvelle plaque (ce sont les chutes).

Comme ces chutes ne sont pas utilisables par l'entreprise, elle les jette (on peut supposer qu'une entreprise de recyclage les récupère). On veut donc minimiser la surface totale des chutes.

Nature des découpes

Dans une grande plaque, on peut disposer les vitres dans le sens qu'on veut, mais les découpes se font uniquement parallèlement aux bords de la grande plaque. On considère que l'épaisseur de coupe est négligeable.

Fonctionnement des commandes

On propose que l'entreprise regroupe les commandes des clients, chaque semaine, dans une liste de vitres à découper. C'est selon cette liste qu'on souhaite minimiser les chutes.

Quelques précisions :

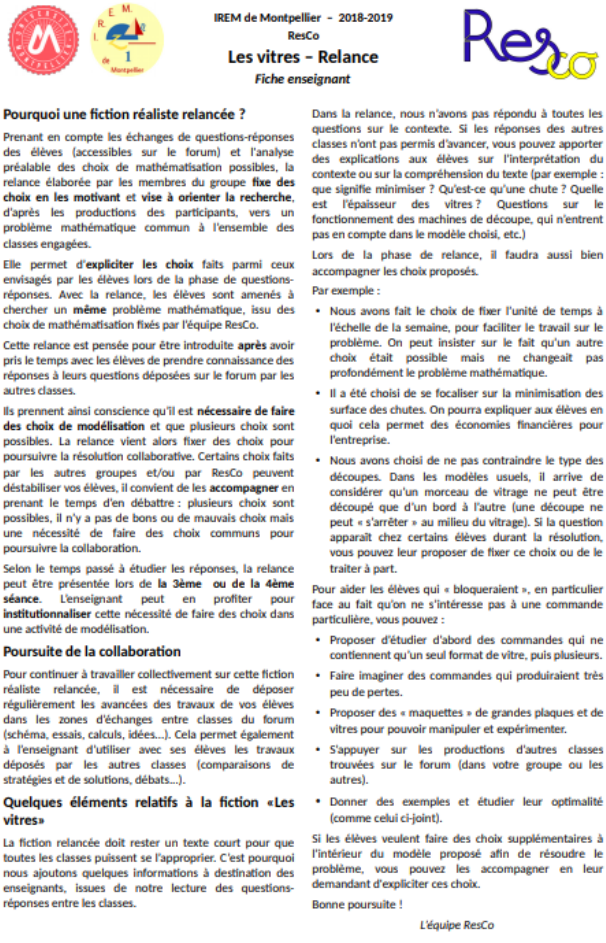
Dans le choix de modèle proposé :

- Le nombre de machines n'a pas d'importance.
- On dispose d'autant de grandes plaques que nécessaire pour produire les vitres commandées.
- On ne tient pas compte de la casse possible des vitres lors des manipulations.

Le problème commun sur lequel vous allez tous chercher est donc celui de trouver une méthode pour minimiser la surface totale des chutes selon les commandes chaque semaine.

J'attends avec impatience de lire vos recherches, dans vos échanges sur le forum !

Simon Modeste



IREM de Montpellier - 2018-2019
ResCo

Les vitres – Relance

Fiche enseignant

Resco

Pourquoi une fiction réaliste relancée ?

Prenant en compte les échanges de questions-réponses des élèves (accessibles sur le forum) et l'analyse préalable des choix de mathématisation possibles, la relance élaborée par les membres du groupe **fixe des choix en les motivant** et **vise à orienter la recherche**, d'après les productions des participants, vers un problème mathématique commun à l'ensemble des classes engagées.

Elle permet d'**expliciter les choix** faits parmi ceux envisagés par les élèves lors de la phase de questions-réponses. Avec la relance, les élèves sont amenés à chercher un **même** problème mathématique, issu des choix de mathématisation fixés par l'équipe ResCo.

Cette relance est pensée pour être introduite **après** avoir pris le temps avec les élèves de prendre connaissance des réponses à leurs questions déposées sur le forum par les autres classes.

Ils prennent ainsi conscience qu'il est **nécessaire de faire des choix de modélisation** et que plusieurs choix sont possibles. La relance vient alors fixer des choix pour poursuivre la résolution collaborative. Certains choix faits par les autres groupes et/ou par ResCo peuvent déstabiliser vos élèves, il convient de les **accompagner** en prenant le temps d'en débattre : plusieurs choix sont possibles, il n'y a pas de bons ou de mauvais choix mais une nécessité de faire des choix communs pour poursuivre la collaboration.

Selon le temps passé à étudier les réponses, la relance peut être présentée lors de **la 3ème ou de la 4ème séance**. L'enseignant peut en profiter pour **institutionnaliser** cette nécessité de faire des choix dans une activité de modélisation.

Poursuite de la collaboration

Pour continuer à travailler collectivement sur cette fiction réaliste relancée, il est nécessaire de déposer régulièrement les avancées des travaux de vos élèves dans les zones d'échanges entre classes du forum (schéma, essais, calculs, idées...). Cela permet également à l'enseignant d'utiliser avec ses élèves les travaux déposés par les autres classes (comparaisons de stratégies et de solutions, débats...).

Quelques éléments relatifs à la fiction «Les vitres»

La fiction relancée doit rester un texte court pour que toutes les classes puissent se l'approprier. C'est pourquoi nous ajoutons quelques informations à destination des enseignants, issues de notre lecture des questions-réponses entre les classes.

Dans la relance, nous n'avons pas répondu à toutes les questions sur le contexte. Si les réponses des autres classes n'ont pas permis d'avancer, vous pouvez apporter des explications aux élèves sur l'interprétation du contexte ou sur la compréhension du texte (par exemple : que signifie minimiser ? Qu'est-ce qu'une chute ? Quelle est l'épaisseur des vitres ? Questions sur le fonctionnement des machines de découpe, qui n'entrent pas en compte dans le modèle choisi, etc.)

Lors de la phase de relance, il faudra aussi bien accompagner les choix proposés.

Par exemple :

- Nous avons fait le choix de fixer l'unité de temps à l'échelle de la semaine, pour faciliter le travail sur le problème. On peut insister sur le fait qu'un autre choix était possible mais ne changeait pas profondément le problème mathématique.
- Il a été choisi de se focaliser sur la minimisation des surface des chutes. On pourra expliquer aux élèves en quoi cela permet des économies financières pour l'entreprise.
- Nous avons choisi de ne pas contraindre le type des découpes. Dans les modèles usuels, il arrive de considérer qu'un morceau de vitrage ne peut être découpé que d'un bord à l'autre (une découpe ne peut « s'arrêter » au milieu du vitrage). Si la question apparaît chez certains élèves durant la résolution, vous pouvez leur proposer de fixer ce choix ou de le traiter à part.

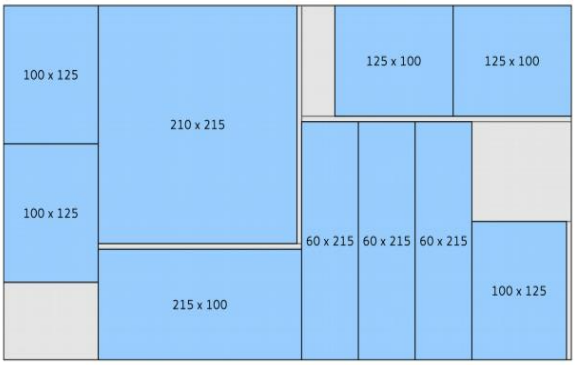
Pour aider les élèves qui « bloqueraient », en particulier face au fait qu'on ne s'intéresse pas à une commande particulière, vous pouvez :

- Proposer d'étudier d'abord des commandes qui ne contiennent qu'un seul format de vitre, puis plusieurs.
- Faire imaginer des commandes qui produiraient très peu de pertes.
- Proposer des « maquettes » de grandes plaques et de vitres pour pouvoir manipuler et expérimenter.
- S'appuyer sur les productions d'autres classes trouvées sur le forum (dans votre groupe ou les autres).
- Donner des exemples et étudier leur optimalité (comme celui ci-joint).

Si les élèves veulent faire des choix supplémentaires à l'intérieur du modèle proposé afin de résoudre le problème, vous pouvez les accompagner en leur demandant d'expliciter ces choix.

Bonne poursuite !

L'équipe ResCo



Fiction relancée élève et fiction relancée enseignants présentées durant l'atelier

3. Clôture du dispositif

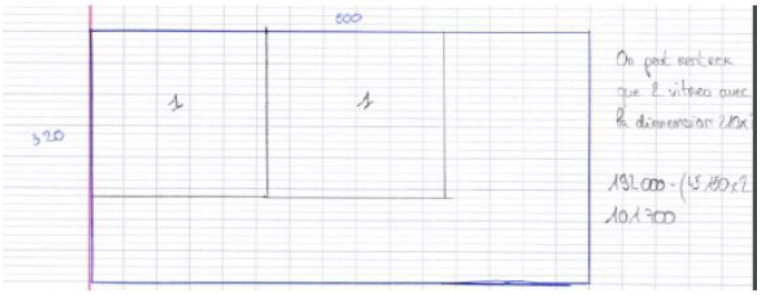
Elle permet d'accompagner les enseignants et les élèves pour conclure la session en leur fournissant généralement :

- Une résolution experte du problème.
- Un récapitulatif des procédures de résolution mises en œuvre par les élèves.
- Un bilan des notions mathématiques pouvant être mises en jeu par les élèves.

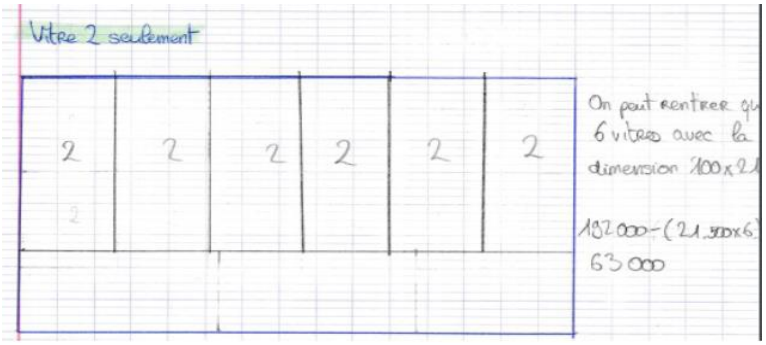
IV - LA FICTION DANS LES CLASSES

Un choix retenu :

- Quelles dimensions des vitres permettent de paver au mieux la grande plaque en n'utilisant qu'un format de vitres ?
- Recherche de diviseurs de la largeur et de la longueur de la plaque.
- Lien entre la largeur et la longueur de la plaque : une optimisation sur la longueur ne fonctionne pas forcément sur la largeur de la plaque.
- Avec des grandes vitres (format 1) :



- Avec des vitres moyennes (format 2) :



Un autre choix retenu :
En utilisant plusieurs formats de vitres :

- décomposition de la largeur et / ou de la longueur de la plaque en multiples des dimensions des vitres choisies ou approximation.
- lien entre la largeur et la longueur de la plaque.

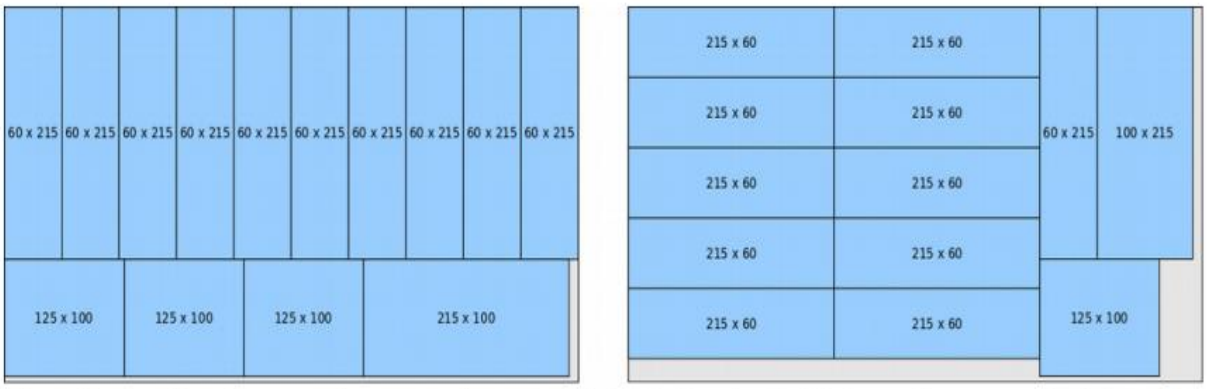
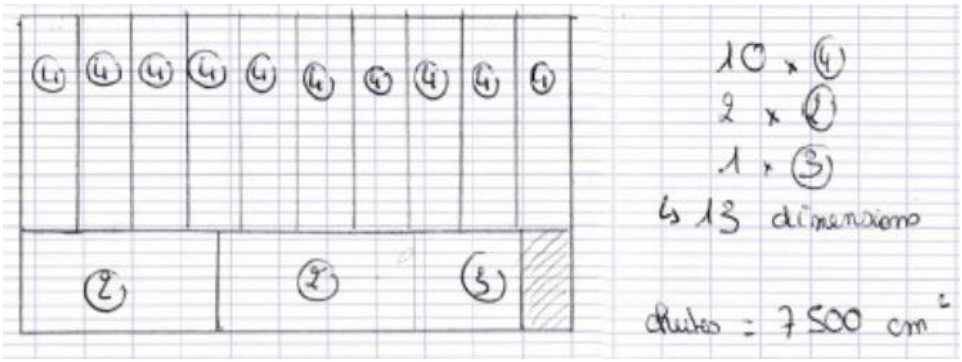
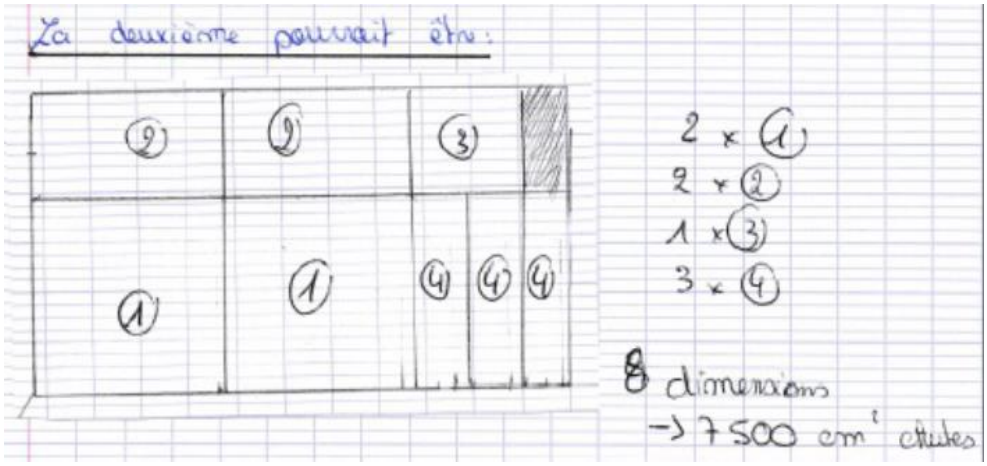
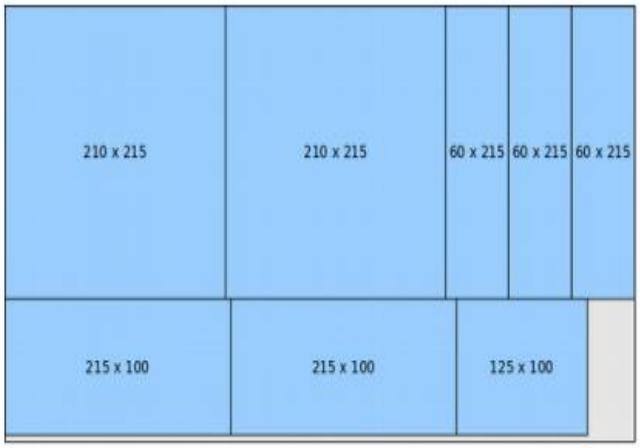


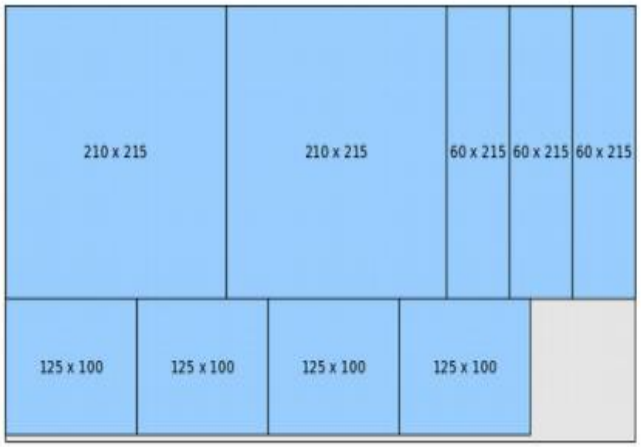
Figure 13. Deux dispositions pour des commandes contenant plus de 10 rectangles (d). La première a une perte de 0,4 m², la deuxième de 1,61 m².



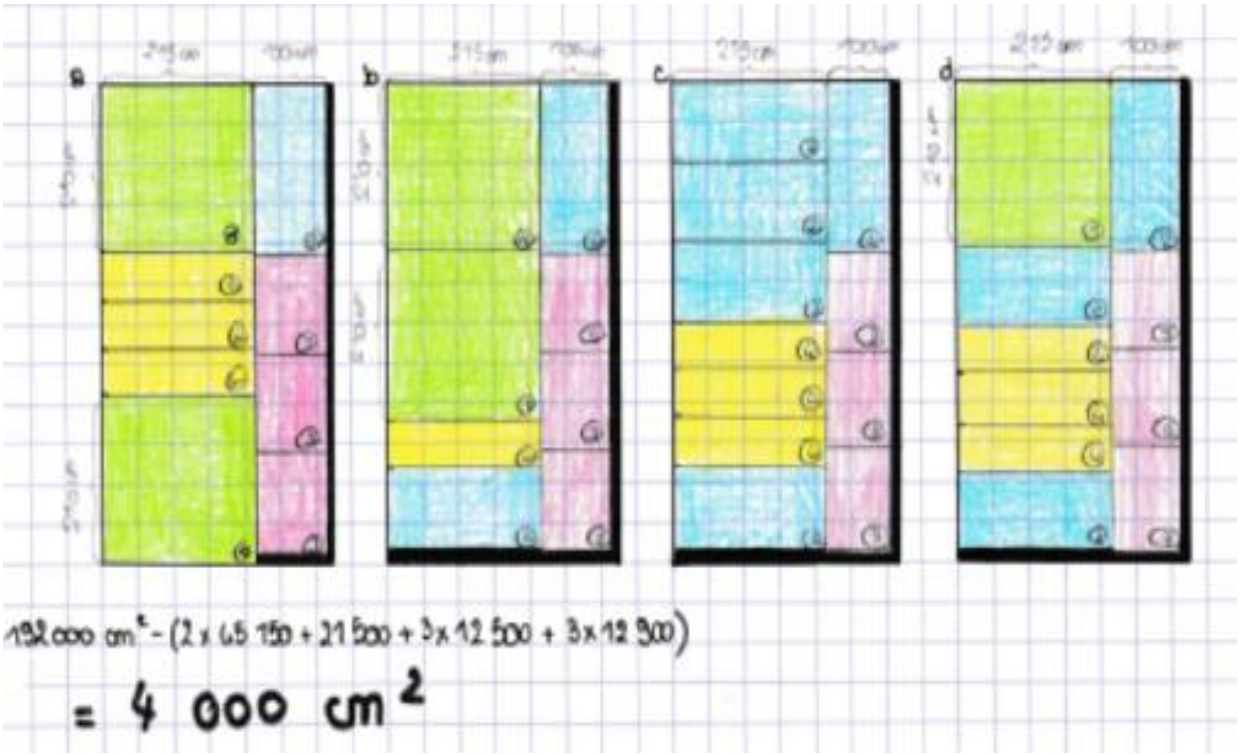
- trouver une décomposition de la largeur de la plaque







- essayer de réaliser des bandes de vitres et les répéter plusieurs fois (avec ou sans panachage).



Autre traitement du problème :

- Calcul des aires de chaque vitre puis estimation d'un majorant du nombre de vitres qui rentrent dans la plaque.

Exemple : on ne peut pas mettre plus de 4 grandes vitres dans la plaque.
Or, en étudiant les dimensions largeur et longueur, on se rend compte rapidement qu'il ne peut y en avoir que 2 maximum. Le fait numérique est simplifié, mais il reste encore à affiner la solution.

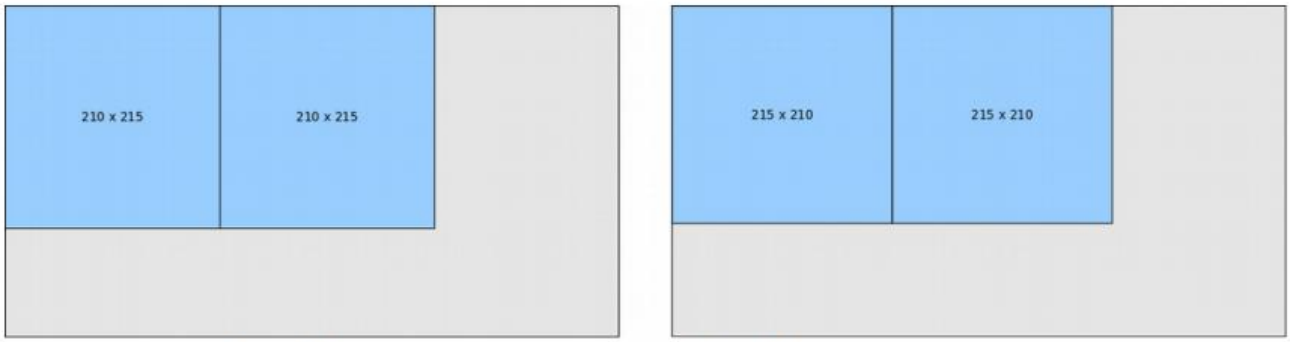
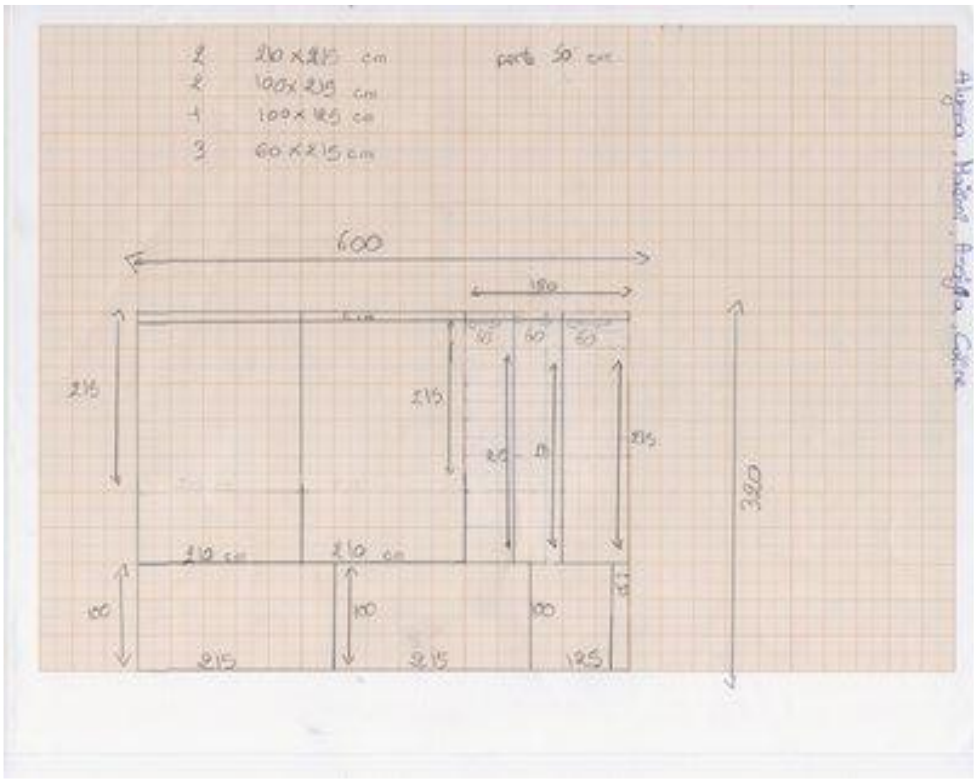


Figure 5. Deux dispositions pour placer un maximum de vitres (a) dans une plaque.

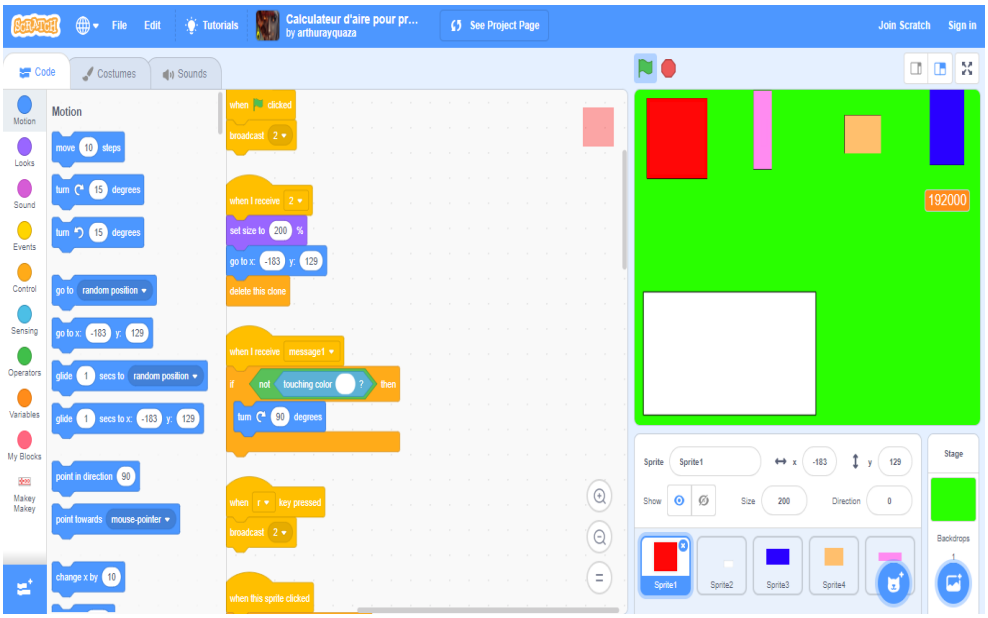
Autres exemples de productions d'élèves :

En Sixième :

Nous avons cherché à améliorer les différents plans fournis ou obtenus (ci-dessous les résultats).
D'autre part nous avons cherché à calculer les pertes.
Pour la majorité d'entre nous, le meilleur plan est le n°1 et d'après nos calculs l'aire des pertes est de 7500 cm².



En Cinquième :



Nos pistes de recherches :

2 groupes ont décidés de faire une recherche avec une maquette.

Nous avons opté pour une échelle au 1/10ème.

Nous avons d'abord testé des découpes avec une seule taille de vitres. (les calculs sont faits)

Puis nous avons essayé de composer des découpes en mixant les tailles de coupes. (les calculs seront faits jeudi)

En parallèle, un groupe a opté pour les calculs, ils se sont finalement associés au 2 groupes précédents pour mettre en calcul les découpes qu'ils avaient composés.

Un dernier groupe essaie de composer les découpes sur Géogébra car nous disposons de tablettes, mais leurs tracés sont moins avancés.

Voici ce que nous avons testé : Nous avons calculé l'aire de la grande plaque : 192 000 cm²

Composition découpe	Aire des vitres découpées (cm²)	Aire des chutes (cm²)
2 x (210 x 215)	90 300	101 700
8 x (100 x 215)	172 000	**20 000**
13 x (60 x215)	167 700	24 300
12 x (100 x 125)	150 000	42 000
2 x (210 x 215) 7 x (100 x 125)	177 800	**14 200**
2 x (210 x 215) 3 x (100 x 125) 2 x (100 x 215)	170 800	21 200
2 x (210 x 215) 3 x (100 x 125) 1 x (100 x 215) 2 x (60 x 215)	175 100	16 900
2 x (210 x 215) 4 x (100 x 125) 1 x (100 x 215) 1 x (60 x 215)	174 700	17 300
1 x (210 x 215) 3 x (100 x 125) 5 x (100 x 215)	190 150	**1 850**
4 x (100 x 125) 5 x (100 x 215) 3 x (60 x 215)	182 900	**9 100**
5 x (100 x 125) 6 x (100 x 215)	179 000	**13 000**
1 x (210 x 215) 2 x (100 x 215) 3 x (60 x 215) 5 x (100 x 125)	189 350	**2 650**

Composition découpe	Aire des vitres découpées (cm²)	Aire des chutes (cm²)
1 x (210 x 215) 3 x (100 x 215) 3 x (60 x 215) 3 x (100 x 125)	185 850	**6 150**
1 x (210 x 215) 4 x (100 x 215) 3 x (60 x 215) 1 x (100 x 125)	182 350	9 650
4 x (100 x 215) 6 x (60 x 215) 1 x (100 x 125)	175 900	16 100
3 x (100 x 215) 4 x (60 x 215) 4 x (100 x 125)	166 100	25 900
4 x (100 x 215) 5 x (60 x 215) 3 x (100 x 125)	188 000	**4 000**
3 x (100 x 215) 6 x (60 x 215) 3 x (100 x 125)	179 400	12 600
2 x (210 x 215) 2 x (100 x 215) 1 x (60 x 215) 3 x (100 x 125)	183 700	8 300
2 x (210 x 215) 3 x (100 x 215) 1 x (60 x 215) 1 x (100 x 125)	180 200	11 800
3 x (100 x 215) 6 x (60 x 215) 3 x (100 x 125)	179 400	12 600
5 x (60 x 215) 9 x (100 x 125)	177 000	15 000

Bilan:

- la méthode « maquette » est la plus efficace associée aux calculs: elle a permis de trouver quelques découpes vraiment économiques, mais comment les associer en fonction des commandes ? Elle présente cependant des limites :
  - fastidieuse (longue),
  - avec des erreurs de composition, de calcul, (avec plus de temps nous aurions pu utiliser un tableur pour simplifier les calculs)
  - des répétitions de compositions déjà faites sans être sûrs d'avoir tout essayé.

- Avec géogébra dans le même temps, on n'a fait que 3 simulations : trop long.

On pense que l'entreprise doit utiliser des logiciels qui prennent en compte simultanément : l'aire des différentes vitres et de la plaque, mais aussi les longueurs et les largeurs (car nous avons remarqué que nous mettions 8 x (100 x 215) + 2 x (60 x 215) horizontalement, alors que nous ne parvenions à mettre que 6 x (100 x 215) + 1 x (60 x 215) verticalement), et les commandes.

En Première :

LES VITRES

Lycée JACQUES PREVERT- St Christol lez Alès

SECTION	1TRPT GROUPE C – Classe 3
SEANCE	3ème – 4ème semaine

Les élèves ont choisi de représenter, à l'échelle, la plaque où seront réalisées les découpes.

Puis, en utilisant la même échelle, ils ont reproduit sur une autre feuille les quatre modèles à réaliser, en plusieurs exemplaires chacun.

Le tableau ci-dessous résume les caractéristiques des dimensions réelles et à l'échelle pour chacune des pièces:

		Dimensions réelles			Dimensions à l'échelle	
		Longueur	Largeur	Surface	Longueur	Largeur
		mm	mm	m²	cm	cm
PLAQUE		600	320	0,192	12	6,4
MODELES	N°1	210	215	0,04515	4,2	4,3
	N°2	100	215	0,0215	2	4,3
	N°3	100	125	0,0125	2	2,5
	N°4	60	215	0,0129	1,2	4,3

Ces modèles ont enfin été découpés et ils sont été utilisés pour faire des essais de calepinage, en essayant de réduire au minimum les chutes.

Les solutions retenues ont étés les suivantes:

SOLUTION 1	SOLUTION 2
	

Ensuite nous avons procédé à une comparaison des deux solutions:

SOLUTION 1

		Longueur	Largeur	Surface	Quantité	Surface par modèle	
		mm	mm	m²		m²	
MODELES	N°1	210	215	0,04515	0	0	
	N°2	100	215	0,0215	5	0,1075	
	N°3	100	125	0,0125	5	0,0625	
	N°4	60	215	0,0129	1	0,0129	
					Surface TOT	0,1829	m²
					Chutes	4,7	%

SOLUTION 2

		Longueur	Largeur	Surface	Quantité	Surface par modèle	
		mm	mm	m²		m²	
MODELES	N°1	210	215	0,04515	2	0,0903	
	N°2	100	215	0,0215	2	0,043	
	N°3	100	125	0,0125	1	0,0125	
	N°4	60	215	0,0129	3	0,0387	
					Surface TOT	0,1845	m²
					Chutes	3,9	%

CONCLUSIONS

On constate que la solution 2 présente deux avantages par rapport à la solution 1:

- Tous les modèles apparaissent sur la plaque à découper;
- Les chutes sont moindres (presque 1 % de moins).

La solution 2 a donc été retenue par notre étude.

En Terminale :

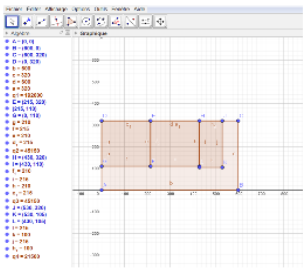
Jeudi 31/01/19

Après avoir lu les réponses postées des 2 groupes à nos questions et le sujet relancé, nous avons commencé à résoudre le problème:

- Au tableau, on a représenté à main levée la plaque aux dimensions 320*600, puis on a placé des vitres de différentes dimensions pour minimiser les chutes

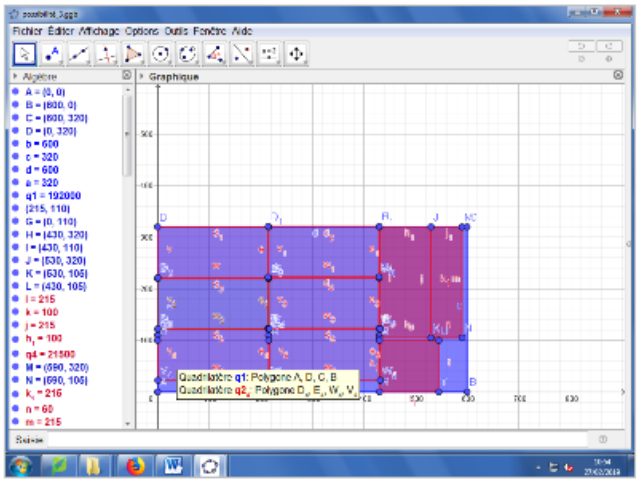
- On a voulu calculer l'aire de la surface des chutes mais le dessin était confus.

- On a donc utilisé Géogébra: on a placé des points des différentes coordonnées pour représenter:
  - La plaque aux dimensions 320*600
  - 2 vitres 215*210
  - 1 vitre 100*215



La suite, la semaine prochaine.....

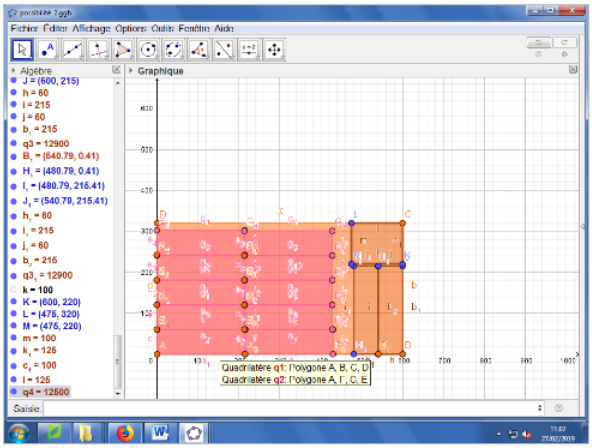
Possibilité 2:



Aire de la surface des chutes : 192000-21500*7-12900-11500=17100cm² = 1,71 m²

Mercredi 27 février

Possibilité 3:



Aire de la surface des chutes : 192000-12900*12-11500=23700cm² = 2,37 m²

On constate que la 1ère possibilité utilise tous les formats de vitres sont utilisés et génèrent le moins de chutes.
La 3ème possibilité utilisent que 2 formats de vitres et génèrent beaucoup de chutes.

V - RÉSUMÉ DE L'ATELIER-TP

Tout au long de l'atelier, des consignes pour l'activité « vivre le dispositif en accéléré » et des questionnements ont permis de faire prendre conscience aux enseignants des points cruciaux nécessaires à une activité de résolution de problèmes en classe.

1. **Première consigne : Commencez à résoudre le problème. Écrivez les questions que vous vous posez à destination d'un autre groupe (1re semaine).**

Les participants ont commencé par prendre connaissance de l'énoncé. Puis, ils ont effectué leurs premières recherches. Rapidement, ils se sont rendu compte qu'il leur manquait certains éléments pour résoudre le problème. Ils ont donc dû poser des questions en fonction des informations qu'il leur manquait. Dans un premier temps, ils ont rédigé leurs questions individuellement. Ensuite, ils ont échangé leurs questions en groupe, ils en ont discuté afin de sélectionner les 10 questions au maximum qui leur semblaient les plus pertinentes.

2. **Deuxième consigne : Échangez vos questions avec un autre groupe et rédigez les réponses aux questions reçues (2e semaine).**

Chaque groupe a reçu les questions d'un autre groupe.
Tout d'abord, les enseignants ont pris connaissance de ces questions.
Cette phase leur a permis de constater que certaines questions étaient celles qu'ils se posaient eux-mêmes mais aussi que les enseignants de l'autre groupe s'étaient posés d'autres questions.
Pour répondre aux questions, les enseignants ont dû faire des choix et proposer leurs hypothèses en argumentant à partir des connaissances ou des idées de chacun. Ainsi, une ou plusieurs réponses ont été rédigées dans les groupes. Ici, les participants ont répondu en s'appuyant sur leurs connaissances personnelles en fonction de leur familiarité avec le thème.

3. Troisième consigne : Récupérez vos questions et prenez connaissance des réponses qui y ont été associées (début de la 3e semaine).

Chaque groupe a récupéré ses questions de départ avec les réponses apportées par l'autre groupe.
Ils ont pris un temps pour en prendre connaissance et pour y réagir.
Ce moment a créé différents effets :

- certaines réponses ont conforté les premières recherches et modélisations envisagées.
- certaines réponses montraient des nouveaux choix ou des options complémentaires de résolution.
- certaines réponses remettaient en cause les premiers choix de modélisation.

4. Premier questionnement : Selon vous, à quoi sert cette phase de questions réponses?

Cette discussion a permis de faire prendre conscience que la phase de questions-réponses permet aux élèves de :

- prendre conscience qu'il est nécessaire de faire des choix de modélisation et que plusieurs choix sont possibles pour résoudre le problème pour passer d'une situation extra-mathématique au monde mathématique.
- émettre des hypothèses simplificatrices (généralement prises en charge par les manuels ou l'enseignant).
- expliciter les choix de modélisations qu'ils ont entrepris.
- prendre connaissance des choix de modélisation faits par les autres classes.

5. Second questionnement : La phase de questions-réponses est-elle porteuse d'apprentissages au regard de la modélisation mathématique ?

A travers les échanges, les participants ont répondu positivement à ce questionnement en concluant que la phase de questions réponses s'appuie sur les collaborations entre classes pour faire entrer les élèves dans une activité de modélisation. De plus, cette phase permet de faire saisir aux élèves la nécessité de la modélisation pour résoudre le problème. Enfin, les échanges de questions-réponses font prendre conscience que la modélisation mathématique implique de faire des choix.

6. Troisième questionnement : Quelles sont les caractéristiques de l'énoncé de la fiction réaliste qui favorisent le travail de modélisation mathématique ?

Le débat a permis de faire émerger les caractéristiques de la fiction réaliste telles qu'elles sont présentées dans la partie III_1.

7. Quatrième questionnement : Quel est le rôle de cette fiction réaliste relancée ?

Le débat a permis de faire émerger les caractéristiques de la fiction réaliste relancée telles qu'elles sont présentées dans la partie III_2.

8. Cinquième questionnement : Quelles stratégies (arithmétiques) pourraient être mises en place par des élèves pour répondre à cet énoncé ?

Cette discussion a fait émerger des stratégies similaires à celles présentées dans la partie IV *La fiction dans les classes*.

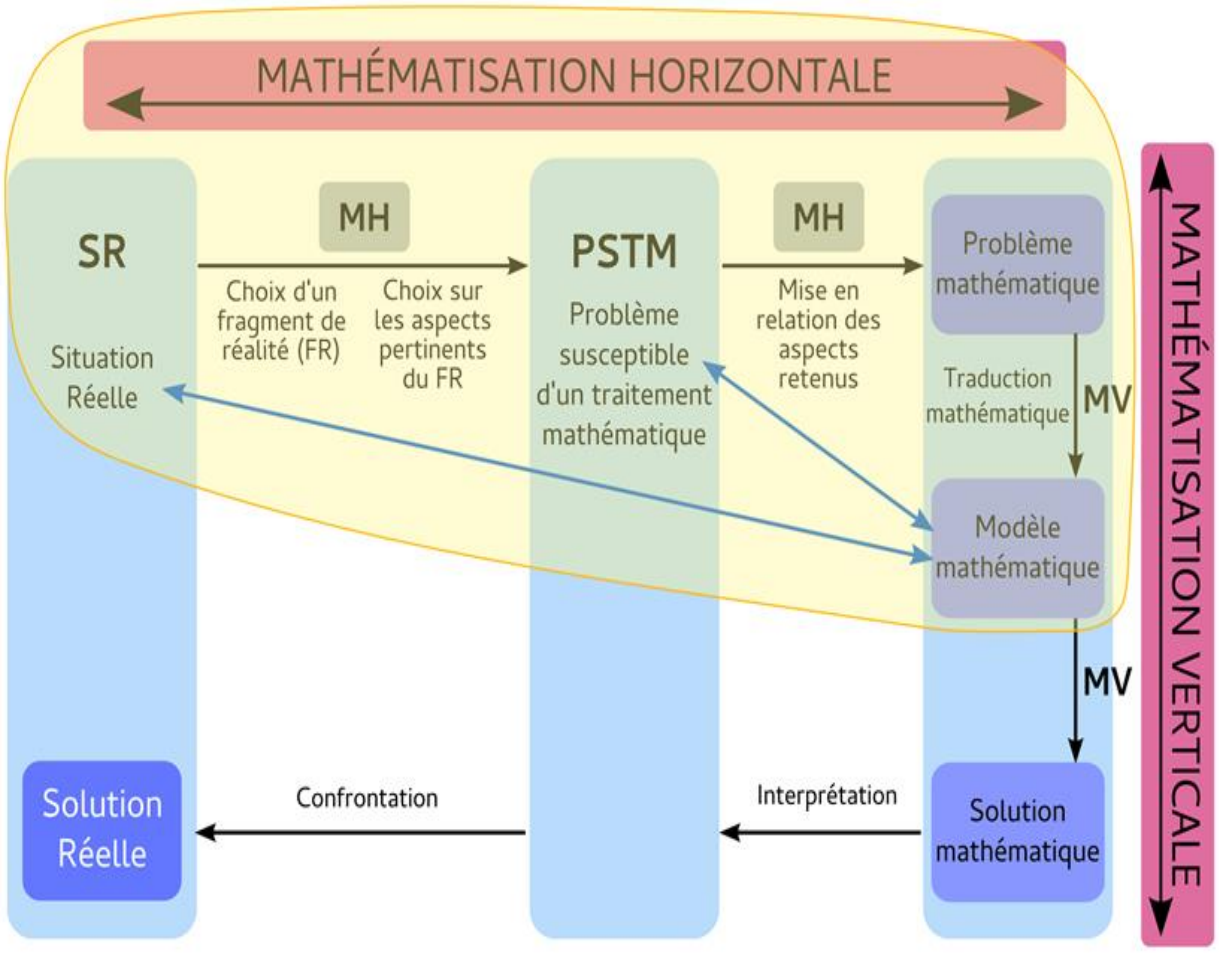
VI - BIBLIOGRAPHIE

Sauter Mireille ; Combes Marie-Claire ; De Crozals Aurélia ; Droniou Jérome ; Lacage Michel ; Saumade Henri ; Théret David ; Groupe ResCo, IREM de Montpellier (2008). Une communauté d'enseignants pour une recherche collaborative de problèmes. . *REPERES-IREM* (numéro 72), p 25 – 45.

Groupe ResCo, IREM de Montpellier (juillet 2014). La résolution collaborative de problèmes comme modalité de la démarche d'investigation. *REPERES-IREM* (numéro 96), p 73 - 96.

Sonia Yvain-Prébiski (2018). Étude de la transposition à la classe de pratiques de chercheurs en modélisation mathématique dans les sciences du vivant. Analyse des conditions de la dévolution de la mathématisation horizontale aux élèves. *HAL Thèses*.

VII - ANNEXE 1 : ASPECTS THÉORIQUES

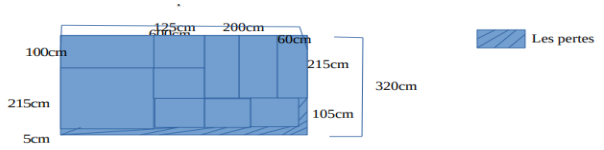
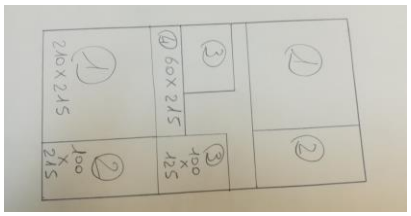


VIII - ANNEXE 2 : EXEMPLES DE QUESTIONS D'ÉLÈVES (1ÈRE SEMAINE DU DISPOSITIF RESCO)

Identifications de grandeurs pertinentes	Recherche d'un modèle (mathématique)	Questionnements d'éléments de contexte
Combien y a-t-il de vitres commandées selon les dimensions ?	Combien de vitres peut-on faire sur une plaque ?	Est-ce qu'on découpe de bord à bord ? Ou en plein milieu ?
Peut-on stocker plusieurs verres en même temps ? Si oui, combien ?	Quel calcul doit-on faire avec les 4 dimensions des petites vitres pour obtenir les dimensions de la grande vitre ?	Peut-on recycler les chutes ?

VIII - ANNEXE 3 : EXEMPLES DE QUESTIONS D'ÉLÈVES (2E SEMAINE DU DISPOSITIF RESCO)

A propos du contexte	Concernant la pertinence de la question
Peut-on faire fondre les chutes de verre pour refaire des plaques ? Oui nous pouvons faire refondre les chutes à partir du moment où le coût est inférieur à l'achat d'une plaque neuve.	Faut-il tenir compte du salaire des employés ? Non, on pense que ça ne présente pas d'intérêt.
Comment les machines s'adaptent-elles aux dimensions des vitres ? Grace à un logiciel de commande numérique.	Combien d'employés ? Hors sujet.
Quelles sont les dimensions les moins demandées ? Nous n'avons pas accès au livret des commandes. Et ça peut dépendre des saisons.	Quel type de verre coupe-t-on ? Peu importe, on est obligé de négliger ce détail pour résoudre.
Faut-il laisser une marge pour polir le verre ? Si la découpe est nette (c'est-à-dire si la machine est performante), on ne devrait pas laisser de marge.	Quelles sont les demandes de dimensions les plus fréquentes ? On ne sait pas mais ça pourrait nous donner une indication pour optimiser notre réponse.

À propos du choix de modèle	À propos du choix des grandeurs
Peut-on faire une grande plaque pour chacune des 4 dimensions à découper ? Oui nous avons répondu à l'aide du schéma ci-dessous. 	Combien peut-on faire rentrer de vitres rectangulaires des 4 différentes dimensions citées dans l'énoncé dans une grande plaque rectangulaire de 600cm*320cm ? Selon votre schéma 7, mais il faudrait voir si on peut faire plus (il s'agit du but de l'étude). 
On demande de proposer un type de « méthode » : Est-ce une démarche mathématique ? Est-ce une programmation de la machine qui va couper ? On peut envisager à la fois une étude mathématique et un algorithme qui aidera à la programmation.	Combien de vitres peut-on découper dans une plaque de 600 cm x 320 cm ? Possibilité n°1 : On peut découper 12 vitres de dimension 100 cm x 125 cm. Possibilité n°2 : On peut découper 2 vitres de 100 cm x 215 cm + 3 vitres de 60 cm x 215 cm. Possibilité n°3 : On peut découper 10 vitres de 60 cm x 215 cm. Possibilité n°4 : On peut découper 2 vitres de 210 cm x 215 cm. Possibilité n°5 : On peut découper 12 vitres de 100 cm x 125 cm.
Est-ce qu'on est obligé d'avoir toujours les quatre dimensions sur les grandes plaques ou juste une partie ? Non, nous ne sommes pas obligés d'avoir toujours les 4 dimensions, mais ça dépend du stock disponible et de la commande.	Quel est le détail des commandes ? Détail de commandes envisageables n°1: - 8 vitres de dimensions 210 cm x 215 cm. - 20 vitres de dimensions 100 cm x 215 cm. - 10 vitres de dimensions 100 cm x 125 cm. - 15 vitres de dimensions 60 cm x 215 cm. Détail de commandes envisageables N°2: - 30 vitres de dimensions 210 cm x 215 cm. - 50 vitres de dimensions 100 cm x 215 cm. - 70 vitres de dimensions 100 cm x 125 cm. - 45 vitres de dimensions 60 cm x 215 cm.

MÉTHODES ET PRATIQUES ARITHMÉTIQUES DU XVI^{e} SIÈCLE

Frédéric MÉTIN
Formateur INSPÉ, UNIVERSITE DE BOURGOGNE
IREM de Dijon
Frederic.metin01@u-bourgogne.fr

Résumé
Les ouvrages d'arithmétique de la Renaissance (souvent qualifiés d'arithmétiques commerciales) initient le nouveau lectorat du 16e siècle à la numération décimale de position, ainsi qu'à de nombreuses méthodes de résolution de problèmes monétaires ou financiers dépassant les simples questions commerciales. Basées sur la « règle de trois » (qualifiée comme telle), ces méthodes et pratiques laissent peu de place aux raisonnements, pourtant nécessaires aux lecteurices modernes pour les comprendre. Faisant suite à l'atelier, l'article propose une exploration de ces anciennes méthodes, ainsi qu'une illustration des manipulations des jetons de compte, qui permettaient même aux analphabètes de calculer.

Le premier plan de Bordeaux, établi en 1565, l'a été par un humaniste saintongeais, Elie Vinet (1509-1587), qui allait devenir célèbre comme historien du Bordeaux de l'antiquité. Vinet est pour nous bien davantage qu'un simple érudit, car en tant que Principal du collège de Guyenne au temps de Montaigne, il eut à cœur d'y restaurer l'apprentissage des sciences, particulièrement de l'arithmétique. Dans le programme des études qu'il conçoit pour le collège de Guyenne (Vinet, 1583), il mentionne clairement l'apprentissage des *Éléments* d'Euclide et des quatre disciplines du *quadrivium* (arithmétique, géométrie, musique et astronomie), qui complètent celles du *trivium* (grammaire, rhétorique et dialectique) pour former les sept arts libéraux de l'enseignement médiéval. Il a d'ailleurs déjà publié deux ouvrages qui ont pu servir de supports à son enseignement : un *Quadrivium* d'après Michel Psellos (Vinet, 1553) et une *Logistica* (Vinet, 1573), comprenant la numération décimale, les opérations sur les entiers et les radicaux, et enfin les rapports et proportions.

L'objectif principal de ces manuels est d'enseigner la pratique de la numération décimale de position et les techniques opératoires qui en découlent à des étudiants maîtrisant le latin et destinés pour la plupart à l'état ecclésiastique. L'arithmétique en jeu ici est directement issue des mathématiques grecques qui ne peuvent être abordées que par des érudits comme les étudiants des collèges de l'époque. Il s'agit donc d'une discipline théorique inscrite dans une vision métaphysique du monde et de la réalité. Nous en voulons pour preuve cet extrait de l'*Arithmétique* de Jacques Peletier du Mans (Peletier, 1554), dont nous avons jugé l'*ortografe françoese* plus facile à décrypter que le latin de Vinet :

> *ARITMETIQVE sẹlon l'ordrẹ droẹt et naturẹl, ẹt la prẹmierẹ des quatrẹ partiẹs dẹ Matematiquẹ : E ẹt cẹllẹ qui anseignẹ la suitẹ, la propriete e la prattiquẹ des Nombrẹs : commẹ la Musiquẹ des Tons, la Geometriẹ des Lignẹs, Supẹrficẹs e Cors : L'Astronomiẹ des cors e mouuẹmans celestẹs. L'Aritmetiquẹ e Musiquẹ s'antrẹtienẹt, e ont toutẹs deus pour suget la Quātite Discrettẹ (Peletier, 1554, p. 12).*

Dans cet esprit, les divers composants du savoir mathématique doivent être intimement liés dans un corpus ordonné de manière à refléter l'unité du monde. La définition du nombre (entier) est alors conforme à la doctrine pythagoricienne :

> *Nombre donq ét une quantite composee de plusieurs Vnitez : Comme 2, 3, 4, 5, 6, e tous autres sans fin : Car il ne se peùt donner Nombre si grand, qui ne se puisse augmanter d'vn […] L'Vnite, qui represante le Point an Geometrie, n'ét point Nombre, mes seulemant origine de Nombre. Qui plus ét, origine de soe-méme : Car celle méme ét sa Multiplication, sa Diuision, sa Racine, son Quarre, son Cube (Peletier, 1554, p. 12-13).*

Cependant, en quoi cette vision du nombre est-elle utile aux commerçants, aux artisans, aux jaugeurs et autres mesureurs auxquels Stevin adressera sa *Disme* à la fin du siècle ? Ceux-ci n'ont aucun intérêt à connaître les catégories du nombre « perœmantper, perœmantnomper, e non perœmantper »[1] de Peletier, pas plus que les dénominations des proportions « superparticuliere, sesquiseconde, sesquitierce »[2], etc.

Ainsi, pour l'utilité pratique des diverses activités numériques humaines, il était nécessaire que soient rédigés des ouvrages de référence dans la langue commune des praticiens des comptes et des calculs, et non celle des savants. Les nombreux traités d'arithmétique commerciale qui subsistent de cette époque témoignent à la fois de la demande et de l'offre d'une formation mathématique pour tous ces praticiens, ainsi que pour les maîtres d'arithmétique qui se chargeraient de guider les débutants (Spiesser, 2008).

I - UNE PRATIQUE « BRIÈVE ET FACILE » ?

Soyons clair, les ouvrages d'arithmétique pratique de la Renaissance puisent à la fois aux deux registres théorique et pratique. Difficile en effet d'expliquer la tenue de livres de comptes ou les règles compliquées des échanges commerciaux sans passer par l'écrit, et sans fournir de cadre théorique, même minimal. Mais d'un autre côté, comment mettre ces contenus difficiles à la portée de personnes non-érudites ? Les titres des ouvrages vantent « la pratique, la plus briève et facille, qui ait esté encore mise en lumiere » (Denorry, 1574) ou promettent de « beaulx exemples et pratiques » (Anonyme, 1510), mais nous allons voir que l'élémentaire côtoie le plus ardu dans ce corpus assez disparate, comme devait l'être l'ensemble des lecteurs auxquels s'adressaient les auteurs.

Parmi ces nombreux ouvrages, nous avons choisi de présenter ceux que nous utilisons à la fois dans la formation initiale et continue des enseignants et dans des animations grand public, pour leur côté attrayant et dépaysant. En effet, lorsqu'il s'agit de réfléchir à notre propre lien à la discipline, il est souvent bénéfique de mettre les savoirs que nous pensons maîtriser à l'épreuve de leurs formulations anciennes que nous n'arrivons pas toujours à reconnaître.

[1] Dans la nomenclature pythagoricienne (Berthier, 1978) : pairement pair, pairement impair et impairement pair, catégories de nombres qui se traduisent respectivement par : puissance de 2, double d'un nombre impair et multiple impair d'une puissance de 2 supérieure ou égale à 2^2.

[2] De même, dans la théorie pythagoricienne (Berthier, 1978), les rapports superparticuliers sont ceux qu'entretiennent deux entiers consécutifs (comme les rapports de 3 à 2, de 4 à 3, de 5 à 4, etc.), et parmi ceux-ci, le rapport sesquialtère, que Peletier nomme sesquisecond, est le rapport de 3 à 2, le sesquitierce celui de 4 à 3 et ainsi de suite.

Nos lecteurices trouveront donc dans les exemples qui suivent toute une variété de méthodes oubliées et/ou difficilement déchiffrable d'un premier regard superficiel. Parfois il n'est question que de les reformuler dans des termes familiers, et c'est alors que l'on mesure toute l'économie, la simplification et la clarté qu'apporte l'algèbre. Parfois, il faut étudier les textes plus en profondeur pour y découvrir des techniques opératoires étranges ou des résolutions d'équations sans utilisation d'inconnues, du moins sans calcul littéral, mais là encore se manifeste la « libération de l'algèbre » selon l'expression de Claude Merker[3]. Au-delà de leur caractère pittoresque, ces textes, élémentaires ou non, sont l'occasion d'un questionnement des certitudes liées à la maîtrise des connaissances, ce qui les rend encore plus précieux en formation des enseignants, lorsqu'il s'agit d'interroger notre rapport aux mathématiques. Nous espérons que les quelques extraits donneront envie aux lecteurices d'examiner les ouvrages présentés (tous sont disponibles en ligne).

1. Les tables de multiplication selon Peletier

Jacques Peletier du Mans est aux côtés de Ronsard, l'un des poètes de la Pléiade, un réformateur créatif et défenseur de la langue française face au latin de l'élite. Médecin et mathématicien acquis aux idées de la Réforme, il cherche à diffuser le savoir mathématique auprès d'un public élargi aux besoins nouveaux, par exemple les bourgeois-marchands sédentarisés des grandes villes comme Lyon, Paris ou Rouen (Spiesser, 2008). Mais ne croyez pas qu'il vive dans un mode exclusivement masculin : parmi les poètes que fréquentait Peletier, la lyonnaise Louise Labé semble avoir occupé une place proéminente.

Outre ses recueils de poésie, Peletier a publié quelques traités de mathématiques élémentaires, parmi lesquels un abrégé des six premiers livres des *Éléments* d'Euclide, une géométrie pratique et un traité d'algèbre dans lequel l'on trouve pour l'une des premières fois l'usage des lettres dans la résolution des systèmes d'équations à plusieurs inconnues.

Dans l'*Arithmétique*, Peletier exprime clairement son projet : « jɇ trouvɇ qu'il n'ɇt pas impossiblɇ d'ɇtrɇ facilɇ é brief tout ansamblɇ » (Peletier, 1554, p. 77). Ce souci de clarté se traduit par la progression suivie dans le Premier Livre, que ne réprouveraient pas les enseignants actuels et qui semble universelle : numération, addition, soustraction, multiplication et division, assorties du vocabulaire et des « preuves » de ces opérations, le tout expliqué pas à pas. Cependant, quand il en vient à la « Multiplicacion des Antiers », Peletier n'expose pas immédiatement la table de multiplication habituelle. Au lieu de cela, il donne une méthode de calcul d'un produit de deux nombres à un chiffre, avec l'exemple suivant :

> *Examplɇ : Jɇ veù multiplier 7 par 6 : J'otɇ 7 dɇ 10 restɇt 3 : samblablɇmant 6 dɇ 10 restɇt 4 : Aprɇs, jɇ dì einsi, 3 foɇs 4 font 12 ; j'ecrì 2 pour ma prɇmierɇ figurɇ : Puis j'ajoutɇ 6 avɇc 7, ce sont 13 : dont jɇ gettɇ la sɇcondɇ figurɇ, 1, e pràn la prɇmierɇ 3 : a laquelɇ j'ajoutɇ l'unite gardeɇ 1, cɇ sont 4, quɇ j'ecrì aprɇs 2. Einsi, jɇ trouvɇ 42, qui ɇt la valeur de 7 multiplie par 6 (Peletier, 1554, p. 33).*

Bien que le texte en soit très bien écrit, tout n'est peut-être pas parfaitement clair (en tout cas pour des yeux modernes) dans l'exposé de cette technique. Dans son souci de facilité et de brièveté, Peletier offre une disposition schématique (Figure 1) qui permet de visualiser les opérations successives :

[3] Expression mentionnée oralement par Claude Merker de l'IREM de Besançon au cours du colloque de la CII Épistémologie et Histoire à Lille en 1990.

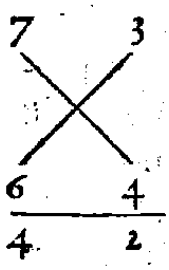


Figure 1. Peletier 1554

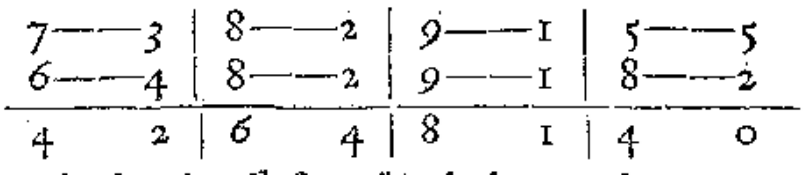


Figure 2. Vinet, 1573

Pour la multiplication de 7 par 6, on dispose ces deux nombres dans une même colonne, puis leurs compléments à 10 (qui sont respectivement 3 et 4) dans une seconde colonne à droite de la première. Le produit des deux compléments donne 12, dont on pose 2 et retient 1 ; la croix tracée permet de se rappeler que le chiffre des dizaines est obtenu comme différence de 7 et 4 ou de 6 et 3 (ce qui est toujours la même chose), auquel on ajoute la retenue pour obtenir 4, et finalement : 6 × 7 = 42, étonnant, non ?

Les étudiants (ou les jeunes enseignants) auxquels on demande d'étudier cette méthode s'inquiètent de sa généralité. On peut leur présenter l'extrait de la *Logistica* d'Elie Vinet proposé en Figure 2 (Vinet, 1573, p. 30) pour les convaincre qu'elle semble donner le bon produit dans de nombreux cas. Après avoir ainsi titillé leur curiosité, il ne reste qu'à les lancer dans une démonstration générale utilisant les conventions algébriques !

Cette disposition avait déjà été décrite en Angleterre par Robert Recorde de la même façon, avec la justification suivante : « En ce qui concerne les petits nombres à un chiffre (*dygetes*) inférieurs à 5, ce serait folie d'enseigner quelque règle, voyant que [les multiplications] sont si faciles qu'un enfant peut le faire. » (Recorde, 1543, fol. 47v). Notons qu'en bien des points, Recorde et Peletier ont des profils similaires, en particulier les aptitudes littéraires et le souhait de promouvoir les mathématiques au-delà du cercle des érudits en écrivant des traités en langue commune. Et c'est justement vers Recorde que nous nous tournons maintenant pour examiner une méthode multiplication qui ne nous paraît pas très conventionnelle.

2. Multiplier sans retenue

2.1. Le « truc » de Robert Recorde

Le fameux livre d'arithmétique de Robert Recorde, *The Ground of Artes* (Recorde, 1543), est le premier livre imprimé en Angleterre et en anglais sur ce sujet, si l'on excepte la traduction anglaise de l'*Art et science de arismetique* (Anonyme, 1510), dont on ne connaît que la page de titre et un autre ouvrage dérivé de celui-ci dont une édition complète n'a été découverte qu'en 2005 (Williams, 2012). *The Ground of Artes* reste néanmoins le plus important et le plus diffusé des anciens traités arithmétiques anglais (quarante-deux éditions), son succès ayant probablement été assuré par la qualité et la simplicité de son discours didactique à la portée des débutants. En effet, comme Peletier, Recorde prend soin de détailler chaque étape des algorithmes qu'il présente, et d'assortir ces schémas progressifs de commentaires explicatifs.

L'une des caractéristiques (déroutante pour nous) de la multiplication chez Recorde est l'absence de retenues en cours de calcul si ce n'est lors de l'addition finale, ce que l'on trouve également dans la plupart des livres imprimés à son époque. Recorde énonce la méthode générale Nous avons rassemblé dans la

Figure 3 les schémas qui accompagnent progressivement le texte explicatif de l'exemple donné par Recorde, texte que nous résumons ensuite :

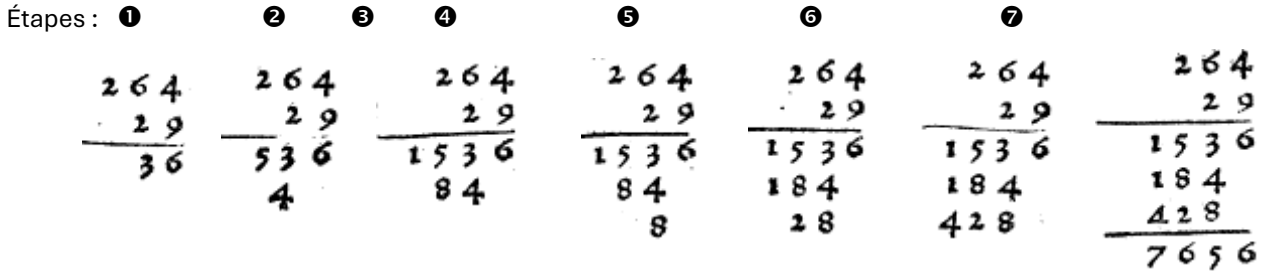


Figure 3. Multiplication de 264 par 29 (Recorde, 1543, 50v-52)

❶ : la multiplication 264 × 29 est posée comme de nos jours et entreprise avec l'algorithme usuel qui permet d'écrire le produit 36 sans retenir le chiffre 3 ;

❷ : ceci engendre un problème technique pour écrire 54, produit de la multiplication de 6 par 9, puisque la place du chiffre 4 est occupée par le chiffre 3 des dizaines du produit précédent ; qu'à cela ne tienne ! L'important pour l'addition finale est que ce 4 se trouve dans la colonne des centaines, on le place donc en dessous du 3. Le 5 se retrouve alors dans la troisième colonne, celle des milliers ;

❸ : de même, les deux chiffres 1 et 8 du produit de 2 par 9 sont placés respectivement dans la colonne des milliers et celle des centaines, le plus haut possible (sans doute pour ne pas occuper plus de lignes que nécessaire).

❹, ❺ et ❻ : le même principe est utilisé pour les multiplications par 2, tous les chiffres des produits étant inscrits sans retenir quoi que ce soit, sur trois lignes au lieu de deux seulement dans la méthode avec retenues.

❼ : l'addition finale est effectuée de manière ordinaire, avec les retenues évidemment, mais celles-ci ne sont pas indiquées.

Pourquoi ce choix de ne pas utiliser les retenues ? Cette question n'est pas judicieuse, car les auteurs du XVI^e^ siècle possédant cette technique n'imaginaient probablement pas que l'on puisse procéder différemment. Quoi qu'il en soit, remarquons que cet algorithme de multiplication ne nécessite pas de la part du calculateur la faculté de mémoriser un chiffre et de l'additionner mentalement à un nombre au cours du processus. La technique de multiplication sans retenue en elle-même est probablement dérivée du calcul *par jalousie* que nous présentons brièvement dans l'ouvrage de Juan de Ortega ci-dessous.

2.2. Quelques variations de Juan de Ortega

On connaît mal la vie de Juan de Ortega, dominicain espagnol né au XV^e^ siècle, si ce n'est qu'il est l'auteur de divers traités dont l'un des premiers ouvrages de mathématiques publiés en espagnol. Imprimé à Lyon faute d'imprimerie en Espagne, le rarissime *Conpusicion de la arte de la arismetica y juntamente de geometria* (Ortega, 1512) sera rapidement reproduit en français sous le titre *Œuvre tressubtille et profitable de lart & science de aristmeticque: & geometrie* (Ortega, 1515), puis dans une version espagnole revue et corrigée, *Tratado subtilissimo de arismetica y de geometria* (Ortega, 1537) mainte fois rééditée en Espagne.

Nous portons un intérêt particulier au chapitre traitant de la multiplication. En effet, après avoir exposé comme Recorde et Peletier la multiplication telle que nous la connaissons, Ortega mentionne trois autres pratiques qu'il expose de manière graphique et sans les commenter, si ce n'est l'indication qu'elles se font sans retenue. Nous reproduisons ci-après (Figures 4, 5 et 6) les trois versions successives de cet extrait, qui présentent chacune la multiplication de 43 060 par 4085, *par jalousie* (cadre de gauche), par une technique équivalente à notre multiplication posée usuelle (à droite) et par une technique intermédiaire utilisant un tableau à double entrée (au centre). Notons que dans les trois éditions, le dispositif de *jalousie* a été gravé sur bois, tandis que les deux autres ont été composés avec des caractères mobiles. La police de caractère utilisée est de type gothique en 1512 et d'un modèle plus arrondi pour la seconde édition lyonnaise en 1515, ainsi qu'en 1537. Les chiffres gravés sur bois sont inspirés de la première police de caractère, comme on le remarque particulièrement pour le chiffre 2. Du point de vue de la gravure, les deux premières versions sont quasiment identiques, mais il ne s'agit pas du même bois car certaines différences de formes dans les signes sont visibles. La troisième gravure reste sur le même modèle, copié sur les deux précédents, mais nous notons toutefois que le graveur de 1537 a gravé les 2 dans le mauvais sens ! Nous examinons maintenant de plus près les trois techniques présentées par Ortega.

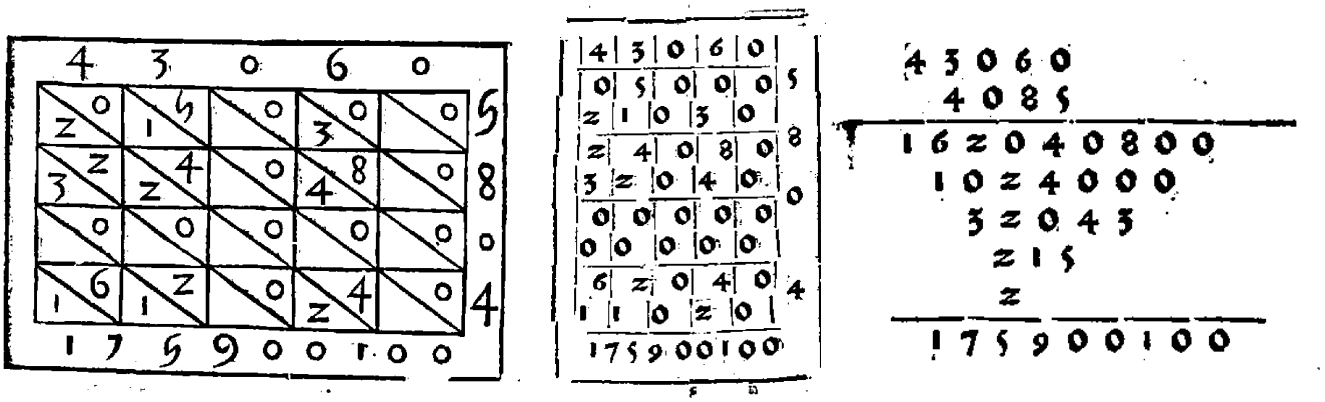


Figure 4. Trois façons de multiplier 43 060 par 5804 (Ortega, 1512, fol. 18v-19)

La multiplication par jalousie

À l'époque d'Ortega, cette technique de multiplication, peut-être d'origine orientale, est déjà connue en Europe car elle a été exposée par divers auteurs dont Luca Pacioli dans son célèbre ouvrage *Summa de arithmetica geometria proportioni & proportionalita* (Chabert et al., 1994, 26-32). Si l'on excepte la contrainte du cadre, nous allons constater qu'elle présente l'avantage de rendre simples et bien lisibles tous les calculs, du fait de l'absence de retenue et de l'organisation spatiale qui prévoit l'exacte place de chacun des chiffres des produits partiels, aussi bien que le regroupement de ceux-ci dans des « colonnes obliques » par ordre de grandeur décimale. Nous décrivons ci-dessous l'usage du dispositif.

Les cellules carrées d'un tableau à double entrée sont divisées en deux par l'une de leurs diagonales, toutes l'étant de la même façon (ici, de haut à gauche en bas à droite) ce qui engendre des lignes obliques comme on le voit sur les figures. Chaque colonne du tableau correspond à un chiffre du multiplicande et chaque ligne à un chiffre du multiplicateur. Les produits partiels (à deux chiffres au maximum) sont inscrits dans la cellule correspondante, celui des dizaines dans la partie basse et celui des unités dans la partie haute. On lit par exemple sur la première ligne 2\0 (= 4 × 5), 1\5 (= 3 × 5), 0 (= 0 × 5), 30 (= 6 × 5) et encore 0.

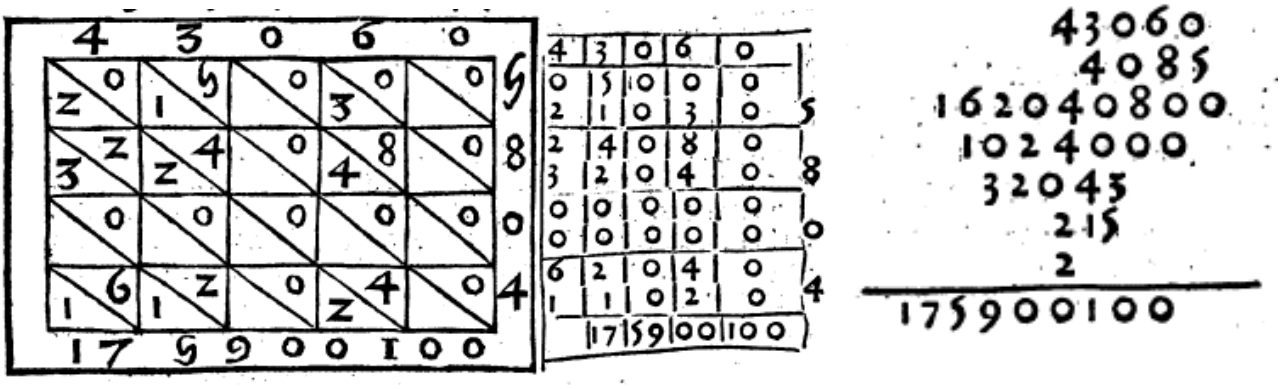


Figure 5. Trois façons de multiplier 43 060 par 5804 (Ortega, 1515, fol. 15v)

La demi-cellule supérieure droite contient le seul nombre contribuant au chiffre des unités du résultat, c'est 0. La demi-cellule inférieure qui lui correspond fait partie de la colonne oblique des dizaines, qui contient deux zéros s'additionnant pour obtenir le résultat 0. La colonne oblique des centaines contient 0, 3, 8 et 0, pour un montant total de 11, donc on conserve le chiffre 1 (de droite) et dont on retient l'autre, ce qui n'est indiqué nulle part sur le schéma. Le principe des retenues n'est donc pas tout à fait inconnu, mais celles-ci ne sont employées que pour les sommes finales, et pas en cours de multiplication.

Nous pouvons remarquer que dans les deux versions initiales imprimées à Lyon, les chiffres du multiplicateur ont été gravés à droite de la grille, ce qui rend impossible l'inscription des chiffres du résultat à l'extrémité des colonnes obliques correspondantes. En principe, le multiplicateur devrait être placé du côté de la grille correspondant aux extrémités supérieures des diagonales et les chiffres du produit sur les deux côtés restants, comme on le voit sur la Figure 6. Le graveur de 1537 a été attentif sur ce point, mais il a quand même gravé les 2 à l'envers !

La multiplication posée en tableau

Pour cette deuxième technique, les illustrations sont composées en caractères d'imprimerie et non plus gravées, et les trois versions sont sensiblement différentes. Longtemps nous avons utilisé en formation celle de la figure 5, lorsque nous n'avions pas accès à la version espagnole de 1512 qui n'était disponible qu'à Madrid. Cette illustration nous laissait perplexe, la disposition des chiffres dans le tableau ne permettant pas de comprendre aisément comment ils étaient additionnés.

Il aura fallu que la Banque d'Espagne mette en ligne la version scannée de l'exemplaire de sa bibliothèque pour confirmer notre intuition que le graveur lyonnais de 1515 ne savait probablement pas ce qu'il composait. En effet, le tableau de 1512 se lit facilement comme une version « redressée » du tableau de *jalousie*, qui laisse clairement apparaître les mêmes alignements obliques et les mêmes contenus numériques (avec l'intégralité des zéros). Le résultat est également disposé de la même façon sous la ligne inférieure du tableau, et le multiplicateur le long du côté droit.

De par sa disposition en colonnes verticales, l'illustration de 1515 prête le flanc à une interprétation moderne, ce qui ne manque jamais en formation initiale ou continue, notre regard étant conditionné par la méthode usuelle de multiplication posée. Évidemment, cela engendre l'incompréhension puisque les sommations verticales ne permettent pas d'obtenir le résultat affiché.

Dans ce contexte, la version de 1537 nous intrigue, car les chiffres du tableau ne sont plus exactement ceux de la grille de *jalousie*. En outre, le nombre de cellules y est réduit par rapport aux deux versions antérieures. On reconnaît les chiffres de la première ligne qui sont les mêmes, les zéros mis à part, que ceux de la première ligne du tableau de jalousie, mais dès la seconde ligne, cela ne convient plus. La quatrième ligne diffère également de son homologue du tableau de *jalousie*.

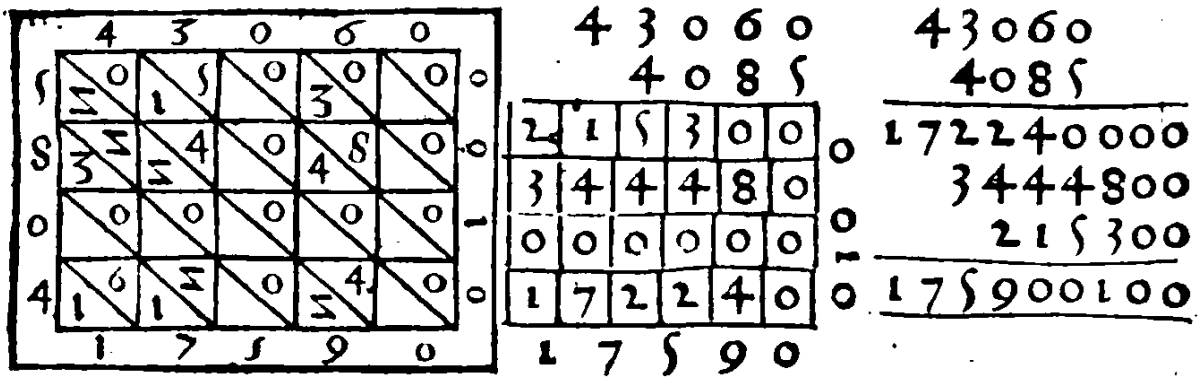


Figure 6. Trois façons de multiplier 43 060 par 5804 (Ortega, 1537, fol. 20)

Il est possible de retrouver un algorithme de calcul cohérent avec la disposition des chiffres de ce tableau, et c'est tout simplement notre technique moderne, comprenant l'usage de retenues : la première ligne est le produit de 43 060 par 5, la seconde par 8 et ainsi de suite. Comme le résultat final est disposé de manière identique à celui du tableau de *jalousie* qui jouxte celui-ci, on comprend que les sommes finales sont effectuées en diagonale, ce qui donne la forme la plus compacte possible pour la multiplication, dans une table carrée sans cellule inutile, si l'on excepte la ligne de zéros.

Cette présentation va constituer une transition idéale vers la multiplication posée qui fait l'objet de la troisième illustration que nous allons analyser.

La multiplication posée « à l'ancienne »

La troisième illustration de la Figure 4 constitue un document qu'il vaut la peine de proposer à des étudiants redécouvrant les mathématiques ou à des enseignants gagnés par la routine. Ceux-ci ont en effet très naturellement tendance à vérifier les résultats des opérations en appliquant mécaniquement l'algorithme usuel de la multiplication, ce qui les laisse perplexes quand ils découvrent que celui-ci ne fonctionne pas du tout ici. Il y a plus de lignes que prévu (tant qu'on ne se penche pas sur la version de 1537), et trop de zéros dès la première ligne.

C'est que contrairement à toute procédure contemporaine, l'auteur entame le calcul par la gauche, avec le produit 4 × 4, dont il inscrit intégralement le résultat 16 en première ligne. Nous retrouvons un algorithme sans retenue comparable à celui de Recorde vu plus haut, dans lequel les chiffres sont placés dans la bonne colonne, à l'endroit où il reste de la place pour les écrire. La présence des zéros et leur placement peut être interprété de plusieurs manières, mais il n'y a pas d'incohérence. Les chiffres sont plutôt correctement alignés verticalement, ce qui donne néanmoins quelques distorsions entre les chiffres des résultats partiels, qui peuvent se trouver assez éloignés les uns des autres. Les seules petites difficultés tiennent à un léger décalage de la ligne du 215 (le 5 devrait être au-dessous du 4) et de celle du résultat.

La comparaison avec l'illustration de 1515 ne laisse plus de doute : le typographe lyonnais ne comprend pas ce qu'il compose et aligne les chiffres sans logique apparente.

En revanche, la version de 1537 témoigne d'une parfaite maîtrise de la technique opératoire. Cette fois-ci, et c'est aussi déstabilisant, la multiplication est effectuée avec retenue, en commençant par le chiffre des milliers du multiplicateur et par le chiffre des unités du multiplicande. Un zéro est ajouté à l'extrémité de chaque ligne à chaque changement de ligne, à moins que les zéros ne soient placés en bloc directement à la fin de chaque ligne en fonction de l'ordre de grandeur du chiffre du multiplicateur traité. Cette fois-ci les alignements verticaux sont tous respectés, et les sommes finales sont identiques à celle du tableau central.

La figure 6 n'ayant pas fait l'objet d'un montage, elle reproduit fidèlement la mise en page originale de l'édition de 1537, qui met en évidence le lien entre les trois techniques de multiplication en promouvant de manière indirecte la troisième. C'est un extrait qui engendre d'intéressantes discussions en formation, en ce qu'il montre une sorte d'évolution d'une technique vers une autre. L'auteur en avait-il conscience ? Dans la mesure où le texte de l'ouvrage reste succinct à propos de ces techniques, et puisqu'il n'y a pas de changement notable entre les trois éditions, il n'est pas possible d'en avoir le cœur net.

II - « RÈGLE DE TROIS » ET AUTRES RÈGLES D'ALGÈBRE

Les ouvrages d'arithmétique pratique que nous étudions ne sont pas tous exclusivement réservés à l'apprentissage de la numération et des opérations à l'usage du commerce. Dans bon nombre d'entre eux, il est aussi question de la résolution de problèmes liés à la pratique marchande. Dans la plupart des cas, ces problèmes sont du premier degré et leur résolution ne nécessite pas le recours à l'algèbre, que probablement bien peu de destinataires des ouvrages auraient été à même de maîtriser. D'ailleurs, c'est jusqu'au XX^{e} siècle que les enfants des écoles primaires apprendront des méthodes purement numériques comme la méthode dite « de fausse position », qui sont largement suffisantes pour la résolution d'équations du premier degré lorsqu'il y a proportionnalité, ce qui est généralement le cas dans le contexte commercial. Comme on le sait, l'introduction du calcul littéral au collège pose problème à beaucoup de jeunes, qui posent souvent la question de son utilité dans « la vraie vie ».

Pour cette partie de notre présentation, et comme nous le faisons en formation initiale et continue, nous puisons à des sources de la seconde moitié du XV^{e} siècle, et particulièrement aux ouvrages de Valentin Mennher (Mennher, 1556), et Edouard Léon Mellema (Mellema, 1582) qui offrent un discours clair et une vue complète sur l'arithmétique commerciale de leur époque (Kool, 1999). Tous deux maîtres d'arithmétique ou comptables exerçant à Anvers, ils publient des ouvrages à l'intention de leurs élèves, dans lesquels ils détaillent et mettent sur le papier un ensemble complet de pratiques de résolution de problèmes faisant toutes appel à la « règle de trois ». Mais de quoi s'agit-il au juste ? Nous citons la définition de Valentin Mennher et quelques applications des deux auteurs.

1. Qu'est-ce que la « règle de trois » ?

Disciple allemand de Christoff Rudolff et adepte de la *Coss* (pratique allemande renaissante du calcul algébrique), Valentin Mennher se fixe à Anvers en 1549 comme maître d'arithmétique et publie divers textes d'arithmétique et de comptabilité, dont nous apprécions la lisibilité, ce qui nous a induit à proposer

des extraits de l'*Arithmétique seconde* en formation continue, tant pour les enseignants de primaire que pour ceux du secondaire. Sa définition de la *règle de trois* nous rappelle qu'il s'agit bien d'une règle, avec un énoncé et des conditions d'application, et non pas de ce que nos étudiants qualifient abusivement de *produit en croix* qui n'est qu'une des propriétés de la proportionnalité. Précisons, pour faciliter la lecture de cette citation, qu'il y est questions d'unités monétaires (*£, ß, d'* : livres, sols et deniers), de poids (dont l'*esterlin*, à rapprocher de l'anglais *sterling*) et qu'il est fondamental que les données correspondantes soient exprimées dans la même unité, ou, selon l'expression de l'époque, réduites en un *nom* commun.

> *La Regle de trois contient 3 choses : ce qu'on demande sçavoir doit estre mis derriere, et la chose qui lui est en nom semblable doibt estre mise devant, & la tierce chose entre deux, qui est au milieu. Et quand l'une de ces 3 ou toutes 3 ont divers noms comme £, ß, d', ou marcs onces esterlins ou livres et onces &c., adonc il faut les reduire en son moindre nom. Quand cela est faict & que le dernier & premier ont noms semblables & que le nombre du milieu est reduict en son moindre nom, adonc il faut multiplier le nombre du milieu par le dernier & le produict partir par le premier nombre, & ce qui en vient de ceste division est le fact qu'on ha demandé et ha semblable nom que celuy du milieu. (Mennher, 1556, partie I, fol. signé Bij)*

Pour illustrer le propos simplement, viennent quelques mises en pratique élémentaires. Premier exemple : « Si 3 aulnes coustent 9 *d'* combien sousteront 36 aulnes ? 3 … 9 … 36 multiplies 36 par 9 & en viendront 324 lesquels divises par 3 et produiront 108 *d'* les mesmes divises par 12 & feront 9 *ß — d'* » ; troisième exemple : « Si une aulne couste *ß* 6 combien cousteront 27 aulnes ? Multiplies 27 par 6 et en viendront 162 *ß* lesquels divises par 20 pour faire en £ et feront 8 £ et 2 *ß*. »

Les textes ne posent pas problème aux lecteurices modernes, si ce n'est la gêne occasionnée par les impératifs se terminant en *s* et les conversions non décimales de monnaie : une livre vaut vingt sols, un sol douze deniers. De même, dans l'exemple bancaire qui suit, il faut savoir que le *daalder* d'argent est l'équivalent du *thaler* allemand, ancêtre du *dollar*. On s'aperçoit à la lecture de l'énoncé que la valeur faciale des pièces n'est pas leur valeur réelle et que le « caissier » doit manier avec aisance les conversions de monnaie pour tirer toujours profit de son activité, du moins ne pas y perdre :

> *Un Cassier doibt recevoir une somme d'argent laquelle on luy presente payer en dalders à* $58\frac{1}{2}$ *qui ne valent que d' 58 ou d'escus à ß 6 d' 9 qui ne valent que ß 6 d' 8. La demande est de laquelle sorte il doibt prendre pour avoir moins de dommage*
>
> $58\frac{1}{2}$ ♦ ♦ 58 ♦ ♦ 100 *faict* $99\ \frac{17}{117}$
>
> 81 ♦ ♦ 80 ♦ ♦ 100 *faict* $98\frac{62}{81}$
>
> *faict* $\frac{400}{1053}$ *pour cent vaut il mieux de prendre des dalders que des escus (Mennher, 1556, partie I, fol. signé Dij)*

Il s'agit donc pour le banquier de comparer la valeur réelle des deux monnaies en les convertissant en deniers (le « moindre nom » de la règle) et ramener leurs valeurs à l'indice 100, afin de savoir en quelle monnaie il a intérêt à être payé. Rappelons que les 6 sols et 9 deniers que vaut un écu sont équivalents à 6 × 12 + 9 = 81 deniers (qui n'en valent en fait ici que 80, ou 6 sols et 8 deniers seulement). Sur chacune des deux lignes, Mennher a soigneusement rangé les données dans l'ordre préconisé pour la règle de trois. Il cherche combien 100 deniers valent en réalité, selon l'un ou l'autre paiement, avec des daalders ou des

écus dépréciés. En fait, les résultats expriment les pourcentages valeur réelle / valeur faciale. Ceux-ci ne sont pas exprimés en nombres décimaux (la *Disme* de Stevin ne sera publiée qu'en 1585) mais sous la forme partie entière + partie fractionnaire : $100 \times \frac{58}{58,5} = \frac{58\,000}{585} = \frac{11\,600}{117} = 99 + \frac{17}{117}$, et il en va de même pour la seconde : $100 \times \frac{80}{81} = \frac{8\,000}{81} = 98 + \frac{62}{81}$. Enfin, la différence pour cent est $1 + \frac{17}{117} - \frac{62}{81} = \frac{3600}{9477} = \frac{400}{1053}$ en faveur des daalders.

2. Des applications domestiques

Natif de Leuwwarden en Frise, Edouard Léon (dit Elcius) Mellema fut forcé de quitter la Flandre et se réfugier en Allemagne après le sac d'Anvers par les Espagnols en 1576. Il enseigna alors la comptabilité et l'arithmétique quelques années à Aix-la-Chapelle avant de reprendre son activité à Anvers (Mellema, 1582, épître). Son rarissime traité d'arithmétique est aussi impressionnant par la quantité de questions résolues sans algèbre (plus de trois mille) que par la diversité des approches proposées, outre le nombre important de poèmes et anecdotes de voyage qu'il contient. Il constitue un témoignage détaillé des pratiques commerciales du nord de l'Europe au XVI^{e} siècle.

Nous présentons en Annexe 1 un exercice portant sur les « frais de bouche » d'un quidam non identifié, probablement hollandais. À proprement parler, ce n'est pas un exercice très difficile, puisqu'il ne s'agit que d'évaluer le montant total des frais engagés par le quidam pour ses repas pendant une période de près de trois mois, connaissant ce montant pour deux jours : 5 patards et 2 deniers de Hollande. C'est donc une préoccupation d'intendant.

L'intérêt de l'extrait ne réside pas tant dans l'énoncé lui-même que dans le dispositif graphique de présentation des calculs, que l'on interprète ainsi : 5 patards et 4 deniers font $5 \times 16 + 4$, soit 84 deniers, dépensés en deux jours, ce qui revient à 42 deniers par jour ; deux mois et 24 jours totalisent 84 jours, donc le montant total des dépenses est le produit 84×42, calculé de manière usuelle (avec retenue) pour un produit de 3528 deniers, converti en 220 patards et 8 deniers ($3528 = 16 \times 220 + 8$), puis en 11 florins ($220 = 20 \times 11$) et 8 deniers.

Lors de l'exposé de la « Reigle de troix », Mellema avait codé les diverses quantités proportionnelles avec les lettres A, B et C, et la quatrième proportionnelle D s'obtenait en calculant $A \times C \div B$. Il reprend cette codification dans le texte accompagnant l'exemple. La division finale de 3528 par 16 (quotient 220 et reste 8) est faite « à la galère », mais sans que le dividende soit repris, et la conversion des 220 patards en florins est immédiate.

La méthode de division est plus lisible dans la vérification faite plus bas, mais il faut prendre garde au fait que Mellema l'a simplifiée (« abbréviée ») en prenant la moitié du dividende et du diviseur. En résumé, il a calculé la dépense totale en deniers (3528), l'a divisée par 84 (jours) et multiplié par 2 (jours) en posant $1764 \div 21$, dont le résultat 84 (deniers) est converti en patards par une division par 16 : quotient 5 (patards) et reste 4 (deniers).

3. Et les équations du second degré ?

Revenons à Mennher pour notre dernier exemple, un peu plus difficile celui-ci, purement mathématique et résolu par l'algèbre, c'est le problème 72 que nous reproduisons en Annexe 2. Un cercle de diamètre 12 contient six cercles identiques, tangents entre eux, et qui forment un assemblage triangulaire dont les trois

« cercles-sommets » sont tangents au grand cercle. La question est de trouver le diamètre commun des petits cercles.

La résolution est peu détaillée, beaucoup de propriétés géométriques n'étant pas justifiées et les calculs intermédiaires non écrits. Mennher nomme x le diamètre demandé et z son carré ; le côté MN du triangle équilatéral (non justifié) MNR sera égal à $2x$ (non justifié) et par conséquent sa hauteur RS égale à $\sqrt{3\,x^2}$, résultat justifié par un évasif « par la troisième », correspondant à la troisième affirmation du chapitre auquel appartient ce problème. Il soustrait de cette hauteur son tiers pour obtenir RE égal à $\sqrt{\frac{4}{3}\,x^2}$ (propriété du triangle équilatéral non justifiée, E étant le centre de gravité du triangle RMN). Nous l'écrivons plutôt $\frac{2\sqrt{3}}{3}x$, ce qui revient à la même quantité.

Puisque le rayon AE vaut 6, et que par ailleurs c'est aussi AR + RE, Mennher établit l'équation :

$$\frac{1}{2}x + \frac{2\sqrt{3}}{3}x = 6.$$

La solution de l'auteur est $x = \sqrt{40 + \frac{152}{169}} - \left(2 + \frac{10}{13}\right)$, alors qu'une résolution moderne de l'équation du premier degré ci-dessus nous donne $x = \frac{36}{3 + 4\sqrt{3}}$. Une simplification de la solution de Mennher et une transformation (multiplication par l'expression conjuguée du dénominateur) permettront à tout un chacun de vérifier qu'il s'agit de la même quantité.

Comme nous le constatons, l'algèbre n'est pas exclue de tous les ouvrages d'arithmétique commerciale. Il est vrai que les auteurs anversois ont développé une réelle virtuosité dans ce domaine, sous l'influence des *Cossistes* allemands. Cependant, le monde n'était pas fait que d'algébristes experts et les ouvrages que nous étudions abordent aussi diverses méthodes de numération et les opérations, selon que les apprentis savent ou non lire et écrire. Pour les premiers, il s'agira de l'art du calcul « par la plume » (i.e. en écrivant) et pour les autres, celui du calcul « par les gets » ou par les jetons, que nous allons illustrer maintenant, reprenant brièvement la seconde partie de l'atelier consacrée à la manipulation des jetons.

III - COMPTER ET CALCULER AUX JETONS

La pratique du calcul est intimement mêlée au système de numération dont il fait usage. Les divers abaques connus dans l'histoire mettent en évidence l'identification de chaque nombre entier usuel avec la collection d'unités qui le composent. Ainsi, tout nombre entier de taille raisonnable peut être représenté par un ensemble de coquillages, de perles, de cailloux, ou autres objets à manipuler en lieu et place des nombres écrits en chiffres (Schärlig, 2003).

Si vous connaissez par cœur la « comptine numérique », chère aux enseignants de l'école maternelle, il vous sera facile d'ajouter deux entiers sans connaître par cœur la table d'addition. Par exemple, pour le calcul de 3 + 2 (cailloux), il vous suffira d'énumérer 1-2-3 (cailloux) d'une part, 1-2 (cailloux) d'autre part et, rassemblant les deux collections, 1-2-3-4-5 (cailloux) pour le total, que vous pourrez résumer par la formule « 3 plus 2 font 5 ». Pour calculer ainsi, pas besoin de capacités de mémorisation. Mais dès que les quantités en jeu deviennent importantes, ces manipulations deviennent fastidieuses et peu fiables. Autant

il est aisé de dénombrer ainsi une quantité de l'ordre de la dizaine, autant cela deviendra périlleux lorsqu'il s'agit de centaines, de milliers voire au-delà. Tout dépend donc de l'usage que vous en avez, mais aussi de la position que vous occupez, ainsi que de votre naissance : dans un milieu où vous avez appris à lire et à écrire, vous saurez effectuer les calculs à la plume ; si vous n'êtes qu'un pauvre marchand ambulant analphabète, les jetons vous seront précieux.

Il semble que les deux pratiques ont cependant coexisté, même dans les milieux financiers, à l'époque des textes que nous présentons. Une illustration en est donnée par la vignette de titre de l'ouvrage de Robert Recorde que nous avons déjà évoqué (Recorde, 1543). On y voit en effet (figure 7) plusieurs personnages représentés calculant dans une pièce dont on ne voit pas clairement s'il s'agit d'une taverne ou d'une forme médiévale de bureau d'expert-comptable. Sur les stalles n'est installé qu'un homme, les autres restent debout. Le contraste est saisissant : l'homme assis porte les cheveux courts et la barbe, il tient une épée à son côté, tandis que les hommes debout ont les cheveux longs et ne portent aucune arme.

Par ailleurs, celui qui est assis a devant lui une sorte de quadrillage sur lequel sont posés des jetons. C'est l'*échiquier* dont Recorde décrit la construction et l'usage dans la dernière partie de son ouvrage, *Accomptynge by counters* (Recorde, 1543, 116-134). Cependant, Recorde ne montre que le tracé des lignes tandis que la vignette du titre présente un réel quadrillage, ce qui l'apparente davantage à la pratique germanique qu'aux dispositifs décrits dans l'ouvrage, comme le montre une autre vignette de titre, celle du célèbre ouvrage allemand d'Adam Ries, *Rechenung auff der Linien vnd Federn*, présentée également figure 7 (Riese, 1535). Cette seconde image est plus explicite en ce qui concerne le local, bien que le tonneau sur la droite soit surtout destiné à montrer le travail des jaugeurs.

Figure 7. Vignette de titre des ouvrages (Recorde, 1543) et (Riese, 1535)

Dans les deux illustrations, nous remarquons la présence d'un homme debout à côté de la table, et coiffé d'un couvre-chef contrairement aux autres personnages de la scène. Comme il a l'air de ne pas travailler mais de superviser les comptables, les étudiants trouvent rapidement une interprétation de sa position : c'est celui qui possède l'argent.

Nous allons nous intéresser plus particulièrement à la pratique décrite dans les ouvrages en français, car il nous est bien plus facile en formation d'apporter un sac rempli de jetons qu'un certain nombre de tables gravées d'un quadrillage.

1. L'arbre aux jetons et la numération

Les ouvrages d'arithmétique pratique publiés en France au XVI[e] siècle décrivent une pratique similaire à ceux que nous venons de citer, mais qui ne nécessite pas tout l'attirail mobilier d'un *accountant* anglais ou d'un *Rechenmeister* allemand.

La pratique française est référencée dans de nombreux ouvrages élémentaires comme l'*Art et science de arismetique* (Anonyme, 1510) ou le *Livre de chiffres et de getz* (Anonyme, 1502) dont nous nous servons en formation initiale et continue. Les ordres décimaux (unités, dizaines, centaines…) sont matérialisés, non pas par des lignes gravées sur le bois d'une table, mais par la simple juxtaposition de jetons qui indiquent l'endroit des lignes le long desquelles on posera ceux qui représenteront les quantités numériques : c'est ce que l'on appelle l'*arbre aux jetons* (figure 8, que nous présentons à l'horizontale pour des raisons éditoriales).

Figure 8. Un arbre aux jetons *(Art et science de arismetique, vers 1510, fol. Ai-v*)

Cet arbre va être utilisé tout d'abord pour la numération (représentation des nombres entiers, voire quelques fractions simples) puis pour les quatre opérations usuelles.

L'exemple fondamental donné dans l'*Art et science de arismetique* (Anonyme, 1502)) est celui du nombre trente-quatre mille deux cent douze (figure 9). Les enseignants de tous niveaux, comme les élèves d'élémentaire, n'ont besoin d'aucune explication pour placer leurs jetons aux bons endroits : trois jetons sur la ligne des dizaines de milliers, quatre immédiatement en dessous, puis deux, puis un et deux.

Figure 9. Exemple de numération (Art et science de arismetique, vers 1510, fol. Eii)

Dans le *Livre de Chiffres et de getz*, l'exemple est plus compliqué : deux cent-quatorze millions cent-douze mille cent trente-huit (Anonyme, 1502, fol. Aii non signé). Il faut aller jusqu'en haut de l'arbre, au niveau des centaines de million, mais la répartition se fait aussi simplement que dans l'exemple plus haut. Cependant, les huit jetons de la ligne des unités peuvent poser problème. En effet, cette quantité n'est pas

perceptible immédiatement (*subitizing*) par le commun des mortels, donc probablement pas non plus par les gens ordinaires de l'époque médiévale. Cela signifie qu'un arithméticien malhonnête et rapide peut poser seulement sept jetons sans que les usagers le remarquent, et ainsi fausser les calculs en direct à son plus grand profit, sans qu'il soit possible de vérifier leur justesse en cours de manipulation. Pour éviter cette situation, il existe depuis l'Antiquité la pratique du jeton *quinaire* que l'on place à l'intermédiaire entre les lignes et qui a la valeur de cinq jetons de la ligne au-dessous.

2. Les opérations

2.1. Addition et soustraction

Revenons à notre discours initial : si l'on conçoit un entier comme assemblage d'unités, ce qui semble conforme à la vision pythagoricienne des entiers, l'addition n'est qu'une autre forme d'assemblage, et la soustraction une forme de séparation d'une collection en deux parties.

Avec les élèves de primaire et ceux de collège, on commence donc par des manipulations simples pour calculer une somme comme 253 + 124. Les jetons sont posés à droite de l'arbre, d'abord en deux groupes séparés afin de distinguer les nombres à ajouter et de pouvoir vérifier que les jetons sont correctement posés. Souvent, les élèves les posent en commençant par le haut, comme dans le sens de lecture usuel, le chiffre des centaines en premier, puis celui des dizaines, et enfin celui des unités.

Quand il faut additionner les deux nombres, le regroupement des jetons peut commencer par les centaines ou par les unités, voire par les dizaines, cela n'a aucune importance. D'ailleurs, les élèves ont tendance à commencer par les jetons des centaines, contrairement à ce qu'ils font en posant le calcul. Est-ce différent en cas de retenue ? En fait non. Dans l'exercice qui suit, nous proposons aux élèves d'additionner 127 et 234, somme pour laquelle on sait que le calcul posé nécessite une retenue (car 7 + 4 font 11). Mais il n'y a pas de gêne dans l'arbre aux jetons : vous trouvez onze jetons pour les unités, cinq jetons pour les dizaines et trois jetons pour les unités. Puisque 11 dépasse 10, vous ramassez dix jetons de la ligne des dizaines pour les remplacer par un jeton dans la ligne des centaines. Cette simple opération s'apparente à un transfert avec conversion, et elle permet de retrouver le sens de la retenue d'une dizaine.

2.2. Multiplication

Dans l'*Art et science de arismetique*, l'exemple illustré de la multiplication avec jetons concerne la conversion des monnaies (figure 10). On demande combien il y a de sols dans 61 francs. Lorsque ce type d'exemple est proposé à des élèves, il vaut la peine de ne pas les informer sur les monnaies anciennes et donc ne pas leur expliquer dès le départ que le multiplicateur n'est pas 10. En effet, un franc, équivalent à une livre, vaut vingt sols, lesquels valent chacun douze deniers. L'idée ici est de laisser les élèves trouver eux-mêmes les taux de conversion en analysant ce qui est donné. Détaillons la figure 10 : la partie centrale est occupée par l'arbre, des unités aux dizaines de milliers ; la somme de 61 francs se lit à gauche (avec un jeton quinaire pour 59, un jeton simple pour 10 et un simple pour 1 ; la somme équivalente en sols (ou sous) est sur la droite, on lit : 1000 + 2 × 100 + 2 × 10 soit 1220 sols.

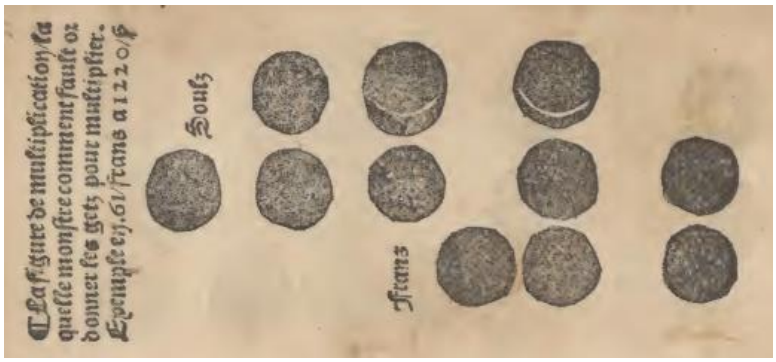


Figure 10. Multiplication de 61 par 20 (Anonyme, 1510, fol. Ei-v)

L'exemple du *Livre de chiffres et de gets* que nous utilisons aussi porte sur une conversion identique de 1223 francs en sols. L'énoncé y est quasiment identique à celui que nous venons de lire, mais il est imprimé de manière un peu plus sibylline : « en 1223 f a d s 24 460 ».

En formation ou avec des classes, nous prolongeons l'étude du texte par quelques exercices simples susceptibles d'engendrer des erreurs, ce qui ne manque jamais d'arriver. Il s'agit d'abord de multiplier par 20, en trouvant les gestes simples qui conviennent : poser deux jetons à droite chaque fois qu'il s'en trouve un à gauche, et remonter l'ensemble des jetons obtenus d'un échelon dans l'arbre. Ensuite, on demande de multiplier 27 par 12 et les choses se gâtent : les élèves ont tendance à reproduire les mêmes gestes que pour la multiplication précédente, assimilant la décomposition additive 10 + 2 avec la décomposition multiplicative 10 × 2. Il n'est pas difficile de les amener à se corriger en utilisant la distributivité de la multiplication par rapport à l'addition.

2.3. Division

Notre dernier exemple concerne le partage d'une somme de 1170 francs entre quinze hommes, comme l'indique la légende de la figure 11. L'exemplaire dont nous avons copie, celui de la collection Plimpton de la bibliothèque de l'université de Columbia, porte une correction manuelle ancienne : le 65 imprimé dans la légende a été remplacé par 78 qui est le bon résultat de la division de 1170 par 15. L'ancienneté de la correction est manifestée par la graphie des chiffres. Quel est alors le véritable énoncé ? Il faut le vérifier sur la figure de l'arbre aux jetons.

Cependant, il y a un problème : on repère facilement les jetons de l'arbre au centre, ils sont assez espacés. Mais le nombre de droite est 650 et celui de gauche 261, aucun rapport avec l'énoncé ! Pour y voir plus clair, nous devons nous rappeler que la figure est imprimée comme une gravure, tandis que le texte est composé. La feuille, munie de ses disques noirs représentant les jetons, est repassée sous presse au moment d'imprimer le texte, il y a parfois des incidents et c'est le cas ici : la feuille a été placée à l'envers, et le texte est imprimé en sens inverse du sens de lecture de la figure.

Prenons donc la page (ou la figure 11) dans l'autre sens et décryptons : à droite le nombre 1170 (utilisant un quinaire selon la décomposition 70 = 50 + 20), et à gauche 65 (50 + 10 + 5).

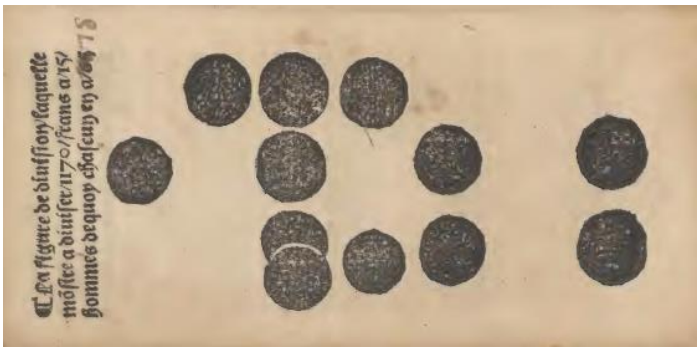


Figure 11. Division de 1170 par 15 (Anonyme, 1510, Eiii-v non signé)

Nous avions espéré comprendre cette différence entre le texte et la gravure en consultant une autre édition de l'ouvrage (Anonyme, 1520) souvent référencée sous le titre d'*Arithmétique de Pierre Sergent*, d'après le nom de l'imprimeur. Notre espoir fut vain : la gravure est identique, quoique de moins bonne qualité et avec un placement un peu approximatif des jetons de gauche. Cette gravure est également disposée à l'envers, ce qui fait soupçonner une recomposition à partir de l'édition de 1510, mais il faut être prudent sur l'estimation de la date de parution car aucun des deux ouvrages n'en porte. Pour ce qui est de notre problème de hiatus entre le texte et l'image, nous ne sommes pas avancés, d'autant plus que dans le texte de 1520 il est question de « diviser 1140 francs à 15 hommes » et non plus 1170 francs, même si curieusement la solution reste « de quoy chascun en a 65 ». Un bref coup d'œil à la multiplication précédente (celle de 61 par 20 vue plus haut) confirme la non fiabilité de l'ensemble dans l'édition de 1520 : le nombre 1220 est représenté comme 1110 sur l'arbre, et le texte indique un multiplicande de 91 au lieu de 61…

Dans les exercices de suite donnés aux élèves, aux enseignants en formation ou aux participants d'ateliers, nous proposons de diviser 1220 par 20, ce qu'ils réalisent facilement en renversant la succession de manipulations inventée pour la multiplication par 20. Mais la division de 2436 par 12 les laisse davantage perplexes (on ne peut pas l'assimiler aux deux divisions successives par 2 puis par 10). Une méthode toute visuelle est néanmoins possible : poser à gauche de l'arbre un jeton pour chaque bloc de douze jetons que l'on peut isoler à droite. En y réfléchissant bien, c'est conforme au principe même de division, par lequel on cherche à retrouver le diviseur dans le dividende autant de fois que possible, en commençant par les ordres supérieurs.

IV - CONCLUSION

Dans tous les exemples élémentaires cités, les problèmes résolus l'ont été sans raisonnement, mais en appliquant des méthodes standard, qui sont exposées de manière répétitive dans les ouvrages que nous avons consultés. Alors, peut-on penser que le raisonnement n'est pas indispensable en arithmétique à la Renaissance ? Les praticiens de l'époque auraient-ils trouvé cette idée incongrue ?

Nous avons surtout lu des extraits de textes adressés à des praticiens de l'arithmétique pour le commerce, voire la finance et, en tout cas, les changes de monnaies. Est-ce que les clients de ces praticiens demandaient des explications ? Certainement pas si les clients étaient seulement intéressés par leur expertise et l'efficacité de leurs méthodes. On en revient donc à la visée principale de notre enseignement : tête bien faite ou tête bien pleine ?

La réponse n'est pas immédiate, car ce n'est en aucun cas élémentaire. Il nous est souvent arrivé de nous trouver face à des personnes déplorant le manque d'habileté des jeunes adultes dans le maniement des chiffres et dans la résolution concrète de problèmes simples de proportionnalité. C'est même une réflexion récurrente à l'Institut de formation en soins infirmiers : les jeunes ne maîtrisent pas la règle de trois et ne peuvent pas effectuer de tête un simple calcul de proportion.

Comme en géométrie, l'aspect pratique des mathématiques est souvent minimisé dans notre enseignement. Alors, même s'il n'est pas du tout incongru de raisonner en arithmétique, nous voudrions rappeler que certains élèves tireront davantage profit de méthodes performantes et utiles, qu'il ne s'agit donc pas d'exclure des connaissances à acquérir à l'école.

V - BIBLIOGRAPHIE

Anonyme (1502). *Livre de chiffres & de getz nouvellement imprimé*. Lyon : Pierre Mareschal & Barnabé Chaussard.

Anonyme (vers 1510). *Art et science de arismetique moult utille et p[rou]ffitable… pour ceulx qui ne scavent lyre ne escripre nouvellement imprimé a Paris*. Paris : la veuve de Jehan Trepperel & Jehan Jehannot.

Anonyme (vers 1520). *Art et science de arismeticque par beaux exemples et pratiques*... Paris : Pierre Sergent.

Berthier, J. (1978). *Nicomaque de Gérase : Introduction arithmetique*. Paris : Vrin.

Chabert, J.-L. (dir.) (1994). *Histoire d'Algorithmes. Du caillou à la puce*. Paris : Belin.

Kool, M. (1999). *Die conste vanden getale. Een studie over Nederlandstalige rekenboeken uit de vijftiende en zestiende eeuw, met een glossarium van rekenkundige termen*. Hilversum :Verloren.

Mellema, E. L. (1582). *Premier volume de l'arithmetique, composé de plusieurs inventions & problemes nouveaux…* Anvers : Gillis vanden Rade.

Mennher, V. (1556). *Arithmetique seconde*. Anvers : Jan van der Loë.

De Norry, M. (1574). *[L']Arithmetiqve de Milles Denorry... Avec la maniere universelle des remises, traictes et retours des changes, ensemble leurs differences de monnoyes... le tout par la pratique, la plus brièvе et facille, qui ait esté encore mise en lumiere*. Paris : Gilles Gourbin.

Ortega, J. (1512). *Siguese vna conpusicion de la arte de la arismetica y juntamente de geometria…* Barcelone : Johannes Trinxer [impr. Lyon : Nicolas de Benedictis].

Ortega, J. (1515). *Œuvre tressubtille et profitable de lart & science de aristmeticque: & geometrie translate nouvellement despaignol en francoys…* Lyon : Simon Vincent.

Ortega, J. (1537). *Tratado subtilissimo de arismetica y de geometria…* Séville : Juan Cromberger.

Peletier, J. (1554). *L'Aritmetiqvе dе Jacqvеs Pelеtier du Mans, dеpartiе an quatrе Liuvrеs. Rеuüе e augmantеe par L'Auteur*. Lyon : Jean de Tournes.

Recorde, R. (1543). *The Ground of Artes teachyng the worke and practise of Arithmetike*… Londres : R. Wolfe.

Schärlig, A. (2003). *Compter avec des jetons. Tables à calculer et tables de compte du Moyen Age à la Révolution.* Lausanne : Presses polytechniques et universitaires romandes.

Ries, A. (1535). *Rechenung auff der Linien vnd Federn*… Francfort : Christian Egenolph.

Spiesser, M. (2008). L'arithmétique pratique en France au seuil de la Renaissance : formes et acteurs d'un enseignement. *Lull, volume 31*, 81-102.

Vinet, E. (1553). *Ex Mathematico Pselli Breviaro : Arithmetica, Musica, Geometria, Sphæra ex Procli Græco, Elia Vineto Santone interprete*. Bordeaux : François Morpain.

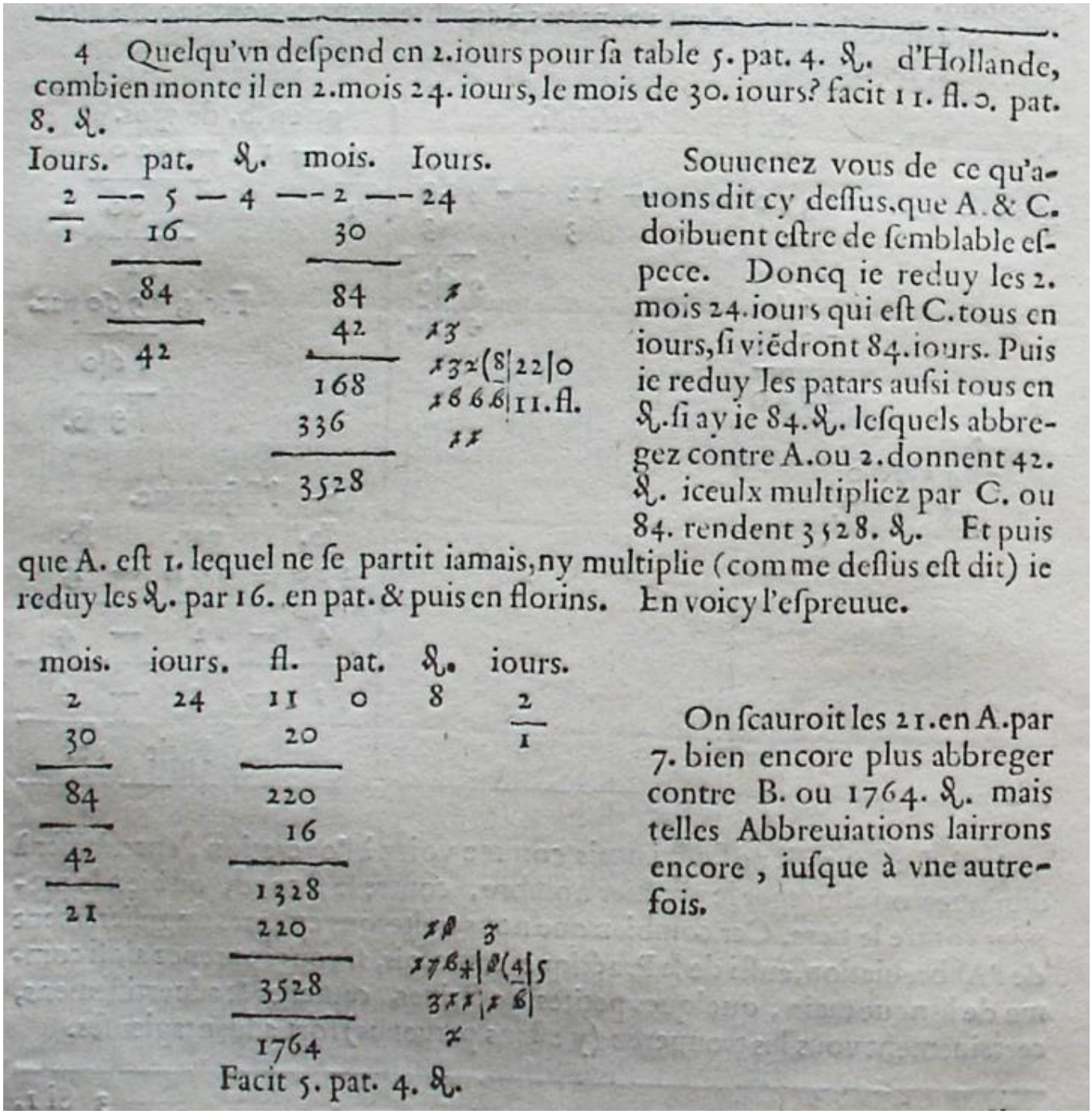
Vinet, E. (1573). *Elia Vineti Santonis De Logistica Libri tres.* Bordeaux : Simon Millange.

Vinet, E. (1577). *L'Arpanterie d'Élie Vinet, livre de geometrie, enseignant à mezurer les champs, & pluzieurs autres chozes*. Bordeaux : Simon Millange.

Vinet, E. (1583). *Schola aquitanica*. Bordeaux : Simon Millange.

Williams, T. D. (2012). The Earliest English Printed Arithmetic Books. *The Library. The Transactions of the Bibliographical Society*, 7th series, 13(2), 164-184.

VI - ANNEXE 1 : UN PROBLÈME GOURMAND



4 Quelqu'vn deſpend en 2. iours pour ſa table 5. pat. 4. ß. d'Hollande, combien monte il en 2. mois 24. iours, le mois de 30. iours? facit 11. fl. 0. pat. 8. ß.

Iours. pat. ß. mois. Iours.
2 — 5 — 4 — 2 — 24
1 16 30
84 84
42 42
168
336
3528

Souuenez vous de ce qu'auons dit cy deſſus, que A. & C. doibuent eſtre de ſemblable eſpece. Doncq ie reduy les 2. mois 24. iours qui eſt C. tous en iours, ſi viẽdront 84. iours. Puis ie reduy les patars auſsi tous en ß. ſi ay ie 84. ß. leſquels abbregez contre A. ou 2. donnent 42. ß. iceulx multipliez par C. ou 84. rendent 3528. ß. Et puis que A. eſt 1. lequel ne ſe partit iamais, ny multiplie (comme deſſus eſt dit) ie reduy les ß. par 16. en pat. & puis en florins. En voicy l'eſpreuue.

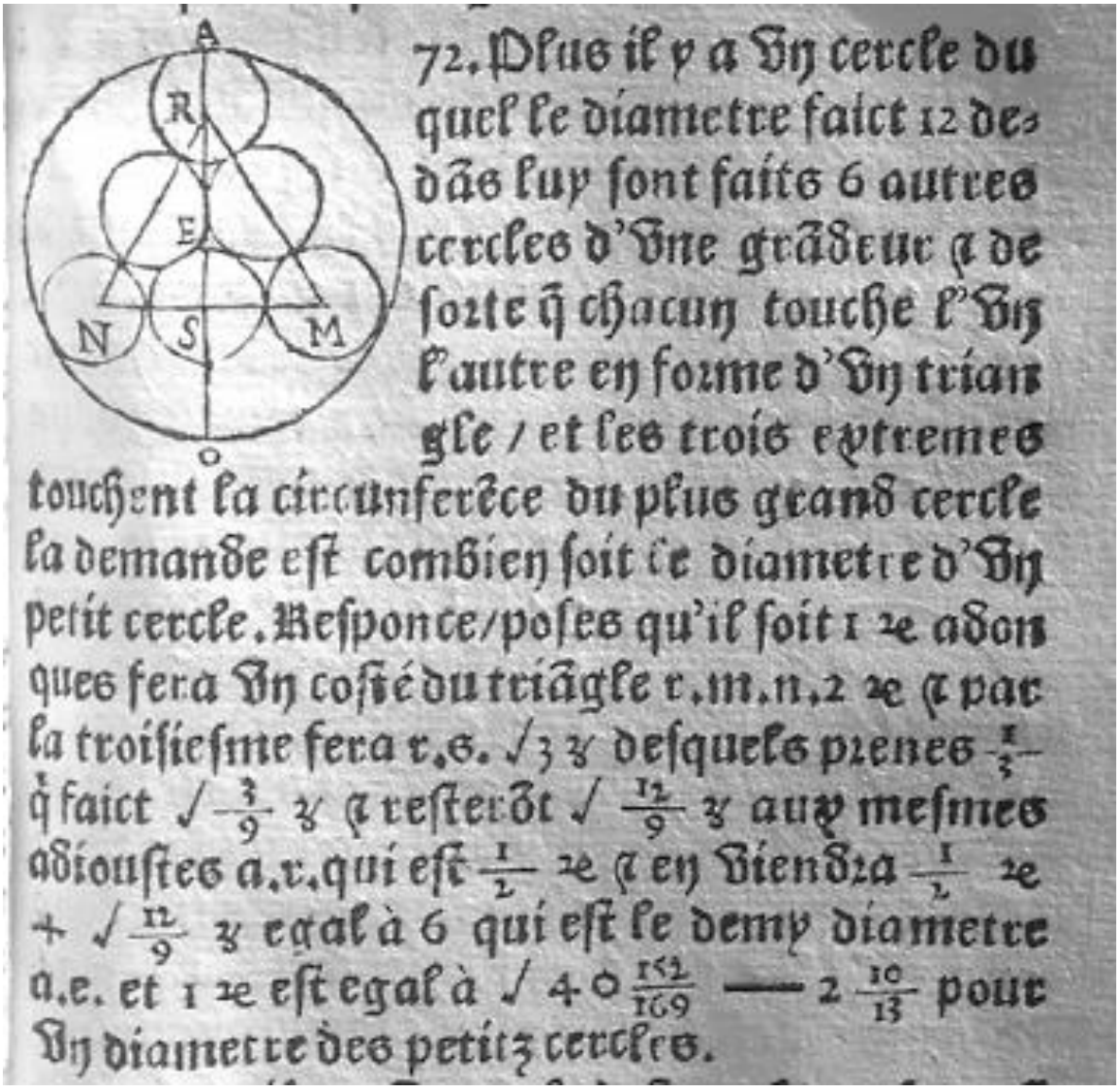
mois. iours. fl. pat. ß. iours.
2 24 11 0 8 2
30 20 1
84 220
42 16
21 1328
220
3528
1764

Facit 5. pat. 4. ß.

On ſcauroit les 21. en A. par 7. bien encore plus abbreger contre B. ou 1764. ß. mais telles Abbreuiations lairrons encore, iuſque à vne autrefois.

Edouard Léon Mellema, Premier volume de l'arithmetique, 1582, p. 104.

ANNEXE 2 : UNE ÉQUATION DU SECOND DEGRÉ CHEZ MENNHER



72. Plus il y a vn cercle duquel le diametre faict 12 dedãs luy sont faits 6 autres cercles d'vne grãdeur q de sorte q̃ chacun touche l'vn l'autre en forme d'vn triangle / et les trois extremes touchent la circunferẽce du plus grand cercle la demande est combien soit le diametre d'vn petit cercle. Responce/poses qu'il soit 1 ze adonques fera vn costé du triãgle r.m.n.2 ze q par la troisiesme fera r.s. $\sqrt{3}$ z desquels prenes $\frac{1}{3}$ q faict $\sqrt{\frac{3}{9}}$ z q resterõt $\sqrt{\frac{12}{9}}$ z auxq mesmes adioustes a.r. qui est $\frac{1}{2}$ ze q en viendra $\frac{1}{2}$ ze + $\sqrt{\frac{12}{9}}$ z egal à 6 qui est le demy diametre a.e. et 1 ze est egal à $\sqrt{40\frac{1521}{169}}$ —— $2\frac{10}{13}$ pour vn diametre des petitz cercles.

Valentin Mennher, Arithmetique seconde, 1556, fol. signé T2.

ARITHMÉTIQUE ET RAISONNEMENT MATHÉMATIQUE

Denis GARDES
IREM DIJON
denis.gardes@wanadoo.fr

Dominique BERNARD
IREM LYON
dominique.bernard@gmail.com

Résumé
Il s'agit dans cet atelier de montrer que l'arithmétique est un domaine des mathématiques où l'on peut privilégier l'apprentissage du raisonnement et ceci à tout niveau du secondaire. On présente la structure des différents raisonnements habituels en mathématiques. Chaque raisonnement sera accompagné d'exemples avec leur correction de niveau collège, de niveau seconde ou terminale mathématiques expertes. La solution proposée est une solution « experte » et n'est évidemment pas un attendu de la part des élèves. Elle a pour but d'éclairer l'enseignant sur la pertinence de l'exemple.

I - RÉSOLUTION D'UN PETIT AMUSE-BOUCHE

Nous avons commencé l'atelier en demandant de résoudre un exercice légèrement modifié des Olympiades Mathématiques 2008 et de dégager à chaque question le type de raisonnement mathématique utilisé.

Voici l'énoncé :

On dit qu'un nombre entier est *digisible* lorsque les trois conditions suivantes sont vérifiées :

- aucun de ses chiffres n'est nul ;
- il s'écrit avec des chiffres tous différents ;
- il est divisible par chacun d'eux.

1. Proposer un nombre *digisible* à deux chiffres.

2. Déterminer tous les nombres *digisibles* à deux chiffres.

3. Déterminer le plus petit nombre *digisible* à quatre chiffres.

4. Soit n un entier *digisible* s'écrivant avec un 5.

a. Démontrer que 5 est le chiffre de ses unités.

b. Démontrer que tous les chiffres de n sont impairs.

c. Démontrer que n s'écrit avec au plus quatre chiffres.

d. Déterminer le plus grand entier *digisible* s'écrivant avec un 5.

5. Soit n un entier *digisible* quelconque.

a. Démontrer que n s'écrit avec au plus sept chiffres.

b. Si n s'écrit avec sept chiffres, dont un 9, déterminer les chiffres de n.

c. Déterminer le plus grand entier *digisible*.

Voici maintenant une solution de cet exercice. Nous avons écrit en italique les différents types de raisonnement que nous avons repérés.

1. Les nombres 12, 15, 24 et 48 sont *digisibles* par exemple.

Il s'agit de prouver une proposition existentielle. Il suffit d'exhiber un élément satisfaisant les conditions, peu importe la méthode pour le trouver.

2. On va raisonner selon les dizaines.

Si le chiffre des dizaines est 1, cela n'impose aucune condition sur le chiffre des unités puisque 1 divise tous les entiers. On examine un par un les entiers. On remarque alors que seuls 12 et 15 conviennent.
Si le chiffre des dizaines est 2, alors le nombre est divisible par 2. Le chiffre des unités est alors 4, 6 ou 8. Seul 24 convient.
Si le chiffre des dizaines est 3, alors le nombre est divisible par 3. Cela peut être : 36 et 39. Seul 36 convient.
Si le chiffre des dizaines est 4, alors le nombre est divisible par 4. Cela peut être : 48. 48 convient.
Si le chiffre des dizaines est 5, alors le nombre est divisible par 5. Il n'y a pas dans cette dizaine de nombre divisible par 5 ayant des chiffres distincts et non nuls.
Si le chiffre des dizaines est 6, alors le nombre est divisible par 6. Il n'y a pas dans cette dizaine de nombre divisible par 6 ayant des chiffres distincts et non nuls.
Si le chiffre des dizaines est 7, alors le nombre est divisible par 7. Il n'y a pas dans cette dizaine de nombre divisible par 7 ayant des chiffres distincts et non nuls.
Si le chiffre des dizaines est 8, alors le nombre est divisible par 8. Il n'y a pas dans cette dizaine de nombre divisible par 8 ayant des chiffres distincts et non nuls.
Si le chiffre des dizaines est 9, alors le nombre est divisible par 9. Il n'y a pas dans cette dizaine de nombre divisible par 9 ayant des chiffres distincts et non nuls.
Conclusion : l'ensemble des nombres *digisibles* à 2 chiffres est {12 ; 15 ; 24 ; 35 ; 48}.

On a effectué un raisonnement par disjonction des cas (selon le chiffre des dizaines). Dans chaque cas, un raisonnement par conditions nécessaires et suffisantes ou analyse-synthèse a été effectué.

3. Le plus petit nombre écrit avec quatre chiffres distincts est 1 234. Ce nombre ne convient pas car il n'est pas divisible par 4.
Le nombre suivant dans l'ordre croissant est 1 236 car il doit être divisible par 2 et 3. Ce nombre convient car il est divisible par 1, 2, 3 et 6.
Le nombre cherché est donc 1 236.

On a effectué un raisonnement par disjonction des cas, selon l'ordre croissant des nombres, qui s'est arrêté dès que l'on a trouvé un nombre qui convenait.

4. **a**. n s'écrit avec un 5, il est donc divisible par 5. Ainsi son chiffre des unités est soit 0, soit 5. Comme il ne peut pas être 0, il est donc égal à 5.
On a effectué un raisonnement direct par modus ponens pour démontrer une implication.

b. D'après la question précédente, *n* se termine par 5 est donc impair. Il ne contient que des chiffres impairs.
On a effectué un raisonnement direct par modus tollens avec l'implication : « Si n a au moins un chiffre pair alors il est divisible par 2 » ou ce qui est équivalent un raisonnement direct par modus ponens avec la contraposée « si n n'est pas divisible par 2, alors n a tous ses chiffres impairs ».

c. Tous les chiffres de *n* sont impairs et distincts. *n* a donc au plus 5 chiffres. On suppose que *n* est formé des 5 chiffres impairs : 1, 3, 5, 7 et 9. Il est donc divisible par 9 donc la somme de ses chiffres est divisible par 9. Or celle-ci est égale à 1 + 3 + 5 + 7 + 9 = 25 qui n'est pas divisible par 9. On aboutit à une contradiction. Donc le nombre *n* s'écrit avec au plus quatre chiffres.

On a effectué un raisonnement par l'absurde : pour démontrer Q[a] : « Le nombre s'écrit avec au plus 4 chiffres », on a supposé NON Q[a] : « le nombre a s'écrit avec strictement plus de 4 chiffres » puis on a démontré que cela aboutissait à une contradiction, c'est-à-dire une proposition fausse « 25 est divisible par 9 » donc NON Q[a] est fausse, c'est-à-dire Q[a] est vraie.

d. D'après ce qui précède, le nombre cherché *n* s'écrit avec au plus 4 chiffres tous impairs et se termine par 5.

Pour essayer de trouver le plus grand, on commence avec 9 comme chiffre des milliers. Ainsi *n* commence par 9 et se termine par 5. Il reste à déterminer le chiffre des centaines et celui des dizaines. La somme *S* des quatre chiffres doit être divisible par 9. Or *S* est comprise entre 9 +7+3+5 = 24 et 9+1+3+5 = 18.

Elle est donc égale à 18. Les deux chiffres restants sont 3 et 1. On obtient deux valeurs de *n* : 9 315 et 9 135.

Le nombre 9 315 est divisible par 9, 3 et 5. Il est donc digisible et c'est le plus grand nombre digisible s'écrivant avec un 5.

On a commencé un raisonnement par disjonction des cas selon la valeur du chiffre des milliers vite interrompu puisqu'on a une solution dès le premier cas examiné. Dans l'examen de ce cas, on a effectué un raisonnement par analyse-synthèse. L'analyse a permis de restreindre deux possibilités pour le nombre cherché et la synthèse a permis de déterminer lequel de ces deux nombres convient.

5. a. Soit *n* un entier *digisible*. Le nombre s'écrit avec au plus neuf chiffres parmi {1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9}. Soit il contient le 5, il s'écrit avec aux plus quatre chiffres d'après la question **4.c.**
Soit il ne contient pas le 5, il s'écrit alors avec aux plus huit chiffres. S'il s'écrit avec les huit chiffres restants alors il contient le 9. La somme des huit chiffres est égale à 1 + 2 + 3 + 4 + 6 + 7 + 8 + 9 = 40 et n'est pas divisible par 9.
Ceci prouve qu'un tel nombre n'est pas *digisible*. Le nombre *digisible* ne peut contenir les huit chiffres (1, 2, 3, 4, 6, 7, 8, 9). Il a donc au plus sept chiffres.

Plusieurs types de raisonnement s'enchevêtrent :

- *raisonnement par disjonction des cas : présence du chiffre 5 ou non*
- *raisonnement par condition nécessaire*

« si le nombre digisible contient le 5, alors il a au plus 4 chiffres » et « si le nombre digisible contient 9 alors il a au plus 7 chiffres ».

• *raisonnement par modus tollens utilisant l'implication*

« Si le nombre digisible contient 9 et a 8 chiffres, alors il est divisible par 9 » Il est intéressant de noter, qu'à ce stade de la résolution de l'exercice, « avoir au plus 7 chiffres » est une condition nécessaire pour l'existence d'un entier digisible, mais est-elle suffisante ?

b. Soit *n* un entier digisible s'écrivant avec sept chiffres dont 9.
D'après la question **4.c** il ne contient pas 5. Les six autres chiffres sont à prendre dans {1, 2, 3, 4, 6, 7, 8}. Or 1+2+3+4+6+7+8+9 = 40 et pour obtenir un multiple de 9, la seule possibilité est d'enlever le chiffre 4. Les chiffres n sont : 1, 2, 3, 6, 7, 8 et 9.
Il s'agit ici d'obtenir une condition nécessaire obtenue par conditions nécessaires successives amenant à une seule possibilité.

c. D'après la question précédente, si *n* le nombre digisible cherché a 7 chiffres, ceux-ci sont à prendre dans {1, 2, 3, 6, 7, 8, 9}. Le nombre *n* a nécessairement un chiffre pair, il est donc divisible par 2, donc pair.
Pour trouver le plus grand, on peut commencer à chercher les nombres commençant par 9 876. Il reste les trois chiffres 1, 2 et 3 à placer. Comme *n* est pair, il n'y a que deux possibilités : 9 876 312 et 9 876 132. Or 9 876 312 n'est pas divisible par 7 et 9 876 132 n'est pas divisible par 8. Le nombre *n* ne commence pas par 9 876.
On cherche maintenant s'il peut commencer par 9 873. Il reste les trois chiffres 1, 2 et 6 à placer. Sachant que *n* est pair, il y a 4 possibilités : 9 873 126, 9 873 162, 9 873 216 et 9 873 612.
Or 9 873 126,9 873 162 et 9 876 3216 ne sont pas divisibles par 7 et 9 8763 612 n'est pas divisible par 8.
On cherche maintenant s'il peut commencer par 9 872. Il reste les trois chiffres 1, 3 et 6 à placer. Sachant que *n* est pair, il y a 2 possibilités : 9 872 316 et 9 872 136. Or ces deux nombres ne sont pas divisibles par 7.
On cherche maintenant s'il peut commencer par 9 871. Il reste les trois chiffres 2, 3 et 6 à placer. Sachant que *n* est pair, il y a 4 possibilités : 9 871 236, 9 871 326
9 871 362 et 9 871 632. Or ces quatre nombres ne sont pas divisibles par 7.
Le nombre *n* ne peut pas commencer par 987. On cherche maintenant s'il peut commencer par 9 867. Il reste les trois chiffres 1, 2 et 3. Sachant que *n* est pair, il y a 2 possibilités : 9 867 312 et 9 867 132. Or 9 867 312 est divisible par 1, 2, 3, 6, 7, 8 et 9. C'est le plus grand nombre digisible.

On a raisonné par disjonction des cas selon l'ordre décroissant des nombres cherchés et dans chaque cas on a effectué un raisonnement par analyse-synthèse.

Cet exercice est intéressant car il mobilise de nombreux types de raisonnement : *modus ponens*, *modus tollens*, raisonnement par l'absurde, raisonnement par disjonction des cas, raisonnement analyse-synthèse. D'autre part, il ne demande que très peu de connaissances mathématiques. Il se fonde surtout sur la numération décimale et sur les critères de divisibilité. On peut regretter que le raisonnement par équivalence et celui par récurrence n'aient pas été convoqués. Pour le raisonnement par équivalence, nous en reparlerons plus loin.

II - SPÉCIFICITÉ DE L'ARITHMÉTIQUE

1. Comme nous venons de le voir avec l'exemple d'introduction, beaucoup d'exercices ne demandent qu'un niveau de connaissances mathématiques assez faible. C'est un des rares domaines où l'on peut énoncer à des élèves des conjectures non encore démontrées. Nous pensons à la conjecture de Goldbach (tout nombre pair supérieur à 3 est somme de deux nombres premiers), à la conjecture d'Erdös-Straus (pour tout n entier naturel, on peut trouver trois entiers naturels *a*, *b* et *c* tels que $\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$, à la conjecture de Syracuse (la suite est définie de la manière suivante $u_{n+1} = \frac{u_n}{2}$ si $u_n$est pair et $u_{n+1}= 3u_n +1$ si u_n est impair et la conjecture énonce qu'il existe toujours un rang pour lequel $u_n = 1$ quel que soit le premier terme choisi).
Sans aller jusqu'à proposer aux élèves des problèmes ouverts (au sens de la recherche mathématique), on peut proposer aux élèves un grand nombre d'exercices où l'énoncé est simple à comprendre, où l'élève peut s'engager rapidement dans une recherche et mobiliser des raisonnements variés. Ce n'est pas étonnant que l'on trouve beaucoup de tels exercices dans des énoncés de type rallye, olympiades. Évidemment, tous les exercices d'arithmétique n'ont pas ce statut, certains peuvent relever de connaissances très ardues !

2. Au niveau de l'enseignement secondaire, l'arithmétique demande de modifier les « réflexes » acquis notamment en algèbre et en analyse. Par exemple, la résolution d'une équation dans $\mathbb{R}$ est très souvent très différente de la résolution dans $\mathbb{N}$. Le fait que $\mathbb{N}$ soit un ensemble discret amène souvent à pouvoir traiter tous les cas « un par un ». Une équation à deux variables n'a souvent que peu de solutions dans $\mathbb{N}$ alors qu'elle en a souvent une infinité dans $\mathbb{R}$.
Par exemple, résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$: $\frac{1}{x} + \frac{1}{y} = \frac{1}{2}$
Cette équation est équivalente à $(x-2)(y-2) = 4$.
Ainsi $x-2$ et $y-2$ sont des diviseurs de 4 différents de -2 (x et y étant non nuls).
Les diviseurs de 4 sont : $-4, -2, -1, 1, 2$ et 4.
On obtient 6 systèmes à résoudre. Trois seulement donnent une solution avec des entiers naturels non nuls.
Les solutions sont : (3 ; 6), (4 ; 4) et (6 ; 3).
Si on résout dans $\mathbb{R}^* \times \mathbb{R}^*$.
L'équation est équivalente à $y = \frac{2x}{x-2}$ avec $x \neq 2$.
Il y a alors une infinité de couples solutions $\left(x ; \frac{2x}{x-2} \right)$ avec $x \in \mathbb{R}\backslash\{0 ; 2\}$.

3. Le raisonnement par récurrence est très fréquent. Ceci n'est pas étonnant, l'axiome de récurrence est un des axiomes de la définition de $\mathbb{N}$ comme ensemble des entiers naturels.
Le raisonnement par descente infinie de Fermat est aussi utilisé. Il s'appuie sur le principe dit de descente infinie de Fermat « il n'existe pas de suite infinie strictement décroissante d'entiers naturels».
Ce principe est équivalent à l'axiome de bon ordre « toute partie non vide de $\mathbb{N}$ admet un plus petit élément ». Dans $\mathbb{N}$, l'axiome de récurrence et l'axiome de bon ordre sont équivalents.

4. Le raisonnement par analyse-synthèse est très fréquent. Ceci s'explique car peu de résultats sont énoncés sous forme d'équivalence en arithmétique. Par exemple, le théorème de Gauss est une implication et non une équivalence. De même l'implication « pour tous entiers *a*, *b* et *c*, si *a* divise *b* et *c* alors *a* divise *b* + c » ne peut pas s'énoncer sous la forme d'une équivalence. Ceci amène à déterminer,

lors de résolution de problèmes, à des conditions nécessaires. Ces dernières doivent être étudiées pour obtenir des conditions suffisantes.

5. Le raisonnement par disjonction des cas est très souvent employé. En effet, discuter suivant la parité, suivant le reste de la division euclidienne d'un entier naturel est une pratique très courante en arithmétique.
6. Enfin, le principe des tiroirs de Dirichlet « Si m+1 objets ou plus sont rangés dans m tiroirs, alors il y aura au moins un tiroir qui contient deux objets ou plus » peut être un principe pertinent dans certains problèmes d'arithmétique.

III - RAISONNEMENT DIRECT : *MODUS PONENS ET MODUS TOLLENS*

Le *modus ponens* est la règle la plus couramment utilisée dans les raisonnements. Elle est directement liée à l'implication et à ses valeurs de vérité.
Elle s'écrit :
en logique des propositions :

$$\left.\begin{array}{l}(P \Longrightarrow Q) \text{ Vraie} \\ P \text{ Vraie}\end{array}\right\} \text{ DONC } Q \text{ Vraie.}$$

en logique des prédicats :

$$\left.\begin{array}{l}\forall x\ (P[x] \Longrightarrow Q[x]) \text{ Vraie} \\ P[a] \text{ Vraie}\end{array}\right\} \text{ DONC } Q[a] \text{ Vraie.}$$

Une autre règle de raisonnement liée à l'implication est celle appelée *modus tollens* :

$$\left.\begin{array}{l}(P \Longrightarrow Q) \text{ Vraie} \\ Q \text{ Fausse}\end{array}\right\} \text{ DONC } P \text{ Fausse.}$$

en logique des prédicats :

$$\left.\begin{array}{l}\forall x\ (P[x] \Longrightarrow Q[x]) \text{ Vraie} \\ Q[a] \text{ Fausse}\end{array}\right\} \text{ DONC } P[a] \text{ Fausse.}$$

Ces deux règles s'observent aisément grâce à la table de vérité de l'implication :

P	Q	$P \Longrightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Nous ne donnerons pas d'exemples d'exercices où on applique la règle du *modus ponens* car celle-ci est la plus fréquemment employée. En revanche, la règle du *modus tollens* est rarement énoncée. L'habitude scolaire actuelle veut que l'on utilise plutôt la règle du *modus ponens* avec la contraposée de l'implication ou alors qu'on utilise un raisonnement par l'absurde. Nous donnons les trois exemples suivants :

Exercice Col1

Démontrer que $\sqrt{2}^2 \neq 1{,}414$.

Solution

On a $\sqrt{2}^2 = 2$ et $1{,}414^2 = 1{,}999396$.

Comme $\sqrt{2}^2 \neq 1{,}414^2$, on en déduit que $\sqrt{2} \neq 1{,}414$.

Remarque

On utilise le *modus tollens* avec l'implication : $\forall (a\,;\,b) \in \mathbb{R}^2 \quad a = b \Longrightarrow a^2 = b^2$.

Cette règle permet d'éviter un raisonnement par l'absurde ou d'avoir recours à la notion de contraposée.

Exercice Sec1

Démontrer que la droite d'équation $y = \frac{3}{4}x + \frac{1}{8}$ n'admet pas de points à coordonnées entières.

Solution

Soit $M\,(x\,;\,y)$ un point à coordonnées entières de la droite $(\mathscr{D})$ d'équation $y = \frac{3}{4}x + \frac{1}{8}$.

Une équation équivalente de $(\mathscr{D})$ est $8y = 6x + 1$.

Pour x et y, entiers, $8y$ est pair et $6x + 1$ est impair. Ainsi est $8y \neq 6x + 1$.

On en déduit qu'il n'existe pas de points à coordonnées entières sur la droite $(\mathscr{D})$.

Remarque

On utilise le *modus tollens* avec l'implication :

$\forall (x\,;\,y) \in \mathbb{Z}^2 \quad M\,(x\,;\,y) \in (\mathscr{D}) \Longrightarrow (8y = 6x + 1)$.

Là encore, cette règle permet d'éviter un raisonnement par l'absurde.

Exercice Exp1

Démontrer que la somme de cinq carrés d'entiers consécutifs n'est jamais un carré d'entier.

Solution

On note les cinq entiers consécutifs $n - 2$, $n - 1$, n, $n + 1$ et $n + 2$ avec $n \geq 2$.

La somme $(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2$ est égale à $5(n^2 + 2)$.

Pour que $5(n^2 + 2)$ soit un carré parfait, il est nécessaire que $n^2 + 2$ soit divisible par 5 puisque l'exposant de 5 dans un carré parfait est pair.

On examine la congruence modulo 5 de $n^2 + 2$.

Ainsi on obtient le tableau de congruence modulo 5 :

n	0	1	2	3	4
n^2	0	1	4	4	1
n^2+2	2	3	1	1	3

On peut remarquer que $n^2 + 2$ n'est jamais divisible par 5.

On en déduit que $5(n^2 + 2)$ n'est pas un carré parfait.

Remarque

On utilise le modus tollens avec l'implication : « pour tout entier n, si $5(n^2 + 2)$ est un carré parfait, alors $n^2 + 2$ est divisible par 5 ».

IV - RAISONNEMENT PAR DISJONCTION DES CAS

Le raisonnement par disjonction des cas s'utilise principalement pour démontrer la vérité d'une proposition universelle que l'on note : $\forall x \in E \quad P[x]$.

Soit $(E_i)_{1\leq i\leq n}$ une famille d'ensembles telles que $\bigcup_{i=1}^{n} E_i = E$.

Le raisonnement par disjonction des cas consiste à démontrer successivement les propositions universelles suivantes : pour i de 1 à n, $\forall x \in E_i \quad P[x]$.

Formellement, il peut s'écrire :

$$\text{SI} \begin{cases} E = \bigcup_{i=1}^{n} E_i \\ \forall i \in \{1, \ldots, n\} \ \ \forall x \in E_i \ P[x] \end{cases} \qquad \text{ALORS } \forall x \in E \ P[x].$$

Il n'est pas nécessaire que la famille $(E_i)_{(1\leq i\leq n)}$ soit une partition même si c'est souvent le cas dans les exemples d'application. La notion de recouvrement suffit.

Exercice Col2

Démontrer que $\sqrt{2}$ n'est pas un nombre décimal.

Solution

On suppose que $\sqrt{2}$ est un nombre décimal.

Comme $1 < \sqrt{2} < 2$, $\sqrt{2}$ n'est pas entier. Soit a la dernière décimale non nulle de $\sqrt{2}$. On examine la dernière décimale de $\sqrt{2}^2 = 2$ selon les différentes valeurs de a.

Si $a = 1$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 1.

Si $a = 2$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 4.

Si $a = 3$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 9.

Si $a = 4$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 6.

Si $a = 5$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 5.

Si $a = 6$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 6.

Si $a = 7$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 9.

Si $a = 8$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 4.

Si $a = 9$ alors la dernière décimale non nulle de $\sqrt{2}^2$ est 1.

On remarque que $\sqrt{2}^2$ aurait une décimale non nulle. Ceci est faux puisque 2 est un entier. Ainsi l'hypothèse formulée « $\sqrt{2}$ est un nombre décimal » est fausse.

$\sqrt{2}$ n'est pas un nombre décimal.

Remarque

Le raisonnement par disjonction des cas (selon la dernière décimale non nulle de $\sqrt{2}$) se trouve à l'intérieur d'un raisonnement par l'absurde.

Exercice Sec2

Démontrer que pour tout entier naturel n, $n(n^2 + 5)$ est divisible par 3.

Solution

On raisonne selon le reste de la division euclidienne de n par 3. Il y a donc trois cas à traiter selon que ce reste r est nul, égal à 1 ou à 2.

Premier cas : $r = 0$.

Il existe $k \in \mathbb{Z}$ tel que $n = 3k$.

Ainsi $n(n^2 + 5) = 3k(n^2 + 5)$. Or $k(n^2 + 5)$ est un entier. Donc, dans ce cas, $n(n^2 + 5)$ est divisible par 3.

Deuxième cas : $r = 1$.

Il existe $k \in \mathbb{Z}$ tel que $n = 3k + 1$.

Ainsi $n(n^2 +5) = (3k +1)((3k +1)^2 +5) = (3k +1)(9k^2 +6k +6) = 3(3k +1)(3k^2 +2k +2)$.

Or $(3k + 1)(3k^2 + 2k + 2)$ est un entier. Donc, dans ce cas, $n(n^2 + 5)$ est divisible par 3.

Troisième cas : $r = 2$.

Il existe $k \in \mathbb{Z}$ tel que $n = 3k + 2$.

Ainsi $n(n^2 +5) = (3k +2)((3k +2)^2 +5) = (3k +2)(9k^2 +12k +9) = 3(3k +2)(3k^2 +4k +3)$.

Or $(3k + 2)(3k^2 + 4k + 3)$ est un entier. Donc, dans ce cas, $n(n^2 + 5)$ est divisible par 3. On a bien démontré que, pour tout n entier naturel, $n(n^2 + 5)$ est divisible par 3.

Remarque

On a utilisé la partition suivante de $\mathbb{N}$: $\mathbb{N}$ est la réunion de l'ensemble des entiers divisibles par 3, de l'ensemble des entiers dont le reste par la division euclidienne par 3 est 1 et de l'ensemble des entiers dont le reste de la division euclidienne par 3 est 2.

Exercice Exp2

Démontrer que pour tout couple $(a ; b)$ d'entiers naturels, si 7 divise $a^2 + b^2$ alors 7 divise a et 7 divise b.

Solution

On va effectuer un raisonnement par disjonction de cas, selon les congruences des nombres a et b modulo 7.

On examine, selon les congruences de a modulo 7, les congruences de a^2.

On obtient le tableau suivant :

a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1

Les congruences du carré d'un entier modulo 7 sont au nombre de quatre : 0, 1, 2 et 4.

On écrit les seize résultats modulo 7 de $a^2 + b^2$ dans le tableau suivant :

	$a^2 \equiv 0$	$a^2 \equiv 1$	$a^2 \equiv 2$	$a^2 \equiv 4$
$b^2 \equiv 0$	0	1	2	4
$b^2 \equiv 1$	1	2	3	4
$b^2 \equiv 2$	2	3	4	6
$b^2 \equiv 4$	4	5	6	1

Il n'y a qu'un seul cas où $a^2 + b^2$ est divisible par 7. C'est le cas où a^2 et b^2 sont tous les deux congrus à 0 modulo 7. Or, d'après le premier tableau, a^2 est divisible par 7 si et seulement si a est divisible par 7.
Ainsi, on a démontré que, pour tous entiers relatifs a et b, si 7 divise $a^2 + b^2$ alors 7 divise a et 7 divise b.

Remarque
La disjonction des cas porte sur le reste de la division euclidienne des entiers par 7. Cette disjonction est très courante en arithmétique, elle permet de se ramener à un nombre fini de cas que l'on traite un par un.
On peut aussi remarquer que l'on a démontré l'équivalence pour tout couple $(a ; b)$ d'entiers naturels entre « 7 divise $a^2 + b^2$ » et « a divise 7 et b divise 7 ».

V - RAISONNEMENT PAR CONTRAPOSITION

On sait que l'implication $P \Rightarrow Q$ est équivalente à NON $Q \Rightarrow$ NON P .

Ce raisonnement ne s'applique que quand on veut démontrer une implication puisque l'on remplace l'implication à démontrer par une implication qui lui est équivalente.
On privilégie ce raisonnement quand les propositions P et Q sont difficiles à écrire et que leurs négations sont simples à énoncer.
Il ne faut pas confondre ce raisonnement avec le raisonnement que certains auteurs nomment « raisonnement par contraposée » qui est un raisonnement de type *modus ponens* avec la contraposée d'une implication. Par exemple, dans l'exemple **Col1**, on peut utiliser la contraposée de l'implication « $\forall(a ; b) \in \mathbb{R}^2 \ \ a = b \Rightarrow a^2 = b^2$ » pour conclure que $\sqrt{2}$ est différent de 1,414.

Exercice Col3
Démontrer que pour tout entier naturel n, si n^2 est pair alors n est pair.

Solution
On demande de démontrer l'implication : pour tout n entier naturel, si n^2 est pair alors n est pair.
La contraposée de cette implication est : pour tout n entier naturel, si n est impair, alors n^2 est impair.
Soit n un entier naturel impair. Il existe k entier naturel tel que $n = 2k + 1$.
Ainsi $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2k' + 1$ avec $k' = 2k^2 + 2k$ entier naturel. Donc n^2 est impair.
La contraposée est démontrée, donc pour tout n entier naturel, si n^2 est pair alors n est pair.

Remarque
La négation de « n est pair » est « n est impair ». Il est plus simple de traduire « n est impair » que de traduire et d'exploiter « n^2 est pair ». Ceci donne des indices pour tenter de démontrer la contraposée.

Exercice Col3bis
Démontrer que pour tout entier naturel, si $n^2 - 1$ est divisible par 8, alors n est impair.

Solution
On demande de démontrer l'implication : pour tout n entier naturel, si $n^2 - 1$ est divisible par 8 alors n est impair.
La contraposée de cette implication est : pour tout n entier naturel, si n est pair, alors $n^2 - 1$ n'est pas divisible par 8.
Soit n un entier naturel pair. Il existe k entier naturel tel que $n = 2k$.
Ainsi $n^2 - 1 = 4k^2 - 1 = 2(2k^2) - 1$ et $n^2 - 1$ est impair. $n^2 - 1$ n'est pas divisible par 2, *a fortiori* par 8.

La contraposée est démontrée, donc pour tout n entier naturel, si $n^2 - 1$ est divisible par 8 alors n est impair.

Remarque
On peut faire la même remarque que pour l'exercice précédent. Il semble difficile d'exploiter la proposition « n^2 — 1 est divisible par 8 ».

Exercice Sec3
Démontrer que pour tous entiers naturels a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, si $a_1 + a_2 + ... + a_8 + a_9 = 90$ alors il existe au-moins trois entiers dans $\{a_1 ; a_2 ; ... ; a_8 ; a_9\}$ dont la somme est supérieure ou égale à 30.

Solution
On demande de démontrer l'implication : pour tous a_1, a_2, ..., a_9 entiers naturels, si $a_1 + a_2 + ... + a_9 = 90$ alors il existe au moins trois entiers dans $a_1 ; a_2 ; ... ; a_8 ; a_9$ dont la somme est supérieure ou égale à 30.
La contraposée de cette implication est : pour tous a_1, a_2, ..., a_9 entiers naturels, si la somme de trois entiers quelconques de $\{a_1 ; a_2 ; ... ; a_8 ; a_9\}$ est strictement inférieure à 30 alors $a_1 + a_2 + ... + a_9 = 90$.
Ainsi $a_1 + a_2 + a_3 < 30$, de même $a_4 + a_5 + a_6 < 30$ et $a_7 + a_8 + a_9 < 30$. En ajoutant ces trois inégalités, on obtient $a_1 + a_2 + ... + a_9 < 30 + 30 + 30$ soit $a_1 + a_2 + ... + a_9 < 90$. La contraposée est démontrée, donc pour tout a_1, a_2, ..., a_9 entiers naturels, si $a_1 + a_2 + ... + a_9 = 90$ alors il existe au-moins trois entiers dans $\{a_1 ; a_2 ; ... ; a_8 ; a_9\}$ dont la somme est supérieure ou égale à 30.

Remarque
La négation de la proposition « il existe au moins trois entiers dans $\{a_1 ; a_2 ; ... ; a_8 ; a_9\}$ dont la somme est supérieure ou égale à 30 » est « la somme de trois entiers quelconques de $\{a_1 ; a_2 ; ... ; a_8 ; a_9\}$ est strictement inférieure à 30 ». On peut remarquer la transformation du quantificateur quand on énonce la négation.

Exercice Exp3
Démontrer que pour tout $(x ; y ; z) \in \mathbb{N}^3$, si 9 divise $x^3 + y^3 + z^3$ alors 3 divise x ou 3 divise y ou 3 divise z.

Solution
On demande de démontrer l'implication : pour tout $(x ; y ; z) \in \mathbb{N}^3$, si 9 divise $x^3 + y^3 + z^3$ alors 3 divise x ou 3 divise y ou 3 divise z.
La contraposée de cette implication s'écrit : pour tout $(x ; y ; z) \in \mathbb{N}^3$, si 3 ne divise ni x, ni y, ni z, alors 9 ne divise pas $x^3 + y^3 + z^3$.
On examine les congruences de x^3 modulo 9 suivant les congruences de x modulo 3.
Si $x \equiv 1$ (3) alors il existe $k \in \mathbb{Z}$ tel que $x = 3k + 1$. Ainsi $x^3 = 27k^3 + 27k^2 + 9k + 1 \equiv 1$ (9).
Si $x \equiv 2$ (3) alors il existe $k \in \mathbb{Z}$ tel que $x = 3k + 2$. Ainsi $x^3 = 27k^3 + 54k^2 + 36k + 8 \equiv 8$ (9).
Ainsi x^3 ou y^3 ou z^3 ne peuvent avoir que deux restes modulo 9.
Donc pour $x^3 + y^3 + z^3$ on obtient au maximum 8 résultats possibles.
On peut les déterminer grâce au tableau suivant :

x^3	y^3	z^3	$x^3+y^3+z^3$
1	1	1	3
1	1	8	1
1	8	1	1
1	8	8	8
8	1	1	1
8	1	8	8
8	8	1	8
8	8	8	6

Ainsi $x^3 + y^3 + z^3$ n'est jamais divisible par 9.
La contraposée est démontrée et on a bien démontré que pour tout triplet (x ; y ; z) d'entiers, si 9 divise $x^3 + y^3 + z^3$ alors au moins l'un des trois nombres x, y ou z est divisible par 3.

Remarque
La négation de la proposition « 3 divise x ou 3 divise y ou 3 divise z » s'écrit simplement « 3 ne divise ni x, ni y, ni z », ce qui rend possible de démontrer la contraposée.
Un raisonnement direct par disjonction des cas est possible. Il suffit d'envisager les 729 cas possibles de reste de la division euclidienne de x, y et z par 9 et d'examiner les cas où $x^3 + y^3 + z^3$ est divisible par 9. Ce raisonnement est nettement plus long !

VI - RAISONNEMENT PAR ÉQUIVALENCES

Le raisonnement par équivalences s'emploie principalement dans deux cas :

1- pour démontrer une proposition P, ce raisonnement consiste à déterminer une suite finie de propositions P_i avec i variant de 1 à n telles que et $P_1 = P$, que P_i est équivalente à P_{i+1} et que P_n est manifestement vraie ;

2- pour résoudre une équation ou une inéquation sur un ensemble D, ce raisonnement consiste à transformer successivement une équation en une équation équivalente (c'est-à-dire qui a le même ensemble de solutions) et aboutir à une équation de la forme $x \in A$ où A est un sous-ensemble de D.
Comme nous l'avons évoqué plus haut, le raisonnement par équivalences est assez rare en arithmétique. Il peut être utilisé avec les critères de divisibilité, avec les diviseurs d'un nombre entier... En effet, les critères sont des équivalences et les diviseurs d'un entier sont complètement connus.

Exercice Col4
Soient a et b deux nombres entiers naturels inférieurs ou égaux à 9. On considère le nombre N écrit en base 10 par $\overline{3a7b}$.
Déterminer a et b pour que N soit divisible par 9 et par 5.

Solution
On a les équivalences suivantes pour tous a et b :
N divisible par 9 et par 5 $\iff$ 3+ a + 7+ b divisible par 9 et (b = 0 ou b = 5)
$\iff$ a + b +1 divisible par 9 et (b = 0 ou b = 5)
$\iff$ (a + b = 8 ou a + b = 17) et (b = 0 ou b = 5)
car a + b est compris entre 0 et 18 (a et b représentent des chiffres)

$$\Leftrightarrow \begin{cases} b=0 \\ a=8 \end{cases} \text{ ou } \begin{cases} b=0 \\ a=17 \end{cases} \text{ ou } \begin{cases} b=5 \\ a=3 \end{cases} \text{ ou } \begin{cases} b=5 \\ a=12 \end{cases}$$

$$\Leftrightarrow \begin{cases} b=0 \\ a=8 \end{cases} \text{ ou } \begin{cases} b=5 \\ a=3 \end{cases}$$

car a et b représentent des chiffres, ils sont compris entre 0 et 9.

$\Leftrightarrow N = 3870$ ou $N = 3375$

Il y a exactement deux nombres N qui sont divisibles par 9 et par 5 : 3 870 et 3 375.

Remarque

Le raisonnement par équivalence a été possible car les critères de divisibilité sont des équivalences. Il est donc ici inutile de vérifier.

Exercice Sec4

Déterminer les entiers naturels n tels que $\frac{3n+2}{n+4}$ soit entier.

Solution

On a les équivalences suivantes pour tout entier naturel n :

$\frac{3n+2}{n+4}$ entier $\Leftrightarrow \frac{3n+12-10}{n+4}$ entier

$\Leftrightarrow 3 - \frac{10}{n+4}$ entier

$\Leftrightarrow \frac{10}{n+4}$ entier

$\Leftrightarrow n + 4$ divise 10

$\Leftrightarrow (n + 4 = -10$ ou $n + 4 = -5$ ou $n + 4 = -2$ ou $n + 4 = -1$ ou $n + 4 = 1$ ou $n + 4 = 2$

ou $n + 4 = 5$ ou $n + 4 = 10)$

$\Leftrightarrow (n = -14$ ou $n = -9$ ou $n = -6$ ou $n = -5$ ou $n = -3$ ou $n = -2$ ou $n = 1$ ou $n = 6)$

$\Leftrightarrow (n = 1$ ou $n = 6$ car n est entier naturel)

Il existe exactement deux valeurs de n qui rendent $\frac{3n+2}{n+4}$ entier : 1 et 6.

Remarque

Le raisonnement par équivalence a été possible car les transformations algébriques sont des équivalences et que l'on connaît exactement les diviseurs de 10.

Exercice Exp4

Résoudre l'équation dans $\mathbb{Z}^2$: $x^2 - y^2 = 7$.

Solution

On a les équivalences suivantes pour tous x et y :

$$x^2 - y^2 = 7 \iff (x-y)(x+y) = 7$$
$$\iff \begin{cases} x-y=-7 \\ x+y=-1 \end{cases} \text{ ou } \begin{cases} x-y=-1 \\ x+y=-7 \end{cases} \text{ ou } \begin{cases} x-y=1 \\ x+y=7 \end{cases} \text{ ou } \begin{cases} x-y=7 \\ x+y=1 \end{cases}$$
$$\iff (x\ ;\ y) = (-4\ ;\ 3) \text{ ou } (x\ ;\ y) = (-4\ ;\ -3) \text{ ou } (x\ ;\ y) = (4\ ;\ 3)$$
$$\text{ou } (x\ ;\ y) = (4\ ;\ -3)$$

L'ensemble des solutions est $S = \{(-4\ ;\ 3)\ ;\ (-4\ ;\ -3)\ ;\ (4\ ;\ 3)\ ;\ (4\ ;\ -3)\}$.

Remarque

Le raisonnement par équivalence a été possible car les transformations algébriques sont des équivalences et que l'on connaît exactement les diviseurs de 7.

VII – RAISONNEMENT PAR ANALYSE- SYNTHÈSE

Ce raisonnement comporte deux étapes : l'analyse puis la synthèse.

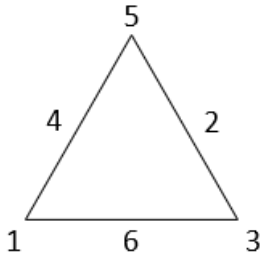
Dans la partie analyse, on suppose l'existence d'au moins une solution au problème et l'on cherche des conditions nécessaires sur cette solution. On en déduit le maximum d'informations permettant de construire ou de réduire l'ensemble des solutions candidates. Dans la partie synthèse, on examine si les conditions nécessaires obtenues dans la partie analyse sont suffisantes. On reporte dans le problème la ou les solutions candidates trouvées précédemment pour vérifier qu'elles sont bien solutions au problème. On obtient alors un ensemble (éventuellement vide) contenant les solutions au problème posé. Cette étape assure l'existence ou non de solutions et parfois l'unicité.

On peut remarquer que les domaines où ce raisonnement est pertinent se raréfient au cours des changements de programmes. Il était très employé dans la recherche d'ensembles de points (lieux géométriques), de constructions en géométrie. Ces problèmes ont disparu. L'arithmétique est aussi un domaine où ce raisonnement est fréquent. Comme nous l'avons dit plus haut, rares sont les situations en arithmétique où l'on peut raisonner par équivalences. Ainsi le raisonnement par analyse-synthèse prend toute sa place et son importance.

Exercice Col5

Les entiers de 1 à 6 sont placés aux sommets et sur les côtés d'un triangle.

La figure ci-dessous donne un exemple de placement des entiers.



On s'intéresse au placement des entiers tel que les sommes des trois entiers de chaque côté soient égales.

Déterminer, s'il existe, le placement donnant la somme minimale.

Même question en considérant un carré avec les entiers de 1 à 8.

Solution pour un triangle

On va effectuer un raisonnement par analyse-synthèse.

Analyse

On note S la somme égale sur chaque côté. Ainsi $3S$ correspond à la somme des 6 premiers entiers et des trois nombres aux sommets.

Donc $3S$ est inférieure ou égale à $(1 + 2 + 3 + 4 + 5 + 6) + (4 + 5 + 6)$ c'est-à-dire à 36 et est supérieure ou égale à $(1 + 2 + 3 + 4 + 5 + 6) + (1 + 2 + 3)$ c'est-à-dire à 27.

D'où S est inférieure ou égale à 12 et est supérieure ou égale à 9.

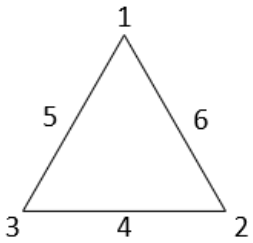
S prend ses valeurs dans l'ensemble $\{9 ; 10 ; 11 ; 12\}$.

Le minimum de S est donc supérieur ou égal à 9.

Synthèse

On vérifie que $S = 9$ est bien possible.

La configuration suivante le prouve :



Conclusion

La somme minimale cherchée est égale à 9 avec un placement possible (voir ci-dessus).

Solution pour un carré

On va effectuer un raisonnement par analyse-synthèse.

Analyse

On note S la somme égale sur chaque côté. Ainsi $4S$ correspond à la somme des 8 premiers entiers et des quatre nombres aux sommets.

Donc $4S$ est inférieure ou égale à $(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8) + (5 + 6 + 7 + 8)$ c'est-à-dire à 62 et est supérieure ou égale à $(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8) + (1 + 2 + 3 + 4)$ c'est-à-dire à 46.

D'où S est inférieure ou égale à 15 et est supérieure ou égale à 12 (S est un entier).

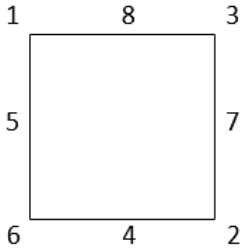
S prend ses valeurs dans l'ensemble $\{12; 13 ; 14 ; 15\}$.

Le minimum de S est donc supérieur ou égal à 12.

Synthèse

On vérifie que $S = 12$ est bien possible.

La configuration suivante le prouve :



Conclusion

La somme minimale cherchée est égale à 12 avec un placement possible (voir ci-dessus).

Remarque

L'analyse a consisté à déterminer un encadrement (en réalité un minorant aurait suffi) de la somme considérée et la synthèse a consisté à vérifier que ce minorant convenait. La difficulté, pour le cas du carré, a été de trouver la bonne configuration des nombres à placer.
On peut prolonger cet exercice, soit en changeant les nombres à placer, soit en travaillant avec un pentagone, un hexagone ... Certaines situations sont intéressantes car le minorant obtenu dans l'analyse ne convient pas. Cela permet de bien appréhender la notion de *condition nécessaire* et de *condition suffisante*.

Exercice Sec5

Déterminer tous les triplets (a ; b ; c) d'entiers naturels non nuls tels que $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1$.

Solution

On va effectuer un raisonnement par *analyse-synthèse.*

Analyse

On note a, b et c les entiers cherchés, *nécessairement* non nuls avec $1 \leq a \leq b \leq c$.

Puisque $a \leq b \leq c$, alors $\frac{1}{a} \geq \frac{1}{b} \geq \frac{1}{c}$ (fonction inverse décroissante sur [1 ; +∞ [), d'où $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \leq \frac{3}{a}$

et donc $1 \leq \frac{3}{a}$ ce qui implique $a \leq 3$.

Raisonnons par disjonction des cas : $a = 1$ ou $a = 2$ ou $a = 3$.

• Supposons $a = 1$. Ainsi $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1$ équivaut à $\frac{1}{b}+\frac{1}{c}=0$ ce qui est sans solution.

D'où $a \geq 2$.

• Supposons $a = 2$. Ainsi $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1$ équivaut à $\frac{1}{b}+\frac{1}{c}=\frac{1}{2}$. Or $2 \leq b \leq c$, d'où $\frac{1}{b}+\frac{1}{c} \leq \frac{2}{b}$ c'est-à-dire $\frac{1}{2} \leq \frac{2}{b}$, ce qui implique $b \leq 4$. Donc si $a = 2$, *nécessairement* $b \in \{2 ; 3; 4\}$. Nous pouvons chercher les solutions possibles :

si $a = 2$ et $b = 2$ alors $\frac{1}{c}=1-\frac{1}{2}-\frac{1}{2}=0$ ce qui est impossible,

si $a = 2$ et $b = 3$ alors $\frac{1}{c}=1-\frac{1}{2}-\frac{1}{3}=\frac{1}{6}$ d'où $c = 6$ et cette valeur convient car $a \leq b \leq c$.

si $a = 2$ et $b = 4$ alors $\frac{1}{c}=1-\frac{1}{2}-\frac{1}{4}=\frac{1}{4}$ d'où $c = 4$ et cette valeur convient car $a \leq b \leq c$.

• Supposons $a = 3$ alors $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1$ équivaut à $\frac{1}{b}+\frac{1}{c}=\frac{2}{3}$. Or $b \leq c$ d'où $\frac{1}{b}+\frac{1}{c} \leq \frac{2}{b}$ c'est-à-dire $\frac{2}{3} \leq \frac{2}{b}$.

D'où *nécessairement* $b \leq 3$ et comme $a = 3 \leq b \leq 3$, la seule valeur possible pour b est 3.

Si $a = 3$ et $b = 3$ alors $\frac{1}{c}=1-\frac{1}{3}-\frac{1}{3}=\frac{1}{3}$, d'où $c = 3$ et cette valeur convient.

Le problème admet trois triplets candidats-solutions : (2 ; 3 ; 6) , (2 ; 4 ; 4) et (3 ; 3 ; 3).

Synthèse

La synthèse est immédiate car $\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=1$, $\frac{1}{2}+\frac{1}{4}+\frac{1}{4}=1$ et $\frac{1}{3}+\frac{1}{3}+\frac{1}{3}=1$.

Conclusion

Le problème admet exactement trois triplets solutions : (2 ; 3 ; 6) , (2 ; 4 ; 4) et (3 ; 3 ; 3).

Remarque
L'analyse a permis d'obtenir une condition nécessaire : « $a \leq 3$ ». Ensuite, un raisonnement par disjonction des cas a permis d'obtenir trois triplets candidats. Grâce à la synthèse, ces trois triplets conviennent et sont donc les solutions au problème.
Comme dans la plupart du temps, la synthèse est très simple. Il suffit de vérifier que les valeurs trouvées dans l'analyse conviennent ou non.

Exercice Exp5
Déterminer les entiers naturels N tels que les 10 chiffres de 0 à 9 soient nécessaires une fois et une seule pour écrire N^3 et N^4 (le chiffre 0 ne pouvant pas être en premier dans l'écriture décimale).

Solution
On va effectuer un raisonnement par analyse-synthèse.

Analyse
On examine le nombre de chiffres possibles pour l'écriture de N .
Si N a un chiffre, alors N^3 a au plus 3 chiffres et N^4 a au plus 4 chiffres car $9^3 = 729$ et $9^4 = 6\,561$. Cela donne un total au maximum de 7 chiffres pour écrire N^3 et N^4. Ce n'est donc pas possible.

Si N a deux chiffres, alors N^3 a au moins 4 chiffres et au plus 6 chiffres et N^4 a au moins 5 chiffres et au plus 8 chiffres car $10^3 = 1\,000$, $98^3 = 941\,192$, $10^4 = 10\,000$ et $98^4 = 92\,236\,816$. Ce cas est *a priori* possible avec N^3 à 4 chiffres et N^4 à 6 chiffres. Le cas où N^3 et N^4 ont chacun 5 chiffres est impossible : si $N^4 \leq 99\,999$ alors $N \leq 17$ et 17^3 a strictement moins de 5 chiffres.

Si N a 3 chiffres ou plus, alors N^3 a au moins 7 chiffres car $102^3 = 1\,061\,208$. Il ne reste plus assez de chiffres pour écrire N^4.

Le seul cas possible est donc N^3 avec 4 chiffres et N^4 avec 6 chiffres.

On a : $\sqrt[3]{1\,023} \simeq 10{,}1$ et $\sqrt[3]{9\,876} \simeq 21{,}4$ et $\sqrt[4]{102\,345} \simeq 17{,}9$ et $\sqrt[5]{987\,654} \simeq 31{,}5$ (toutes les valeurs approchées sont données à 10^{-1} près).

Il ne reste que 4 cas possibles pour N : 18, 19, 20 et 21.

Synthèse
Si $N = 18$ alors $N^3 = 5\,832$ et $N^4 = 104\,976$, ce cas convient.
Si $N = 19$ alors $N^3 = 6\,859$ et $N^4 = 130\,321$, ce cas ne convient pas (deux fois le chiffre 1 par exemple).
Si $N = 20$, alors N^3 nécessite au moins deux chiffres 0. Ce cas ne convient pas.
Si $N = 21$, alors $N^3 = 9\,261$ et $N^4 = 130\,321$, ce cas ne convient pas (trois fois le chiffre 1 par exemple).

Conclusion Il n'existe qu'un seul entier naturel N tel que les 10 chiffres de 0 à 9 soient nécessaires une fois et une seule pour écrire N^3 et N^4 : le nombre 18.

Remarque
L'analyse a permis de réduire les possibilités pour N au nombre de quatre et la synthèse a permis de prouver qu'une seule possibilité sur les quatre était validée. Cet exemple montre que la synthèse est une étape indispensable, sans elle, on aurait donné quatre « solutions ».

VIII – RAISONNEMENT PAR L'ABSURDE

Le raisonnement par l'absurde consiste à démontrer la vérité d'une proposition P en prouvant que sa négation entraîne la vérité d'une proposition que l'on sait fausse, ou la vérité d'une proposition et de sa négation.

On peut distinguer deux schémas avec la structure suivante :

Schéma 1 : ((NON P) $\Longrightarrow R$) vraie ET R fausse

Schéma 2 : [(NON P) $\Longrightarrow$(R ET (NON R))] vraie.

D'après la règle du *modus tollens* si l'implication $P \Longrightarrow Q$ est vraie et si Q est fausse, alors P est fausse.

Dans le schéma 1 : ((NON P) $\Longrightarrow R$) vraie ET R fausse.

La proposition R est fausse et l'implication ((NON P) $\Longrightarrow R$) est vraie. Donc la proposition (NON P) est fausse, donc P est vraie.

Dans le schéma 2 : [(NON P) $\Longrightarrow$ (R ET (NON R))] vraie.

L'implication est vraie mais la proposition (R ET (NON R)) est fausse quelle que soit la proposition R (principe de non-contradiction). Donc la proposition (NON P) est fausse, donc P est vraie.

Les deux schémas diffèrent par la nature de la contradiction :

Dans le premier schéma, on sait par ailleurs que R est fausse alors que dans le deuxième schéma, (R ET NON R)) est fausse quelle que soit la proposition R.

Nous explicitons le cas où la proposition à démontrer est une implication. La proposition P devient $P \Longrightarrow Q$. Nous obtenons alors les deux schémas suivants où R est une proposition :

Schéma 1bis : [(P ET NON(Q)) $\Longrightarrow R$] vraie et R fausse

Schéma 2bis : [(P ET NON(Q)) $\Longrightarrow$ (R ET NON R)] vraie

Nous ne donnerons des exemples des schémas 1bis et 2bis qu'au niveau Terminale Maths Expertes. En effet, pour bien comprendre ces cas, il est nécessaire de savoir nier une implication, tâche que l'on ne peut demander au collège, ni même en classe de seconde. Les cas 2 et 2bis se rencontrent très souvent quand la proposition NON P est la conjonction de deux propositions NON P_1 et NON P_2 et on démontre que NON P implique P_2 et évidemment NON P_2.

Exercice Col6

Démontrer que $\frac{1}{3}$ n'est pas un décimal.

Solution

On effectue un raisonnement par l'absurde.

On suppose que $\frac{1}{3}$ est un décimal. Il existe donc un entier relatif a et un entier naturel n tels que $\frac{1}{3} = \frac{a}{10^n}$.

On en déduit que $3a = 10^n$. Ainsi 3 divise 10^n. Or la somme des chiffres de 10^n est 1, donc 10^n n'est pas divisible par 3.

On en déduit que $\frac{1}{3}$ n'est pas décimal.

Remarque

La proposition à démontrer est une proposition élémentaire et celle-ci est formulée de manière négative (« ne pas être décimal »), donc sa négation est simple à énoncer. Ceci permet une compréhension plus aisée du raisonnement par l'absurde.

D'autre part, nous sommes dans le cas (1) avec la proposition P « $\frac{1}{3}$ n'est pas décimal » et la proposition R « 10^n divisible par 3. ».

Exercice Sec6

Démontrer que 111 111 111 111 n'est pas un carré parfait.

Solution

On effectue un raisonnement par l'absurde.
On suppose que 111 111 111 111 est un carré parfait.
Ainsi $9 \times 111\,111\,111\,111 = 999\,999\,999\,999$ est aussi un carré parfait. Or $999\,999\,999\,999 = 10^{12} - 1$ et 10^{12} est un carré parfait. Ceci est absurde car 0 et 1 sont les deux seuls carrés parfaits qui diffèrent de 1.
Donc 111 111 111 111 n'est pas un carré parfait.

Remarque

Même remarque que pour l'exercice précédent. La négation de la proposition est simple à énoncer : « être un carré parfait ». La difficulté de l'exercice réside dans l'idée de multiplier par 9.
Ce n'est pas la seule démonstration possible. On peut remarquer que 111 111 111 111 est divisible par 3 et n'est pas divisible par 9.
D'autre part, nous sommes dans le cas schéma 1 avec la proposition P « 111 111 111 111 n'est pas un carré parfait » et la proposition R « 10^{12} — 1 et 10^{12} sont des carrés parfaits ».

Exercice Sec6bis

1. Démontrer que $\sqrt{3}$ est irrationnel.
2. Démontrer qu'un triangle équilatéral ne peut pas avoir ses trois sommets à coordonnées entières.

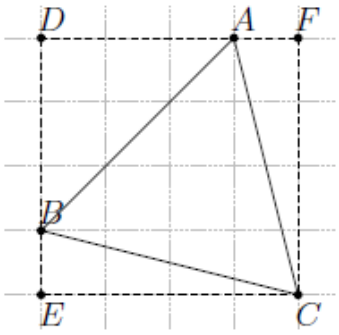
Solution

1. On effectue un raisonnement par l'absurde.
   On suppose que $\sqrt{3}$ est rationnel. Il existe a et b entiers naturels non nuls tels que $\sqrt{3} = \frac{a}{b}$ avec $\frac{a}{b}$ irréductible.
   Ainsi on obtient : $3b^2 = a^2$. D'où a^2 est divisible par 3.
   On démontre l'implication : pour tout $n \in \mathbb{N}$, si n^2 est divisible par 3, alors n est divisible par 3. Sa contraposée s'écrit : pour tout $n \in \mathbb{N}$, si n n'est pas divisible par 3, alors n^2 n'est pas divisible par 3.

   Soit n un entier non divisible par 3. Il existe $k \in \mathbb{N}$, tel que $n = 3k + 1$ ou $n = 3k + 2$. Si $n = 3k + 1$, alors $n^2 = 9k^2 + 6k + 1 = 3(6k^2 + 2k) + 1$ ou $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$. Dans les deux cas, n^2 n'est pas divisible par 3. La contraposée est démontrée et ainsi pour tout $n \in \mathbb{N}$, si n^2 est divisible par 3, alors n est divisible par 3.
   Grâce à cette implication, on déduit que a est divisible par 3. Ainsi il existe $a' \in \mathbb{N}$ tel que $a = 3a'$.
   D'où $b^2 = 3a'^2$. Par conséquent b^2 est divisible par 3 et donc b est divisible par 3. Les deux entiers a et b sont divisibles par 3. La fraction $\frac{a}{b}$ n'est pas irréductible, ce qui est faux.
   Donc $\sqrt{3}$ est irrationnel.

2. On raisonne par l'absurde.

On suppose que le triangle équilatéral, que l'on note ABC, a ses trois sommets à coordonnées entières. On construit le rectangle circonscrit au triangle ayant ses côtés parallèles aux axes. L'aire du rectangle est entière, les aires des triangles rectangles ADB, BEC et AFC sont rationnelles. On en déduit par soustraction que l'aire du triangle ABC est rationnelle. Or l'aire d'un triangle équilatéral de côté c est égale à $\frac{\sqrt{3}}{4}\ c^2$. Comme c^2 est entier (calculé d'après le théorème de Pythagore), on aboutit à la conclusion que $\sqrt{3}$ est rationnel ce qui est faux. Donc les trois sommets de ABC n'ont pas tous les trois des coordonnées entières.



Remarque

Les deux raisonnements par l'absurde sont faciles à débuter car les négations des deux propositions à démontrer s'énoncent aisément. La première question de cet exercice peut être un bon réinvestissement de la démonstration de $\sqrt{2}$ irrationnel et la deuxième question une belle utilisation de l'irrationalité de $\sqrt{3}$.

Pour la question **1.,** nous sommes dans le schéma 2. La proposition P est « $\sqrt{3}$ est irrationnel », ainsi NON P s'énonce « il existe a et b tels que $\sqrt{3} = \frac{a}{b}$ ET $\frac{a}{b}$ est irréductible ».

La supposition de NON P implique $\frac{a}{b}$ est irréductible et évidemment, par définition de NON P, que $\frac{a}{b}$ est irréductible.

Pour la question **2.**, nous sommes dans le schéma 1 avec la proposition P « un triangle équilatéral ne peut pas avoir ses trois sommets à coordonnées entières » et la proposition R « $\sqrt{3}$ est rationnel ».

Exercice Exp6

Démontrer que, pour tout entier $n \geq 3$, il existe un nombre premier tel que $n < p < n!$.

Solution

On va raisonner par l'absurde. La négation de la proposition à démontrer s'écrit « il existe un entier naturel n tel qu'il n'existe pas de nombre premier p tel que $n < p < n!$ ». Soit n un tel entier. On considère alors le nombre $N = n! - 1$.

Comme $n \geq 3$, $n! = 1 \times 2 \times \ldots \times n \geq 2n$. D'où $n! - 1 \geq 2n - 1$ et $2n - 1 > n$ dès que $n > 1$. Ainsi $n! - 1 > n$ et évidemment $n! - 1 < n!$. Ainsi N n'est pas premier car on a supposé qu'il n'existe pas de nombre premier p tel que $n < p < n!$.

N n'étant pas premier, il existe un nombre premier p qui divise N. Comme il n'existe pas de nombre premier strictement entre n et $n!$, ce nombre premier p vérifie $p \leq n$. Ainsi p divise $n!$ et il divise N. Il divise leur différence 1. D'où $p = 1$. Ceci est faux car 1 n'est pas premier.

Donc pour tout entier $n \geq 3$, il existe un nombre premier p tel que $n < p < n!$.

Remarque

La proposition à démontrer est une proposition élémentaire. La démonstration est très proche de celle de l'infinitude des nombres premiers.

Nous sommes dans le schéma 1 avec la proposition P « pour tout entier $n \geq 3$, il existe un nombre premier p tel que $n < p < n!$ » et la proposition R « 1 est un nombre premier ».

Exercice Exp6bis

Démontrer que, pour tout $n \geq 2$ entier naturel, $u_n = \sum_{k=1}^{n} \frac{1}{i}$ n'est pas un entier.

Solution

On effectue un raisonnement par l'absurde. La négation de la proposition à démontrer s'écrit : « il existe un entier naturel n supérieur ou égal à 2 tel que u_n soit entier ».

Soit n un tel entier.

On a $u_2 = 1 + \frac{1}{2} = \frac{3}{2}$ et $u_3 = 1 + \frac{1}{2} + \frac{1}{3} = \frac{11}{6}$. Ainsi n est supérieur ou égal à 4.

Pour tout $i \in [\![1; n]\!]$, on note $i = 2^{k_i} p_i$ où 2^{k_i} la plus grande puissance de 2 qui divise i.

Donc p_i est impair.

On considère k le maximum des k_i pour $1 \leq i \leq n$. Ainsi 2^k est la plus grande puissance de 2 qui divise l'un des entiers de $[\![1; n]\!]$. Comme n est supérieur ou égal à 2, k n'est pas nul. De plus cette puissance 2^k n'intervient qu'une seule fois dans les décompositions en facteurs premiers des entiers de $[\![1; n]\!]$. En effet le nombre le plus petit ayant 2^k comme diviseur est 2^k. Le suivant est $2^k \times 3$, or $2^k \times 3$ est supérieur à 2^{k+1}. Donc $2^k \times 3$ n'appartient pas à $[1 ; n]$ puisque 2^k est la plus grande puissance de 2 divisant les entiers de $[\![1; n]\!]$.

Ainsi $n! = \prod_{\ell=1}^{n} 2^{k_\ell} p_\ell = 2^{k'} p$ où $k' = \sum_{\ell=1}^{n} k_\ell$ et $p = \prod_{\ell=1}^{n} p_\ell$.

On peut remarquer que pour tout $i \in [\![1; n]\!]$ $k' > k_i$ car il y a au moins deux entiers divisibles par 2 dans $[\![1; n]\!]$ (≥ 4).

Donc pour $i \in [\![1; n]\!]$, $\frac{n!}{i} = 2^{k'-k_i} \frac{p}{p_i} = 2^{k'-k_i} q_i$ où $q_i = \frac{p}{p_i}$. D'après la définition de p, q_i est un entier.

On a $n! u_n = \sum_{i=1}^{n} \frac{n!}{i}$. On en déduit : $2^{k'} p u_n = \sum_{i=1}^{n} 2^{k'-k_i} q_i$.

En divisant cette égalité par $2^{k'-k}$, on obtient $2^k p u_n = \sum_{i=1}^{n} 2^{k-k_i} q_i$.

On note j le nombre 2^k, c'est-à-dire l'entier de $[\![1 ; n]\!]$ qui a la plus grande puissance de 2 comme diviseur.

D'où $\sum_{i=1}^{n} 2^{k-k_i} q_i = \sum_{i=1}^{n} \sum_{i \neq j} 2^{k-k_i} q_i + q_j$ et $2^k p u_n = \sum_{i=1}^{n} \sum_{i \neq j} 2^{k-k_i} q_i + q_j$

Le membre de gauche de cette dernière égalité est pair car k est non nul et le membre de droite est impair car pour $i \neq j$, $k - k_i = 0$ et q_j est impair. On aboutit à une contradiction.

Pour tout $n \geq 2$, u_n n'est pas entier.

Remarque

La proposition à démontrer est une proposition élémentaire. Sa négation est très simple à énoncer. La difficulté de l'exercice provient de l'exploitation de cette négation.

Exercice Exp6ter

Démontrer l'implication suivante : $\forall (a ; b ; c) \in \mathbb{N}^3 \quad a + b\sqrt{2} + c\sqrt{3} = 0 \Rightarrow a = b = c = 0$.

Solution

On va démontrer cette implication par l'absurde.

On suppose qu'il existe un triplet $(a ; b ; c)$ de $\mathbb{N}^3$ tel que $a + b\sqrt{2} + c\sqrt{3} = 0$ et ($a \neq 0$ OU $b \neq 0$ OU $c \neq 0$).

On va raisonner par disjonction des cas selon la nullité des nombres a, b et c.

- Premier cas : $b = 0$

On a alors $a + c\sqrt{3} = 0$

Si $c = 0$ alors $a \neq 0$ car au moins un des trois nombres a, b et c est non nul. Et $a + b\sqrt{2} + c\sqrt{3} = 0$ devient $a = 0$. Ceci est faux car $a \neq 0$.

Si $c \neq 0$ alors $\sqrt{3} = -\frac{a}{c}$. Ceci est faux car $\sqrt{3}$ est irrationnel.

- Deuxième cas : $b \neq 0$

Si $c = 0$ alors $a + b\sqrt{2} = 0$ et $\sqrt{2} = -\frac{a}{b}$. Ceci est faux car $\sqrt{2}$ est irrationnel.

Si $c \neq 0$, alors $b\sqrt{2} + c\sqrt{3} = -a$. On en déduit que $(b\sqrt{2} + c\sqrt{3})^2 = a^2$ c'est-à-dire $2b^2 + 3c^2 + 2bc\sqrt{6} = a^2$.

Ainsi $\sqrt{6} = \frac{a^2 - 2b^2 - 3c^2}{2bc}$. Ceci est faux car $\sqrt{6}$ est irrationnel.

Dans tous les cas, on aboutit à une proposition fausse (contradiction). La proposition « il existe un triplet $(a\ ;\ b\ ;\ c)$ de $\mathbb{N}^3$ tel que $a + b\sqrt{2} + c\sqrt{3} = 0$ et ($a \neq 0$ OU $b \neq 0$ OU $c \neq 0$) » est fausse. L'implication cherchée est alors vraie.

Remarque

La proposition à démontrer est une proposition implicative. Pour la démontrer par l'absurde, il est nécessaire de savoir la nier. On rappelle que la négation de $P \Longrightarrow Q$ est P ET NON Q.

De plus un raisonnement par disjonction des cas a été nécessaire pour utiliser l'hypothèse que $(a\ ;\ b\ ;\ c) \neq (0\ ;\ 0\ ;\ 0)$.

D'autre part nous sommes dans le schéma (1bis) avec la proposition P « il existe un triplet $(a\ ;\ b\ ;\ c)$ de $\mathbb{N}^3$ tel que $a + b\sqrt{2} + c\sqrt{3} = 0$ et ($a \neq 0$ OU $b \neq 0$ OU $c \neq 0$) » et la proposition R « $\sqrt{3}$ est rationnel » dans le cas $b = 0$ et la proposition R « $\sqrt{6}$ est rationnel » dans le cas où $b \neq 0$.

IX – RAISONNEMENT PAR RÉCURRENCE

Il existe plusieurs formes du raisonnement par récurrence. Elles sont toutes équivalentes sur $\mathbb{N}$.

On considère une proposition $P[n]$ où n est un entier naturel.

Principe de récurrence « simple »

Si la proposition $P[n]$ vérifie :

$P[0]$ est vraie (initialisation),

et, pour tout entier naturel k, $(P[k] \Longrightarrow P[k+1])$ est vraie (hérédité)[1]

alors, pour tout n, $P[n]$ est vraie.

Plus formellement : $(P[0]$ ET $\forall k \in \mathbb{N}\ \ P[k] \Longrightarrow P[k+1]) \Longrightarrow (\forall n \in \mathbb{N}\ \ P[n])$.

Principe de récurrence « double »

Cette forme du principe de récurrence intervient lorsque la relation de récurrence porte sur deux valeurs consécutives de n.

Si la proposition $P[n]$ vérifie :

$P[0]$ et $P[1]$ sont vraies (initialisation),

[1] Il peut être intéressant de changer le nom de la variable dans l'implication : l'appeler k au lieu de n pour bien distinguer les différents rôles de la variable dans toutes ces écritures.

et, pour tout entier naturel k, $((P[k] \text{ ET } P[k+1]) \Longrightarrow P[k+2])$ est vraie (hérédité)
alors, pour tout n, $P[n]$ est vraie.
Plus formellement :
$(P[0] \text{ ET } P[1] \text{ ET } (\forall k \in \mathbb{N}\ (P[k] \text{ ET } P[k+1]) \Longrightarrow P[k+2]) \Longrightarrow ((\forall n \in \mathbb{N}\ P[n])$.

Principe de récurrence « forte »
On peut avoir besoin, pour prouver que, pour tout n, $P[n]$ est vraie, de faire l'hypothèse que $P[n]$ vraie pour tous les entiers m inférieurs à l'entier n générique. Un cas particulier est celui où la proposition $P[n]$ est définie en fonction de valeurs précédentes de n. Le principe de récurrence s'écrit alors ainsi :
Si la proposition $P[n]$ vérifie :
$P[0]$ est vraie (initialisation),
et, pour tout entier naturel k, $((\forall h \leq k\ , P[h]) \Longrightarrow P[k+1])$ est vraie (hérédité)
alors, pour tout n, $P[n]$ est vraie.
Plus formellement : $(P[0] \text{ ET } (\forall k \in \mathbb{N}\ ((\forall h \leq k\ , P[h]) \Longrightarrow P[k+1])) \Longrightarrow (\forall n \in \mathbb{N}\ P[n])$.

1. Récurrence simple

Exercice Exp7

Démontrer que pour tout $n \geq 3$, l'équation $1 = \frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}$ admet au moins une solution en nombres entiers positifs tous distincts.

Solution

Soit n un entier naturel. On note $P[n]$ la proposition : « l'équation $1 = \frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}$ admet au moins une solution en nombres entiers positifs tous distincts ».
On démontre par récurrence que $P[n]$ est vraie pour tout $n \geq 3$.
Initialisation
$P[3]$ s'écrit : « l'équation $1 = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$ admet au moins une solution en nombres entiers positifs tous distincts.
$P[3]$ est vraie car $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.
Hérédité
On démontre l'implication : $\forall n \geq 3\ \ P[n] \Longrightarrow P[n+1]$.
Soit $n \in \mathbb{N}$ tel que $P[n]$ est vraie. On veut démontrer qu'alors $P[n+1]$ est vraie.
Il existe n entiers positifs tous distincts tels que $1 = \frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}$.
On en déduit que $\frac{1}{2} = \frac{1}{2x_1} + \frac{1}{2x_2} + \ldots + \frac{1}{2x_n}$.
Ainsi $1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + \frac{1}{2x_1} + \frac{1}{2x_2} + \ldots + \frac{1}{2x_n}$. On peut remarquer que pour tout $i \in [\![1\ ;\ n]\!]$ x_i est différent de 1 car $n \geq 3$. Les x_i étant tous distincts entre eux et différents de 1, les entiers 2, $2x_1$, $2x_2$, …, $2x_n$ sont tous distincts. Ceci montre que $P[n+1]$ est vraie.
L'implication $(\forall n \geq 3\ \ P[n] \Longrightarrow P[n+1])$ est démontrée, la proposition est héréditaire à partir de $n = 3$.
Conclusion $P[3]$ est vraie et la proposition $P[n]$ est héréditaire à partir de $n = 3$, d'après le principe de récurrence, $P[n]$ est vraie pour tout $n \geq 3$.
Ainsi pour tout $n \geq 3$, l'équation $1 = \frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}$ admet au moins une solution en nombres entiers

positifs tous distincts.

Remarque
Un des intérêts de cet exercice concerne l'indice d'initialisation et d'hérédité. Il n'est égal ni à 0, ni à 1.

Exercice Exp7bis

Démontrer que pour tout n entier naturel, $4^{2n+2} - 15n - 16$ est divisible par 225.

Solution
On va effectuer un raisonnement par récurrence. On note $P[n]$ la proposition « $4^{2n+2} - 15n - 16$ est divisible par 225 ».
Initialisation
$P[0]$ s'écrit : $4^2 - 15 \times 0 - 16$ est divisible par 225.
Or $4^2 - 15 \times 0 - 16 = 0$ donc $P[0]$ est vraie.
Hérédité
On veut démontrer l'implication $\forall n \in \mathbb{N} \quad P[n] \Longrightarrow P[n+1]$
On veut donc démontrer que pour tout n entier naturel, si $4^{2n+2} - 15n - 16$ est divisible par 225, alors $4^{2(n+1)+2} - 15(n+1) - 16$ est divisible par 225.
Soit n un entier naturel tel que $4^{2(n+1)+2} - 15(n+1) - 16$ est divisible par 225.
Ainsi il existe un entier k tel que $4^{2n+2} - 15(n+1) - 16 = 225k$.
D'où $4^{2(n+1)+2} - 15(n+1) - 16$
$= 16 \times 4^{2n+2} - 16 \times 15n - 16 \times 16 + 16 \times 15n - 15n - 15 + 16 \times 16 - 16$
$= 16\,(4^{2n+2} - 15n - 16) + 15n(16 - 1) + 256 - 31 = 16 \times 225k + 225n + 225$
$= 225(16k + n + 1)$
Ainsi $4^{2(n+1)+2} - 15(n+1) - 16$ est divisible par 225. La proposition $P[n+1]$ est vraie.
L'implication $(\forall n \in \mathbb{N} \quad P[n] \Longrightarrow P[n+1])$ est démontrée, la proposition est héréditaire à partir de $n = 0$.
Conclusion
La proposition $P[0]$ est vraie et l'hérédité est prouvée pour $n \geq 0$. D'après le principe de récurrence, la proposition $P[n]$ est vraie pour tout $n \in \mathbb{N}$.
On a bien prouvé que pour tout n entier naturel $4^{2n+2} - 15n - 16$ est divisible par 225.

Remarque
Le raisonnement par récurrence est ici très performant. Habituellement, pour ce type d'exercice, les congruences sont un outil efficace. Le problème, ici, est que l'on doit travailler modulo 225 et que dans l'expression $4^{2n+2} - 15n - 16$ la variable n figure dans une expression affine et en exposant. Ceci rend la méthode par congruences peu efficace.

2. Récurrence multiple

Exercice Exp8

Soit x un réel tel que $x + \frac{1}{x}$ soit entier.
Démontrer que, pour tout entier naturel n non nul, $x^n + \frac{1}{x^n}$ est entier.

Solution
On va effectuer un raisonnement par récurrence double.

Soit $n \in \mathbb{N}^*$. On note $P[n]$ la proposition : $x^n + \frac{1}{x^n}$ est entier.

Initialisation

$P[1]$ s'écrit : $x + \frac{1}{x}$ est entier. $P[1]$ est vraie par hypothèse.

$P[2]$ s'écrit $x^2 + \frac{1}{x^2}$ est entier. Or $x^2 + \frac{1}{x^2} = (x + \frac{1}{x})^2 - 2$. Donc $x^2 + \frac{1}{x^2}$ est entier.

$P[2]$ est vraie.

Hérédité

On démontre l'implication : $\forall n \geq 1$, $(P[n]$ ET $P[n+1]) \Longrightarrow P[n+2]$

Pour tout n entier naturel, il suffit de démontrer que si $P[n]$ et $P[n+1]$ sont vraies, alors $P[n+2]$ est vraie.

Soit $n \in \mathbb{N}^*$ tel que $P[n]$ et $P[n+1]$ sont vraies. On suppose donc que $x^n + \frac{1}{x^n}$ et $x^{n+1} + \frac{1}{x^{n+1}}$ sont entiers et on veut démontrer que $x^{n+2} + \frac{1}{x^{n+2}}$ est entier.

Ainsi $x^{n+2} + \frac{1}{x^{n+2}} = (x^{n+1} + \frac{1}{x^{n+1}})(x + \frac{1}{x}) - (x^n + \frac{1}{x^n})$

Or $x^{n+1} + \frac{1}{x^{n+1}}$ est entier car $P[n+1]$ est vraie, de même pour $x^n + \frac{1}{x^n}$ car $P[n]$ est vraie. Enfin $x + \frac{1}{x}$ est entier. Ainsi $x^{n+2} + \frac{1}{x^{n+2}}$ est entier.

Ceci prouve que la proposition $P[n+2]$ est vraie si $P[n]$ et $P[n+1]$ sont vraies.

L'implication cherchée est démontrée, la proposition est héréditaire à partir de $n = 1$.

Conclusion

$P[1]$ et $P[2]$ sont vraies et la proposition $P[n]$ est héréditaire à partir de $n = 1$, d'après le principe de récurrence double, $P[n]$ est vraie pour tout $n \geq 1$.

Ainsi, pour tout entier naturel n non nul, $x^n + \frac{1}{x^n}$ est entier.

Exemple Exp8bis

Démontrer que cos 1° est irrationnel.

Solution

On raisonne par l'absurde. On suppose que cos 1° est rationnel et on va démontrer par récurrence double que cos n° est rationnel pour tout $n \in \mathbb{N}$.

On note pour $n \in \mathbb{N}$, la proposition $P[n]$: « cos n° est rationnel ».

Initialisation

$P[0]$ s'écrit : cos 0° est rationnel.

$P[0]$ est vraie car cos 0° = 1.

$P[1]$ s'écrit : cos 1° est rationnel.

$P[1]$ est vraie car c'est ce que l'on a supposé.

Hérédité

On montre l'implication :

$$\forall n \in \mathbb{N}, \quad (P[n] \text{ ET } P[n+1]) \Longrightarrow P[n+2].$$

Pour tout n entier naturel, on veut démontrer que si $P[n]$ et $P[n+1]$ sont vraies, alors $P[n+2]$ est vraie.

Soit $n \in \mathbb{N}^*$ tel que $P[n]$ *et* $P[n+1]$ sont vraies. On suppose donc que cos n° et cos$(n+1)$° sont rationnels et on veut démontrer que cos$(n+2)$° est rationnel.

On a : cos$(n+2)$° + cos n° = 2cos$(n+1)$° cos 1° en appliquant la formule :

cos$(a+b)$ + cos$(a-b)$ = 2cos a cos b.

On sait que cos$(n+1)$°, cos(n)° et que cos 1° sont rationnels. On en déduit que cos$(n+2)$° est rationnel.

L'implication cherchée est prouvée. La proposition $P[n]$ est héréditaire à partir de 0.

Conclusion

Comme $P[0]$ et $P[1]$ sont vraies et que l'implication $\forall n \in \mathbb{N}$, $(P[n] \text{ ET } P[n+1]) \Longrightarrow P[n+2]$, est vraie, d'après le principe de récurrence double, la proposition $P[n]$ est vraie pour tout $n \in \mathbb{N}$.

En particulier P[45] est vraie, ce qui signifie que $\cos 45° = \frac{\sqrt{2}}{2}$ est rationnel. Or ceci est faux, l'hypothèse « cos 1° rationnel » est fausse. Ainsi cos 1° est irrationnel.

Remarque

Cet exemple est intéressant car il s'appuie sur deux types de raisonnement : par récurrence et par l'absurde. Le raisonnement par récurrence est double car $\cos(n+2)$ s'exprime simplement en fonction de $\cos(n+1)$ et de $\cos(n)$.

La récurrence double s'utilise très naturellement pour étudier les suites numériques d'ordre 2.

3. Récurrence forte

Exercice Exp9

Tout entier naturel $n \geq 2$ est soit premier, soit peut s'écrire sous la forme d'un produit de nombres premiers.

Solution

Démontrons ce résultat par un raisonnement par récurrence forte.

Pour tout $n \geq 2$, soit $P[n]$: « L'entier n soit est premier, soit peut s'écrire sous la forme d'un produit de nombres premiers ».

Initialisation

2 est un nombre premier. $P[2]$ est donc bien vraie.

Hérédité

On veut démontrer l'implication suivante : pour tout $n \geq 2$, si $P[k]$ est vraie pour tout $2 \leq k \leq n$ alors $P[n+1]$ est vraie.

Soit $n \geq 2$. Supposons que pour tout $k \in [\![2\ ;\ n]\!]$, $P[k]$ est vraie, i.e. supposons que tout entier k appartenant à $[\![2\ ;\ n]\!]$, soit est premier, soit peut s'écrire comme un produit de nombres premiers.

Deux cas se présentent :

• Si $n+1$ est *premier*, alors $P[n+1]$ est bien vraie.

• Si $n+1$ n'est pas premier, alors il existe (au moins un) diviseur a (entier naturel non nul) tel que : $a \neq 1$ et $a \neq n+1$, et par conséquent il existe b, $b \neq 1$ et $b \neq n+1$ tels que $n+1 = a \times b$.

On en déduit $a \in [\![2\ ;\ n]\!]$, or on a supposé que pour tout $k \in [\![2\ ;\ n]\!]$, k soit est premier, soit peut s'écrire comme un produit de nombres premiers, on peut en déduire que a est premier ou peut s'écrire comme produit de nombres premiers. De même pour b donc b soit est premier, soit peut s'écrire comme un produit de nombres premiers, on en déduit que ab, c'est-à-dire $n+1$ s'écrit également comme produit de nombres premiers. Donc dans ce cas également, $P[n+1]$ est bien vraie.

Ainsi dans tous les cas, pour tout entier naturel $n \geq 2$, $P[n] =) P[n+1]$.

Conclusion

D'après le principe de récurrence forte, pour tout entier naturel n, $n \geq 2$, $P[n]$ est vraie, i.e. tout entier $n \geq 2$ soit est premier, soit peut s'écrire sous la forme d'un produit de nombres premiers.

Remarques

• L'intérêt d'utiliser ici une récurrence forte réside dans le fait que, comme on suppose $P[k]$ vraie pour tous les rangs k compris entre 2 et n, on peut ensuite l'appliquer à a et b (les diviseurs de $n + 1$), même si on ne sait pas explicitement qui ils sont : il suffit de savoir que ce sont des entiers compris entre 2 et n. Si on supposait seulement $P[n]$ vraie, on ne pourrait rien dire a priori sur a et b !

Ceci illustre bien la puissance pratique d'un raisonnement par récurrence forte, par rapport à une récurrence classique dans ce cas.

• Le raisonnement par récurrence forte est particulièrement utile dans certains problèmes de divisibilité comme on vient de le voir ou dans les exercices sur les suites lorsque le terme général de la suite est fonction de tous les termes précédents.

X - RAISONNEMENT PAR DESCENTE INFINIE DE FERMAT

Le principe s'énonce ainsi : « il n'existe pas de suite infinie strictement décroissante d'entiers positifs ». Sur $\mathbb{N}$, cet énoncé est équivalent aux énoncés sur le principe de récurrence donnés précédemment. Dans certains problèmes, il est plus simple à utiliser. C'est le cas, en pratique, lorsque $P[n]$ est une propriété d'un ensemble d'objets indicé par n, qu'on ne peut passer d'un objet quelconque de taille n à un objet quelconque de taille $n + 1$ et que l'on veut démontrer que quel que soit n, $P[n]$ est fausse.

Le raisonnement est le suivant : on démontre que pour tout n tel que $P[n]$ est vraie, on peut trouver un $m < n$ tel que $P[m]$ est vraie. Ce qui revient à construire une suite infinie d'entiers strictement décroissante telle que $P[n]$ est vraie. Ceci est impossible. Donc $P[n]$ est fausse quel que soit n.

Exercice Exp10

Démontrer que $\sqrt{2}$ est irrationnel.

Solution

On suppose que $\sqrt{2}$ est rationnel, c'est-à-dire qu'il existe deux entiers relatifs p et q tels que $\sqrt{2} = \frac{p}{q}$. On peut choisir p et q entiers naturels car $\sqrt{2}$ est positif.

De $\sqrt{2} \neq 0$, on déduit que $p \neq 0$. De même de $\sqrt{2} \neq 1$, on déduit $p \neq q$ et donc $p-q \neq 0$.

Si $p^2 = 2q^2$ alors $p^2 - pq = 2q^2 - pq$, c'est-à-dire $p(p - q) = q(2q - p)$.

On en déduit que $\frac{p}{q} = \frac{2q - p}{p-q}$.

Montrons maintenant que $0 < 2q - p < p$ et que $0 < p-q < q$.

On a : $1 < \sqrt{2} < 2$, donc $q < p < 2q$.

Ainsi $0 < p - q < q$.

De même, on obtient $q < p < 2q < 2p$, donc $0 < 2q - p < p$.

Ainsi $\frac{p}{q} = \frac{p_1}{q_1}$ avec p_1 et q_1 entiers naturels vérifiant $0 < p_1 < p$ et $0 < q_1 < q$. On réitère le procédé opéré sur p et q sur les entiers p_1 et q_1.

Ainsi $\frac{p}{q} = \frac{p_1}{q_1} = \frac{p_2}{q_2} = \ldots$

On construit ainsi deux suites d'entiers naturels non nuls (p_n) et (q_n) strictement décroissantes.

Ceci est en contradiction avec le principe de Fermat.

Ainsi la proposition initiale supposée vraie est fausse.

$\sqrt{2}$ n'est pas rationnel.

Exercice Exp10bis

Démontrer que l'équation $x^3 + 2y^3 = 4z^3$ n'a pas de solution dans $\mathbb{N}^3$ autre que (0 ; 0 ; 0).

Solution

Préliminaire : la proposition « pour tout entier naturel n, si n^3 est pair alors n est pair » est vraie.
Démontrons la proposition équivalente, sa contraposée, « pour tout entier naturel n, si n est impair alors n^3 est impair » : soit n entier naturel ; si n est impair, il existe un entier naturel k tel que $n = 2k + 1$ d'où $n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 4k + 1 = 2(4k^3 + 6k^2 + 2k) + 1$ ce qui prouve que n^3 est impair puisque $4k^3 + 6k^2 + 2k$ est alors un entier naturel. Par contraposition, pour tout entier naturel n, n^3 pair $\Longrightarrow$ n pair.
Le triplet (0 ; 0 ; 0) est solution évidente de (E) dans $\mathbb{N}^3$. Effectuons un raisonnement par l'absurde.

On suppose qu'il existe un triplet (a ; b ; c) solution de (E) avec a, b et c entiers non tous nuls c'est-à-dire (a ; b ; c) $\neq$ (0 ; 0 ; 0). Dans ce cas, $a^3 = 4c^3 - 2b^3 = 2(2c^3 - b^3)$ où $(2c^3 - b^3)$ est un entier naturel donc a^3 est pair. De a^3 pair on déduit a pair (préliminaire) d'où il existe un entier naturel a' tel que $a = 2a'$.
L'égalité $a^3 + 2b^3 = 4c^3$ devient : $8a'^3 + 2b^3 = 4c^3$ soit $4a'^3 + b^3 = 2c^3$ d'où $b^3 = 2c^3 - 4a'^3 = 2(c^3 - 2a'^3)$ où $(c^3 - 2a'^3)$ est entier naturel ce qui entraîne b^3 pair. De b^3 pair on déduit b pair (préliminaire) d'où il existe un entier naturel b' tel que $b = 2b$.
L'égalité $4a'^3 + b^3 = 2c^3$ devient alors $4a'^3 + 8b'^3 = 2c^3$ d'où $2a'^3 + 4b'^3 = c^3$ ce qui entraîne c^3 pair. De c^3 pair on déduit c pair (préliminaire) d'où il existe un entier naturel c' tel que $c = 2c'$. En remplaçant dans l'égalité $2a'^3 + 4b'^3 = c^3$ on obtient $2a'^3 + 4b'^3 = 8c'^3$ c'est-à-dire $a'^3 + 2b'^3 = 4c'^3$.
On vient de démontrer que si (a ; b ; c) est solution dans $\mathbb{N}^3$ de $x^3 + 2y^3 = 4z^3$ autre que (0 ; 0 ; 0) alors $(a'; b'; c') = (\frac{a}{2} ; \frac{b}{2} ; \frac{c}{2})$ est aussi solution dans $\mathbb{N}^3$ de cette même équation $x^3 + 2y^3 = 4z^3$ et autre que (0 ; 0 ; 0). On peut réitérer le procédé.
On a supposé (a ; b ; c) $\neq$ (0 ; 0 ; 0) donc au moins un des entiers a, b ou c n'est pas nul ; on peut supposer $a \neq 0$. On constitue ainsi une suite infinie de solutions entières strictement décroissante ($a' = \frac{a}{2}$ et $\frac{a}{2} < a$), ce qui contredit le principe de descente infinie de Fermat.
On conclut que l'équation $x^3 + 2y^3 = 4z^3$ n'a pas dans $\mathbb{N}^3$ de solution autre que (0 ; 0 ; 0).

XI - CONCLUSION

Nous avons donc bien montré que l'arithmétique est un domaine des mathématiques où l'apprentissage du raisonnement peut être privilégié. En effet, tous les types de raisonnement que l'on rencontre en mathématiques dans le secondaire peuvent être présents. Une des spécificités de l'arithmétique est que l'on peut travailler avec très peu de connaissances, ce qui explique que nous avons pu exhiber des exemples de niveau collège ou seconde. On peut donc regretter que ce domaine ne soit pas plus développé, notamment au lycée dans les programmes de spécialité des classes de première et terminale.

CONJECTURER, DÉBATTRE, RAISONNER EN ARITHMETIQUE, EN FORMATION INITIALE DES ENSEIGNANTS ET AU COLLÈGE

Thérèse GILBERT
Formatrice d'enseignants, HAUTE ÉCOLE GALILÉE
GEM
therese.gilbert@galilee.be

Daniel ZIMMER
Doctorant, UCLOUVAIN
GEM
daniel.zimmer@uclouvain.be

Résumé
Au départ, une situation d'arithmétique. Elle a l'air simple et pourtant… À partir de « vrai ou faux ? » conçus par les participants, on lance le débat. C'est l'occasion de préciser sa pensée, de réfléchir par analogie, ou de se méfier des analogies, de déjouer des pièges, de contredire, de chercher des contre-exemples, d'envisager une réciproque, de structurer la solution et l'argumentation, de penser en mathématiques.
Dans cet atelier, nous avons fait vivre un débat, en avons raconté l'expérimentation au collège et en formation initiale des enseignants et en avons évoqué d'autres.
Ce fut l'occasion de répondre à notre manière à la question « raisonner en arithmétique, est-ce incongru ? ».

> *Quelle partie des mathématiques enseigner ? Ça n'a pas d'importance. Ce qui est important est que les élèves aient rencontré, au moins une fois, un raisonnement qui les ait convaincus de la vérité de tel résultat, alors même que cette vérité ne leur était pas intuitive (Weil, 1991, p. 10).*

I - INTRODUCTION

1. Motivation et accroche

Souvent, dans les manuels, dans les cours de mathématiques, les élèves doivent montrer leur aptitude mathématique en fournissant *la* bonne réponse attendue. C'est le professeur qui est garant de la vérité des énoncés qui circulent dans la classe. Étant l'expert en mathématiques, il sait et a le devoir de corriger les erreurs de ses élèves, de leur montrer *la* bonne méthode. Les mathématiques apparaissent alors comme un absolu dont le professeur détient les clefs et dans lequel lui seul peut guider les élèves. Ce faisant, les élèves risquent fort de se retrouver relégués au rang de simples consommateurs du savoir dispensé par le professeur.

En définitive, pour beaucoup d'élèves, les mathématiques ne sont vraies que parce que le prof le dit et pas forcément parce qu'elles répondent de façon convaincante à une question qu'ils se posent. Les mathématiques sont là, on les étudie, on les applique, mais on ne se pose pas la question de leur véracité, de leur légitimité.

Nous voudrions, au contraire, que les élèves puissent douter, se convaincre, s'exprimer, apprendre à débattre pour se former à la pensée mathématique et mieux s'approprier le cours. Nous aimerions aussi que les élèves apprennent à argumenter en justifiant leur position, développent leur esprit critique et soient capables de recul sur les affirmations qu'ils avancent.

Nous espérons progresser vers ces objectifs à travers, entre autres, la pratique de débats au cours de mathématiques. Concrètement, une question d'ordre mathématique est posée aux élèves, qui ont alors le loisir de se former leur propre opinion, puis de la partager et de la défendre face à leurs pairs. Le temps du débat, le professeur se garde bien d'être l'arbitre de la vérité des énoncés, mais devient un garant du cadre de discussion, se retirant autant que possible au niveau du fond du propos pour en laisser une responsabilité maximale aux élèves.

2. Notre travail au GEM

S'inspirant notamment des travaux de l'IREM de Grenoble sur le débat scientifique en classe (voir par exemple Charlot et al., 2015 ; Lecorre, 2015 ; Legrand, 1993 ; Leroux & Lecorre, 2007) et, au-delà, des travaux du groupe ERMEL (1999) et de l'IREM de Lyon (Arsac et al., 1992), plusieurs membres du Groupe d'Enseignement Mathématique (GEM) à Louvain-la-Neuve, dont nous faisons partie, développent et expérimentent des situations de débat autour de questions mathématiques dans des classes du primaire, du secondaire, et en formation d'enseignants. Un recueil de questions de débats découlant de ce travail est à paraître dans un futur plus ou moins proche. Ce travail a déjà donné lieu à quelques publications, par exemple Ben Aïcha (2019 ; 2021), Gilbert (2021) ou Zimmer & Ninove (2022).

3. Plan succin de l'atelier

Dans l'atelier que nous avons animé, nous avons proposé aux participants de vivre un débat autour d'une question pouvant convenir à presque tout âge, du collège à l'université, avant d'effectuer un retour sur le moment partagé et de présenter des échos de nos expérimentations dans les classes de collège et au-delà, avec quelques exemples d'énoncés pouvant faire débat.

II - UN DÉBAT À VIVRE

1. Cadre de l'activité de débat proposée

1.1. Structure prévue du débat

Après l'annonce de l'énoncé du problème, repris ci-dessous, environ deux minutes sont laissées aux participants pour s'approprier la question et y réfléchir en silence.

Cette première phase de réflexion individuelle est suivie d'une phase dite de débat privé (Leroux & Lecorre, 2007) : pendant deux ou trois minutes, les participants peuvent discuter avec leurs voisins directs de leurs ébauches de résolution et de leurs conjectures.

Ensuite, l'animateur du débat procède au relevé des conjectures, en les inscrivant au tableau. À ce stade, il est demandé de ne pas s'exprimer sur la validité des propositions, ni de donner d'arguments pour ou contre. Ceci est particulièrement difficile pour les participants, qui ont tendance à réagir vite. Cette contrainte a pour objectif de laisser à chacun le temps de réfléchir sans à priori sur les propositions des autres.

On sélectionne ensuite les conjectures à débattre : une ou deux qui soient faciles à traiter, et une ou deux plus délicates.

Vient alors la phase dite de débat public, avec le groupe au complet. Pour chaque conjecture sélectionnée, l'animateur procède à un bref vote pour prendre la température de l'audience, proposant de se positionner entre « vrai », « faux » et « autre » (Leroux & Lecorre, 2007 ; Lecorre, 2015). Suite à ce vote, on procède à l'échange des arguments jusqu'à obtention d'un consensus compris et validé par tous. Si besoin, le recours à de nouvelles phases de débat privé ou de recherche individuelle peut être proposé.

Après environ quarante-cinq minutes de débat, nous faisons le point sur les arguments et les démarches. Ce retour pourrait faire partie d'une institutionnalisation plus importante.

1.2. Quelques règles pour le débat

Voici quelques règles pour s'assurer du bon déroulement du débat, règles inspirées librement de Legrand (2017).

- Chacun peut (mais personne ne doit) prendre la parole, mais tout le monde doit participer.
- Chacun s'adresse à l'ensemble du groupe, et non à l'animateur.
    - On s'exprime pour être entendu de tous, en se tournant et regardant le groupe.
    - On annonce sa thèse (« Je pense que ... ») avant de l'argumenter (« Voilà mes raisons... »).
- Chacun est soucieux de connaitre l'avis des autres.
    - On écoute et on regarde celui qui parle.
    - On réagit à ce que les autres disent (avec respect). On peut utiliser des formulations telles que « ce qui m'échappe dans ce que tu dis, c'est… », « je ne suis pas d'accord avec tel argument, telle affirmation... ».
- On (s')interdit les arguments d'autorité (« Je peux vous assurer que... », « parce que c'est comme ça »).
- On peut aller au tableau pour s'expliquer.
- On peut convenir de gestes pour exprimer brièvement son accord, son désaccord...

2. Énoncé du problème

Le plus grand résultat.

J'ai deux nombres en tête, 10 et un autre nombre, que je ne vous donne pas. Si je veux fabriquer le plus grand nombre, quelle opération vaut-il mieux que j'utilise parmi l'addition, la soustraction, la multiplication et la division ? Le premier terme ou facteur du calcul sera 10.

Donnez un ou des « vrai ou faux ? » raisonnables (ils peuvent être faux, mais pas faux au premier coup d'œil). On peut utiliser des formulations et expressions telles que « toujours », « parfois », « en tout cas », « jamais », « si..., alors ... ».

3. Éléments de solution

En réfléchissant au problème, on se rend compte rapidement que « ça dépend du nombre ». La tâche revient alors à la détermination des domaines dans lesquels chaque opération est « la meilleure », c'est-à-dire donne un résultat supérieur aux trois autres. Dans le domaine des négatifs, la soustraction l'emporte, car la multiplication et la division donnent un résultat négatif et l'addition donne un résultat inférieur à 10, alors que la soustraction donne un résultat supérieur à 10. Voilà déjà un premier raisonnement accessible aux élèves.

Si le « deuxième nombre » est positif, la question se complique. S'il est proche de zéro, il est avantageux de diviser, et s'il est suffisamment grand, il vaut mieux multiplier, alors qu'avec 1, il vaut mieux additionner. Comment donner un sens précis à « suffisamment proche de zéro » et « suffisamment grand » ? Une façon de procéder est d'écrire des (in)équations pour déterminer les nombres charnières, où deux opérations donneront le même résultat. Pour départager l'addition de la multiplication, l'équation à résoudre est $10 + x = 10x$, qui a pour solution le nombre $\frac{10}{9}$.

L'équation départageant l'addition de la division est $\frac{10}{x} = 10 + x$. C'est une équation du second degré, dont l'unique solution positive est $-5 + \sqrt{35}$.

Les conclusions que l'on peut tirer de ces observations sont synthétisées dans le graphique présenté à la figure 1.

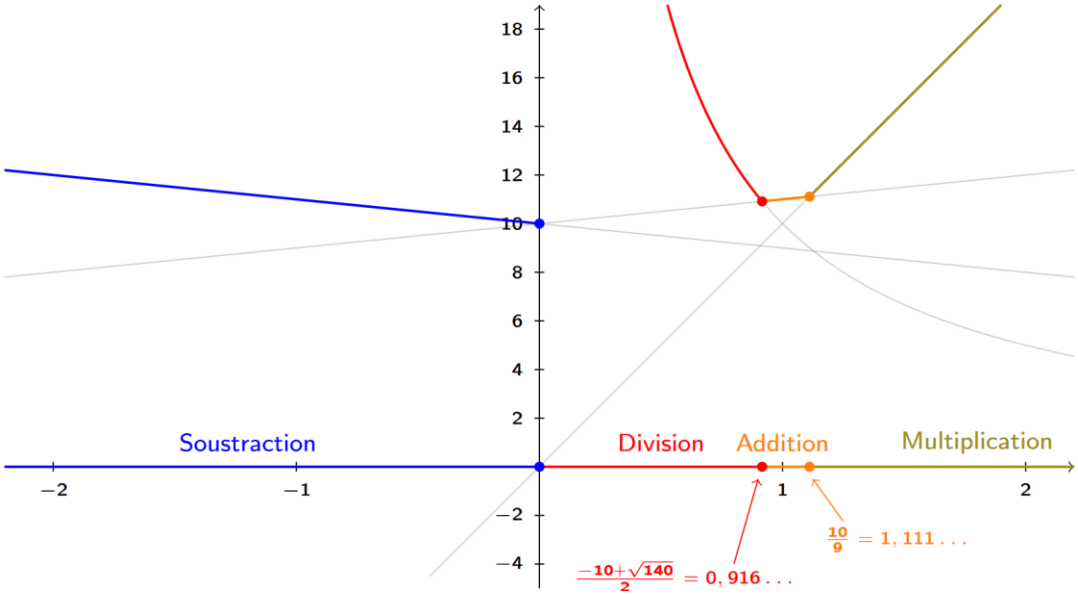


Figure 1. Graphes des fonctions $10 - x$, $\frac{10}{x}$, $10 + x$ et $10x$, représentés dans un repère où l'axe des abscisses est dilaté. En couleur sur l'axe des abscisses, le domaine sur lequel chacune des quatre opérations donne le résultat le plus élevé.

Observons qu'on ne s'attend pas forcément à ce que les élèves, en particulier au collège, usent d'une représentation graphique comme celle présentée ci-dessus. Généralement, le temps de débat est l'occasion de formuler et d'interroger quelques conjectures, mais non de résoudre le problème de fond en comble. La mise en débat du problème peut d'ailleurs tout à fait constituer un prélude à une résolution plus complète, effectuée de façon individuelle ou par petits groupes. C'est d'ailleurs cette dernière approche qui a été explorée lors de nos essais en formation d'enseignants.

4. Quelques conjectures, démarches empruntées et arguments échangés

Le débat a été proposé dans deux groupes. Voici quelques-uns des « Vrai ou faux ? » écrits au tableau dans l'un ou l'autre groupe :

(1) Il faut toujours multiplier.
(2) Il faut soustraire, on aura plus de chance.
(3) Si le deuxième nombre est supérieur à 1, il faut multiplier.
(4) Si le deuxième nombre est 0, il faut diviser.
(5) Si le deuxième nombre est négatif, on peut soustraire.
(6) Si le deuxième nombre est strictement compris entre 0 et 1, il faut diviser.
(7) Ça peut être n'importe quelle opération en choisissant convenablement le deuxième nombre.
(8) Si $x > \frac{5}{4}$, il faut multiplier.

Après le débat proprement dit, nous avons fait le point sur les démarches générales, les arguments mathématiques et les outils mathématiques appliqués. Voici d'abord quelques démarches générales qui ont été empruntées.

Les participants ont parfois éprouvé le besoin d'expliciter le sens de la question et de faire préciser l'une ou l'autre conjecture ambiguë (la (2), la (5) ou la (7)). Dans un des deux ateliers, certains ont proposé d'organiser le débat (« traitons d'abord de cette question », « nous pourrions voir ceci à la fin »). D'autres ont structuré l'argumentation, en cours de débat, ou la réponse (sous forme de droite découpée en intervalles) à la fin.

À certains moments, il a fallu reprendre un argument et s'assurer que rien n'avait été oublié, ou pointer les problèmes qui restaient à résoudre, les affirmations encore à prouver. Des participants ont aussi proposé des variations sur la question de départ.

Citons maintenant les démarches mathématiques appliquées. Les participants ont dû rechercher des conjectures, puis des contre-exemples pour contredire certaines affirmations, faire la distinction entre propositions universelle et existentielle, procéder par élimination pour restreindre les opérations à considérer, comparer les opérations deux par deux.

Certains participants ont témoigné du fait qu'ils avaient d'abord pensé qu'avec un nombre plus grand que 1, ce serait la multiplication qui serait gagnante (affirmation (1)) car « c'est à partir du facteur 1 que la multiplication fait grandir ».

L'affirmation (8) a été l'occasion de faire la distinction entre une conjecture non générale (qui ne donne pas la solution complète à la question), une conjecture non intéressante et une conjecture fausse.

À propos de l'affirmation (2), nous avons évoqué les probabilités et la difficulté de comparer des ensembles infinis.

Plusieurs participants ont évoqué le principe de continuité : si l'addition gagne pour le nombre 1, si la multiplication gagne pour de grands nombres, il doit bien y avoir un nombre pour lequel les deux opérations donnent le même résultat ; où se situe la limite ?

Un participant a pensé qu'il pouvait résoudre un des problèmes par analogie : quand on aura résolu le problème de la limite entre les domaines de l'addition et de la multiplication, on aura résolu celui de la limite entre la division et l'addition. Il s'est avéré que ce n'était pas le cas. Il a alors lu deux citations de Grothendieck, que nous reprenons ci-dessous.

> *Quand je suis curieux d'une chose, mathématique ou autre, je l'interroge. Je l'interroge, sans me soucier si ma question est peut-être stupide ou si elle va paraître telle, sans qu'elle soit à tout prix mûrement pesée. Souvent la question prend la forme d'une affirmation – une affirmation qui, en vérité, est un coup de sonde. J'y crois plus ou moins, à mon affirmation, ça dépend bien sûr du point où j'en suis dans la compréhension des choses que je suis en train de regarder. Souvent, surtout au début d'une recherche, l'affirmation est carrément fausse – encore fallait-il la faire pour pouvoir s'en convaincre. Souvent, il suffisait de l'écrire pour que ça saute aux yeux que c'est faux, alors qu'avant de l'écrire il y avait un flou, comme un malaise, au lieu de cette évidence. Ça permet maintenant de revenir à la charge avec cette ignorance en moins, avec une question-affirmation peut-être un peu moins "à côté de la plaque" (Grothendieck, 2021, p. 200).*

> *Mais il arrive aussi que […] cette image [de la situation] est entachée d'une erreur de taille, de nature à la fausser profondément. Le travail, parfois laborieux, qui conduit au dépistage d'une telle idée fausse […] est souvent marqué par une tension croissante, au fur et à mesure qu'on approche du nœud de la contradiction, qui de vague d'abord se fait de plus en plus criante – jusqu'au moment où enfin elle éclate, avec la découverte de l'erreur et l'écroulement d'une certaine vision des choses, survenant comme un soulagement immense, comme une libération. La découverte de l'erreur est un des moments cruciaux, un moment créateur entre tous, dans tout travail de découverte, qu'il s'agisse d'un travail mathématique, ou d'un travail de découverte de soi (Grothendieck, 2021, p. 200-201).*

Les preuves fournies ont été soit générales (par exemple pour la soustraction), soit expliquées sur un exemple générique.

Enfin, voici une liste d'outils mathématiques utilisés :

- équations, inéquations, du premier ou du second degré,
- sens des opérations et règles les régissant,
- limite d'une fonction en un point.

5. Échos d'expérimentations dans les classes

5.1. Au collège

Le problème a été proposé à plusieurs reprises dans des classes de deuxième et troisième secondaire en Belgique (équivalents respectifs de la quatrième et de la troisième au collège), dans une version réduite aux opérations d'addition, de soustraction et de multiplication. Les élèves n'avaient en effet pas à leur disposition la résolution d'équations du second degré et le problème est déjà suffisamment riche avec ces trois opérations seulement.

L'énoncé n'est pas toujours clairement saisi de prime abord. Parfois, le professeur doit le clarifier en spécifiant bien que l'on compare le résultat des opérations en conservant le même deuxième nombre une fois qu'on l'a choisi. Sans cette contrainte, la question n'est plus si intéressante.

Les élèves envisagent d'abord seulement les nombres naturels et leurs premières conjectures naïves sont de l'ordre de « Forcément, multiplier c'est plus grand » ou « Le moins, il retire. Du coup, c'est pas le meilleur. ». Ces conjectures sont mises à l'épreuve des contre-exemples. Généralement, la modélisation algébrique ne vient pas à l'esprit des élèves, mais le débat est l'occasion d'une grande chasse aux contre-exemples.

Rapidement, ils en viennent à s'intéresser aux nombres négatifs et à démontrer que, dans ce domaine, c'est la soustraction qui gagne. Puis, ils envisagent les nombres « à virgule ». Ce n'est pas forcément la multiplication qui donne le plus grand résultat, puisque par exemple, $10 \cdot 0{,}5 = 5$, alors que $10 + 0{,}5 = 10{,}5$. Des élèves proposent des conjectures comme « Si le deuxième nombre est plus grand que 1,2, c'est la multiplication qui gagne ». Certaines classes sont allées d'elles-mêmes jusqu'à la détermination du point de bascule 1,1111… mais, plutôt que de l'obtenir via la résolution d'une équation, les élèves y arrivent par une succession d'essais-erreurs et d'encadrements.

5.2. En formation initiale des enseignants

Voici quelques moments de débat dans une classe d'étudiants AESI[2] en mathématiques. Ils viennent de commencer leurs études et ne sont pas habitués à débattre. Le niveau de connaissance des mathématiques varie grandement d'un étudiant à l'autre[3].

1. Où il est question de conditions nécessaire et suffisante, d'implication et de réciproque.

(Vrai ou faux ?) « Si n = 1, l'addition gagne. »

Esme. Le +, il peut gagner, oui, mais pas forcément quand $n = 1$. Je dis pas que c'est faux, mais je dis pas que c'est vrai non plus.

Achille. On a mis la condition « $n = 1$ » au début : si « ça », alors l'addition gagne. Ça, c'est vrai.

On retrouve ici le problème soulevé par la conjecture (8) au cours de l'atelier : la phrase est vraie, mais ne dit pas toute la vérité sur la question, ce qui peut paraître perturbant pour certains. On observe également une confusion entre condition nécessaire et suffisante : la première phrase est un contre-argument pour la phrase « L'addition gagne seulement si $n = 1$ », l'implication réciproque de l'affirmation débattue.

2. Un argument de continuité.

(Vrai ou faux ?) « Si le deuxième nombre est > 1, la multiplication gagne. »

Achille. Si $n > 1$, l'addition ne va pas gagner, ça va être la multiplication.

Brahim. Si $n = 1{,}00001$, l'addition sera encore plus forte que la multiplication :

[2] Agrégé de l'Enseignement Secondaire Inférieur, c'est-à-dire des étudiants qui se destinent à l'enseignement des mathématiques au collège.

[3] Il n'y a pas de concours d'entrée.

$10 \cdot 1{,}00001 = 10{,}0001$; $10 + 1{,}00001 = 11{,}00001$.

On peut deviner ici un certain argument de continuité, non exprimé : si pour $n = 1$, l'addition gagne, ce sera aussi le cas pour certains nombres proches de 1.

3. Sur la précision des énoncés et les quantificateurs cachés.

(Vrai ou faux ?) « Si le deuxième nombre est > 1, la multiplication gagne. »

Achille. Je vote « Autre » car ça peut être faux ou vrai selon les nombres :
Si $n = 1{,}00001$, alors l'addition gagne.
Si $n = 1{,}5$, alors l'addition donne 11,5 et la multiplication donne 15.

Bouchra. Donc la multiplication ne gagne pas toujours, donc c'est faux.

Adèle. Dans la conjecture, on n'a pas écrit « toujours ».

Camelia. Je pense comme Bouchra : « la multiplication gagne » induit que « la multiplication gagne dans tous les cas ».

Bouchra. En fait, on devrait dire « la multiplication gagne toujours » ou « la multiplication peut gagner ». [Alors, on pourrait se mettre d'accord.]

Ce type de précision de quantificateurs implicites est assez récurrente dans nos observations de débats en formation des enseignants (voir par exemple Zimmer, 2023). Comme l'observait déjà Durand-Guerrier (1999), la quantification universelle d'énoncés de type « si…, alors… » n'est pas nécessairement évidente pour les élèves et gagne souvent à être explicitée.

6. Extension du problème

Le problème présenté dans ces lignes admet une formulation plus générale, qui peut être adaptée pour des élèves plus âgés, ou si l'on veut prolonger la discussion.

J'ai deux nombres en tête, que je ne vous donne pas. Si je veux fabriquer le plus grand nombre, quelle opération vaut-il mieux que j'utilise parmi l'addition, la soustraction, la multiplication et la division ?

La discussion comprend alors une multitude de cas, que l'on peut représenter graphiquement dans le plan. À noter que, si le problème initial pouvait être résolu en comparant des fonctions de **R** dans **R**, ici il faudrait raisonner à partir de fonctions de deux variables, ce qui corse nettement la difficulté. Il y a alors peu d'espoir de venir à bout du problème dans le courant du débat, mais celui-ci peut être prolongé par une résolution individuelle ou par groupes.

III - D'AUTRES DÉBATS RACONTÉS, VÉCUS AU COLLÈGE

1. Huit divisé par zéro

Combien vaut 8 : 0 ?

Ce sujet de débat se présente généralement spontanément au collège, avec éventuellement un autre nombre que 8. Si cette question survient, au fil d'un cours, plutôt que d'asséner que ça n'a pas de sens ou d'expliquer lui-même pourquoi, l'enseignant peut saisir l'opportunité de renvoyer la balle aux élèves et de leur proposer d'en débattre. C'est une question simple, que tous les élèves peuvent s'approprier et, généralement, la classe n'est pas d'accord à priori. Plusieurs réponses sont généralement proposées par les élèves, par exemple « impossible », « 0 », « 8 » ou « l'infini ».

C'est l'occasion pour les élèves de revenir au sens des opérations : se demander quel nombre est égal au résultat de la division de 8 par 0, c'est se demander *par combien doit-on multiplier 0 pour obtenir 8,* ou *quel est le nombre tel qu'en le multipliant par 0, on trouve 8* ?

Voici quelques arguments des élèves. Certains pensent que 8 : 0 = 8.

- Mais « ça ne peut pas être la même réponse que 8 : 1 ».
- Pourtant, « 8 : 2 a bien la même réponse que $8 \times \frac{1}{2}$ », non ?
- Oui, mais « diviser par deux ou multiplier par un demi, c'est la même chose, alors que diviser par un ou zéro non ».

Le groupe est convaincu et cette solution est rejetée.

Dans une autre classe, un groupe défend que 8 : 0 donne l'infini.

- En effet, « 8 : 2 = 4, parce que 4, il rentre 2 fois dans 8. Du coup, 8 : 0 = l'infini, parce que 0 rentre une infinité de fois dans 8 ».
- Oui, mais « si tu prends 0 une infinité de fois, tu n'obtiens pas 8 », donc ce raisonnement ne tient pas.

Finalement, c'est le sens de l'opérateur de division, inverse de celui de la multiplication, qui permet souvent aux élèves de trancher.

2. Combien de nombres entre $\frac{6}{11}$ et $\frac{7}{10}$?

Combien de nombres y a-t-il entre $\frac{6}{11}$ et $\frac{7}{10}$? (Adapté de Detaille, 2017)

Ce débat est un débat préparé et proposé aux élèves par l'enseignant. Quelques réponses proposées par des élèves de treize ans au collège :

- Il n'y en a pas…
- Il y en a un : c'est 0,6.
- Il y en a quinze, on peut les compter : 0,55, 0,56, 0,57, …, 0,69.
- Il y en a seize, car $\frac{6}{11} = \frac{60}{110}$ et $\frac{7}{10} = \frac{77}{110}$.
- Il y en a une infinité !

Des réponses plus saugrenues peuvent survenir : par exemple un élève dit qu'il y en a 0,16, parce que $\frac{7}{10} - \frac{6}{11} \cong 0{,}16$.

La comparaison de fractions n'est pas forcément une mince affaire dès lors que les deux dénominateurs sont différents. Pour un élève, « on ne peut pas comparer deux nombres si leurs dénominateurs ne sont pas les mêmes ». L'enseignant demande si on en est bien sûr et un autre élève propose de trouver un contre-exemple à cet énoncé. Après quelque temps de recherche, on arrive à voir que, par exemple, $\frac{1}{2}$ et $\frac{4}{3}$ n'ont pas le même dénominateur, mais l'une des fractions est inférieure à 1 tandis que l'autre lui est supérieure. L'une est donc forcément plus petite.

Les élèves peuvent éprouver le besoin d'écrire les deux nombres en écriture décimale pour les comparer et facilement trouver des nombres intermédiaires. Ce peut être l'occasion de revoir avec eux l'algorithme de la division écrite, en particulier dans le cas où la division ne s'arrête pas. Ceci peut révéler des obstacles chez les élèves, liés à la présence de l'infini. Par exemple, pour une élève, « $\frac{6}{11} = 0{,}54545454\ldots$ continue à l'infini, donc comment pourrait-il y avoir un nombre plus grand ? ». C'est l'occasion de se ramener à des exemples plus familiers déjà rencontrés en classe, comme $\frac{1}{3} = 0{,}3333\ldots$, pour lequel on peut très bien imaginer des nombres supérieurs.

IV - CONCLUSION

Le débat vécu, ainsi que beaucoup d'autres, sont une occasion d'apprendre à conjecturer, c'est-à-dire :

- à penser les conjectures, à envisager des conjectures variées ;
- à apprendre à les exprimer correctement, à se rendre compte qu'un mot peut changer le sens ;
- à faire préciser la conjecture d'autres élèves ;
- à faire évoluer les conjectures ;
- à élargir le domaine envisagé des nombres ;
- à remettre en question quelques certitudes.

On y apprend aussi des éléments de logique, notamment :

- à utiliser des implications ;
- à distinguer « il faut que » de « il suffit que », à distinguer une implication et sa réciproque ;
- à préciser « toujours », « jamais », « parfois » et à distinguer les propositions universelles et existentielles ;
- à comprendre qu'un contre-exemple suffit à contredire ; à fabriquer des contre-exemples ;
- à comprendre que le fait de ne pas arriver à trouver de contre-exemple ne suffit pas à démontrer une proposition universelle.

Les débats, en arithmétique ou dans d'autres domaines, sont l'occasion d'éprouver la nécessité de démontrer, d'apporter des arguments généraux.

Pour l'enseignant, ils permettent aussi de se rendre compte des lacunes des élèves (ici, de faire le point sur les opérations) et de se rendre compte de la difficulté des élèves à transférer les connaissances (ici, les équations) et leur en donner l'occasion.

Alors raisonner en arithmétique, est-ce incongru ? Non.

V - BIBLIOGRAPHIE

Arsac, G. Chapiron, G. Colonna, A., Germain, G. Guichard, Y. & Mante, M. (1992). *Initiation au raisonnement déductif au collège*. Lyon : Presses universitaires de Lyon.

Ben Aïcha, H. (2019). Des élèves dignes de grands mathématiciens !, *Traces de changements*, 241.

Ben Aïcha, H. (2021). Argumenter et débattre, *Au fil des maths*, *541*, 45-49.

Ben Aïcha, H. & Gilbert, T. (2019). Quatre débats pour éveiller l'esprit critique, https://changement-egalite.be/Quatre-debats-pour-eveiller-l.

Charlot, G. Lecorre, T. Legrand, M. Leroux, A. & Di Martino, H. (2015). Le débat scientifique en classe : une démarche d'investigation collective pour une culture scientifique commune. Dans Theis, L. (ed.) *Pluralités culturelles et universalité des mathématiques : enjeux et perspectives pour leur enseignement et leur apprentissage – Actes du colloque EMF2015* (pp. 847-860). Alger : Société Mathématique d'Algérie.

Charrière, G. (1995). Algèbre mode d'emploi. Le Mont-sur-Lausanne : LEP – Loisir et Pédagogie SA.

Detaille, J. (2017). Entre deux nombres. Dans Gilbert, T., Ninove, L. (dir.) et le Groupe d'Enseignement Mathématique, *Le plaisir de chercher en mathématiques, De la maternelle au supérieur : 40 problèmes* (pp. 23-25). Louvain-la-Neuve : Presses Universitaires de Louvain.

Durand-Guerrier, V. (1999). L'élève, le professeur et le labyrinthe. *Petit x*, *50*, 57–79.

ERMEL (1999). *Vrai ? Faux ? . . . On en débat ! De l'argumentation vers la preuve en mathématiques au cycle 3*. Paris : Institut national de recherche pédagogique.

Gilbert, T. (2021). Apprendre à débattre et à animer un débat mathématique, *Au fil des maths*, *542*.

Grothendieck, A. (2021). *Récoltes et semailles, I*. Paris : Gallimard.

Lecorre, T. (2015). Définir : une nécessité à construire. Le cas de la définition de la limite d'une fonction, *Repères-IREM*, *100*, 51-64.

Legrand, M. (1993). Débat scientifique en cours de mathématiques et spécificité de l'analyse, *Repères-IREM, 10*, 123-149.

Legrand, M. (2017). Désir de démocratie et d'humanisme authentiques et nécessité d'opérer une révolution dans notre façon de concevoir le savoir et son partage à l'école, La construction collective d'un sens profond, Forum de l'Education Sfax.

Leroux, L. & Lecorre, T. (2007). Le « Débat scientifique » en classe. Comment donner à l'élève une responsabilité scientifique réelle en cours de mathématiques ?, *APMEP – PLOT*, *19*, 2-15.

Weil, A. (1991). Entretien avec Michel Demazure et Martin Andler, *Gazette des mathématiciens*, *50*, 3-10.

Zimmer, D. & Ninove, L. (2022). Un problème de géométrie pour conjecturer et débattre, *Repères-IREM*, *129*, 62-84.

Zimmer, D. (2023). Narration et analyse, sous le prisme de la logique, d'un débat mathématique vécu en formation d'enseignants. À paraître dans le vol. 3 de la revue *Nexus*.

INITIATION AU BOULIER CHINOIS

POURTIER Jean-Charles
Enseignant en lycée
Retraité
jc.pourtier@laposte.net

Résumé
L'atelier a consisté en une initiation à l'utilisation du boulier chinois.
Le but est de mettre en place la numération de position, puis effectuer les quatre opérations élémentaires.
Pour les multiplications et divisions, ne seront présentées que des opérations dans lesquelles :
- un des multiplicateurs a aux plus deux chiffres
- le diviseur a aussi, aux plus deux chiffres

I - UTILISATION

Le boulier chinois est utilisable à tous les niveaux de l'école primaire :

- pour rendre tangible les nombres
- pour la mise en place de la numération de position
- pour l'apprentissage des opérations élémentaires : addition et soustraction
- pour la mise en place de la multiplication à partir de l'addition
- pour développer les capacités de calcul
- il est aussi un bon support pour le calcul mental
- il peut être utile pour l'apprentissage des tables de multiplications

Conclusion : son utilisation n'a que des avantages pédagogiques.

II - L'ATELIER

Les réactions des participants à l'atelier sont identiques aux présentations que j'ai pu faire à des élèves en seconde :

- à la première étape, nous avons positionné les nombres. L'attitude des participants reflétaient la trop grande simplicité. Pour les secondes, cette étape est plus primordiale, elle permet une familiarisation avec l'outil et une prise en main (en annexe les exercices et le ressenti des élèves) ;

- à la deuxième étape, nous sommes passés à l'addition ;

Nous n'avons utilisé, dans un premier temps, que la partie basse du boulier. Pour l'atelier, l'attitude face aux exercices fut de reconnaître une grande simplicité. Pour les élèves de seconde, aussi (voir exercices et ressenti des élèves en annexe.

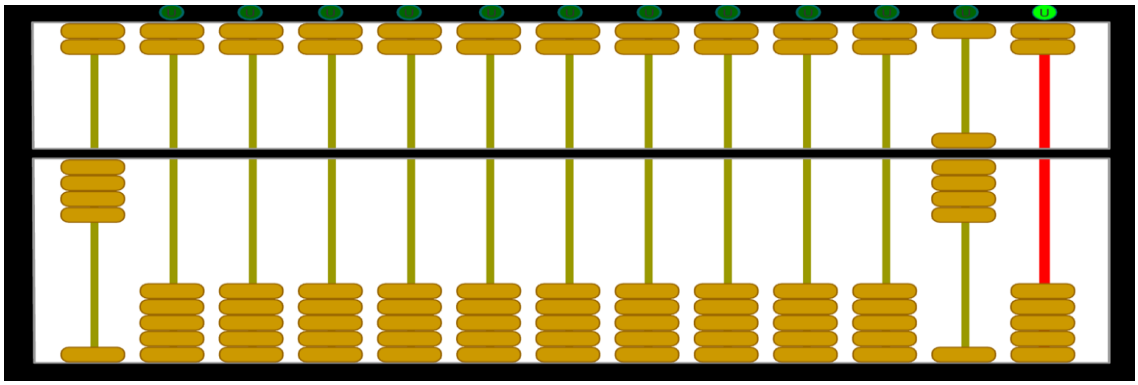
Nous avons utilisé dans un deuxième temps tout le boulier. Les participants à l'atelier n'ont pas modifié leur attitude mais les secondes ont commencé à appréhender la difficulté (voir annexe les exercices et le ressenti des élèves).

- à la troisième étape, nous sommes passés à la soustraction en utilisant tout le tableau.

Les participants à l'atelier se sont rapidement adaptés. Les élèves sont arrivés en fin de séance. Une certaine fatigue s'est fait sentir chez ces jeunes. Un seul a pu terminer sa feuille et me la rendre.

Remarque : avec une classe en une heure, il n'est pas possible d'aller au-delà de la soustraction quelques soient les capacités des élèves.

- L'atelier s'est poursuivi avec la multiplication dont un des multiplicateurs n'a qu'un chiffre.

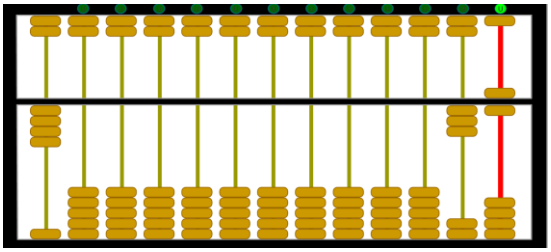


Pour la multiplication à un chiffre (ici 4), on laisse la colonne des unités libres.

Remarque pratique : une fois les 2 multiplicateurs écrits, le réflexe est de poser et de dire 4 fois 9 mais pour s'adapter à une manipulation plus complexe (2 chiffres pour le multiplicateur placé à gauche du boulier), il faut poser 9 fois 4.

Donc on a : unités x unités donnent des unités

ex : 9 unités x 4 unités = 36 unités

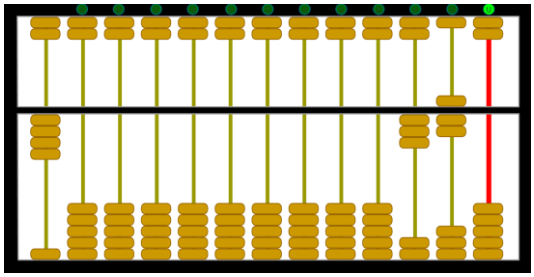
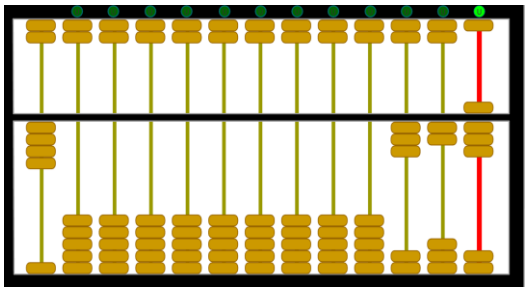
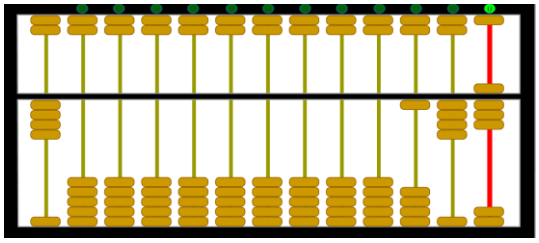
	Le 9 disparaît car il est utilisé alors on écrit 36.

- L'atelier s'est fini par la multiplication avec 2 chiffres à droite. La simplicité d'utilisation en est le principal écueil, car dans un premier temps, on perd ses repères de position pour écrire le nombre obtenu par la table de multiplication.

Il faut manipuler les tables de multiplication et d'addition.

Pour chaque étape, il faut décaler l'unité vers la gauche.

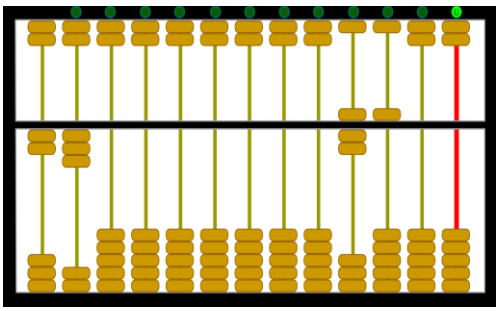
Application : 4 x 37

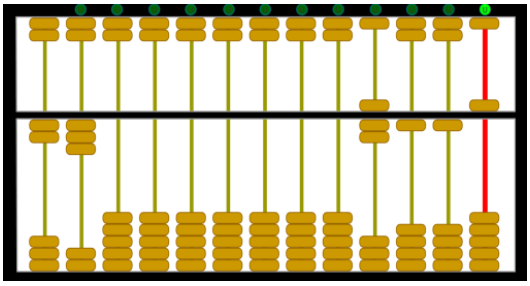
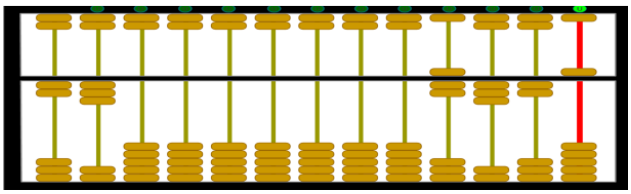
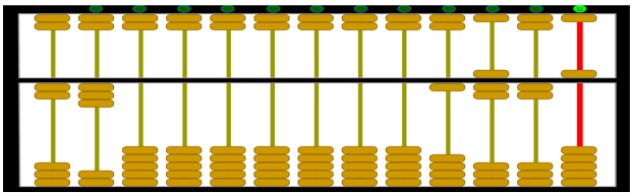
	- pour le positionnement, on utilise l'étape précédente.
	- pour le calcul, tout d'abord : on calcule 7 fois 4, on supprime le 7 car utilisé, on écrit le résultat, soit 28.
	- puis on calcule 3 fois 4, soit 12 on garde 8, on supprime le 3 car utilisé, on ajoute 12+2 = 14, d'où 148 ci-dessous.

Remarque : la méthode (lire la multiplication de droite à gauche) 7 fois 4 puis 3 fois 4 prend ici tout son sens

À vous de vous entraîner !

Complément : multiplication avec 2 chiffres à gauche

Présentation : S'il y a 2 chiffres à gauche, on laisse les 2 dernières colonnes libres à droite quel que soit le chiffre. Ci-contre, présentation 23 x 75. 1ère étape : 5 fois 23 2ième étape : 7 fois 23 en dizaines	

1ère étape : 5 fois 23 donc on a 115 - on calcule 5 x3 - on écrit 15 et on oublie 5 - on calcule 5 x 2 = 10 - on ajoute 10 à 1 d'où 11 - on supprime le multiplicateur 5 car utilisé - On écrit 11 d'où 115 - le 7 n'a pas été utilisé	
2ième étape : 7 fois 23 en dizaines - 5 est fixe - on calcule 7x3 = 21 - on ajoute 21 à 11 d'où 32 - 25 reste fixe : on calcule 7 x2 = 14 7 est supprimé car utilisé d'où 14 + 3 = 17 (centaines)	
Résultat : 1725	

Quant à la division, je l'ai ajoutée dans les documents joints en Annexe.

Pour finir, j'ai rapidement présenté un mode de notation des nombres avec les doigts jusqu'au 17ème siècle, malgré l'apparition de la numération de position transmise par les mathématiques arabes dès le Moyen-Age.

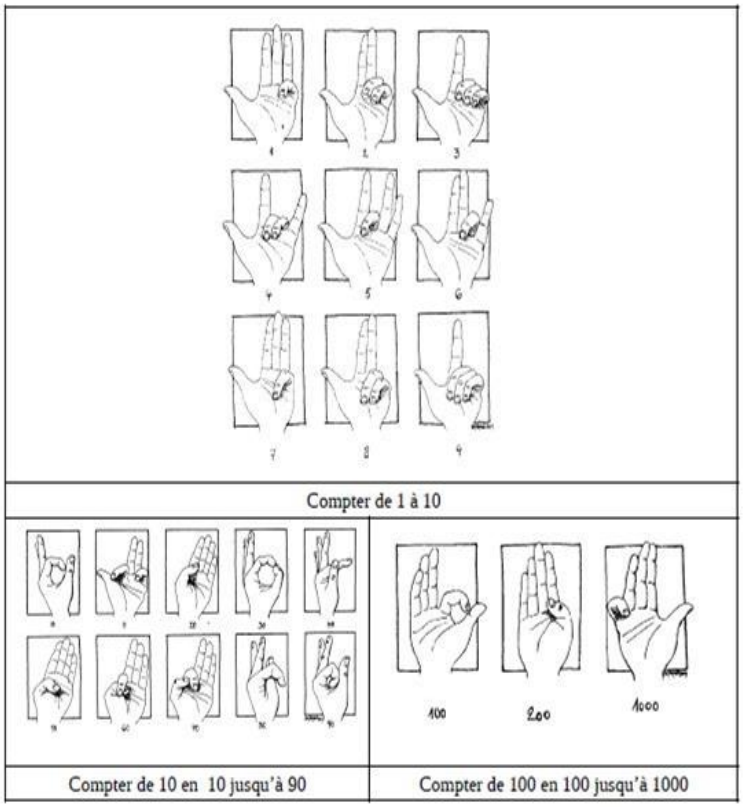


Figure 1 :

« Sur les doigts jusqu'à 9999 » (Jérôme Gavin, Alain Schärlig) ; Presses polytechniques et universitaires Romandes

III - REMARQUES

Je mets en annexe le matériel utilisé durant l'atelier. (Paragraphe V)

J'ai essayé d'être le plus pratique possible.

Nous allons le mettre en pratique avec Jean-Marc Orozco, professeur des écoles à l'école primaire de Cazères-sur-l'Adour.

Des fiches ont été préparées et seront expérimentées.

Nous les mettrons à votre disposition sur simple demande.

Si vous souhaitez des renseignements ou souhaiter une aide, vous pouvez me contacter :

Pourtier Jean-Charles : 06 77 28 11 27 ou jc.pourtier@laposte.net

IV - BIBLIOGRAPHIE ET SITOGRAPHIE

Ferron, J-C. (1987), Le guide pratique du boulier chinois, Editions Sand and Tchou)

GAVIN, J., SCHÄRLIG, A. (2014), Sur les doigts jusqu'à 9999, Presses polytechniques et universitaires romandes, ISBN : 978-2-88915-090-8

Site : https://www.univ-brest.fr/irem/menu/Ressources/Boulier-chinois-virtuel/

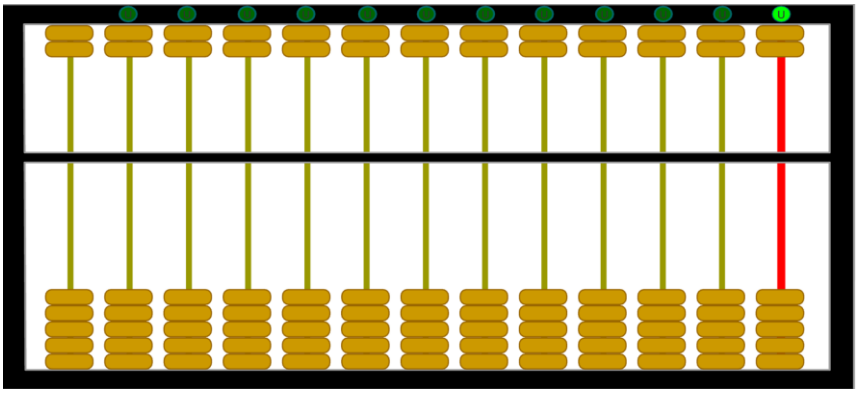
Renseignements complémentaires :

Vous pouvez me contacter sur : jc.pourtier@laposte.net

V - ANNEXE 1

Position des nombres sur le boulier

Chaque boule vaut 5



HAUT

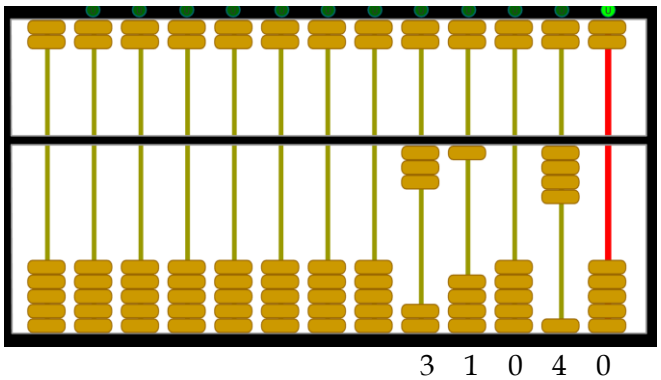
Chaque boule vaut 1

BAS

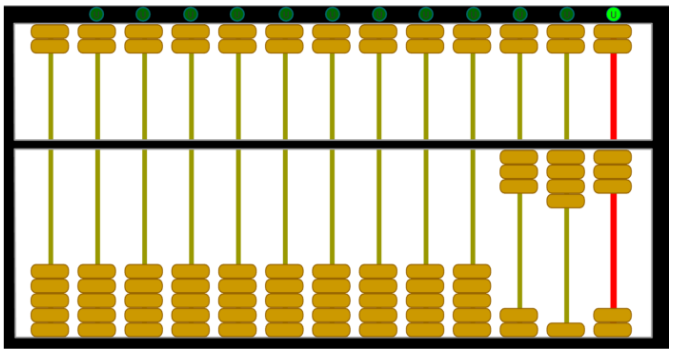
nombre : 0

Exercice 1 : placer les nombres dont les chiffres ne dépassent pas 4.

Exemples :2 ; 3 ; 12 ; 14 ; 20 ; 24 ; 30 ; 40 ; 43 ; 100 ; 140 ; 244 ; 341 ; 1000 ; 1030 ; 204301 ; 123000 ; 100040 etc.



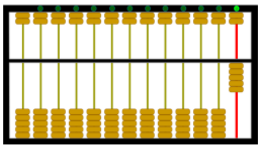
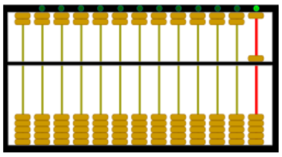
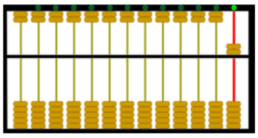
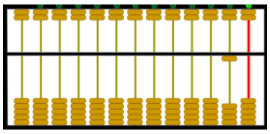
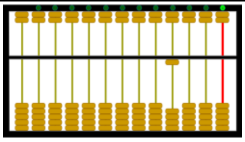
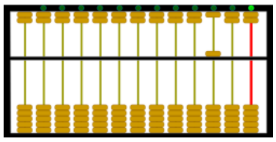
3 1 0 4 0



3 4 3

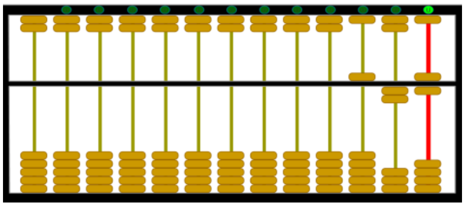
Exercice 2 : placer les nombres « qui utilisent 5 »

Remarques :

Modèle	Notation utilisée	Notation utilisée	Modèle
	=5x1 se lit 5 boules unités du bas Valeur : 5	=1x5 se lit une boule du haut dans la colonne des unités : Valeur : 5	
	=2x5 se lit 2 boules du haut dans la colonne des unités Valeur : 10	=1x10 se lit une boule du bas dans la colonne des dizaines Valeur : 10	
	=1x1000 se lit 1 boule du bas dans la colonne des milliers Valeur : 1000	=1x500 se lit une boule du haut dans la colonne des centaines Valeur : 500	

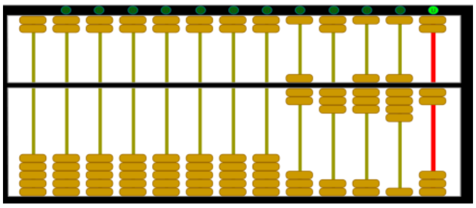
Exemples : 5 ; 6 ; 7 ; 9 ; 10 ; 15 ; 17 ; 19 ; 26 ; 28 ; 29 ; 35 ; 47 ; 150 ; 160 ; 206 ; 3205 ; 3005470…

Exemple :



5 2 6

Exemple :



7 3 8 9 2

Impression et intérêt

Comment avez trouvé cette manipulation ?	Plutôt simple et interessante
Quel intérêt y avez vous trouvé ?	découvrir un moyen ludique afin de calculer en s'amusant.
Avez vous rencontrer des difficultés rencontrées ?	non c'était bien expliqué
Comment abordez vous les nombres après cette manipulation ?	ça n'a pas réellement changer quand on débute.

Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous

Il faut continuer de montrer ça aux élèves c'est interessent à faire.

Impression et intérêt

Comment avez trouvé cette manipulation ?	Passionante.
Quel intérêt y avez vous trouvé ?	Intéressant pour la culture générale et la Réflexion.
Avez vous rencontrer des difficultés rencontrées ?	non, merci.
Comment abordez vous les nombres après cette manipulation ?	d'un nouvel angle.

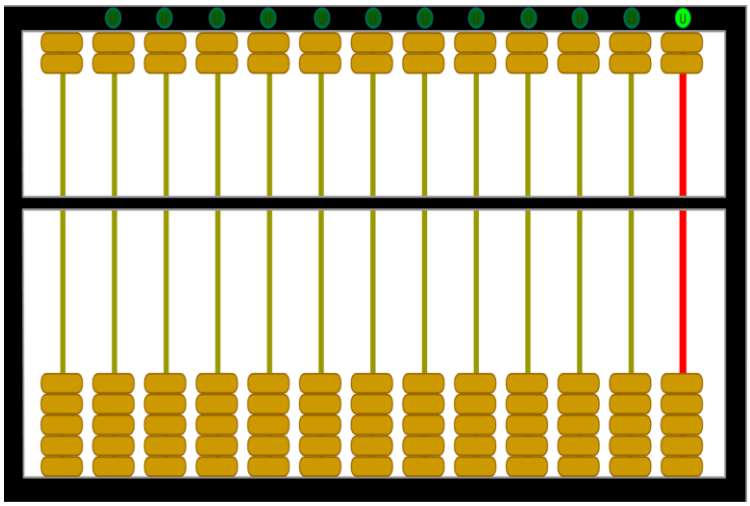
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous

Selon moi, ce travail mélange presque le travail et le loisir car il permet d'aborder de façon ludique les mathématiques et de voir qu'avec cette logique, les nombres peuvent être vus de différentes manières. Je n'ai aucune remarque négative, c'est très interessant.

Addition simple

On utilise que la partie basse du boulier

On soustrait



On ajoute

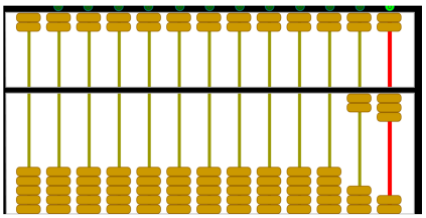
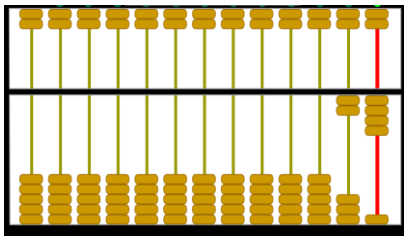
On soustrait

On ajoute

Donc cinq boules du bas peuvent être remplacées par une boule du haut

(Notation : 5 fois 1 en bas =1 fois 5 en haut)

Deux boules du haut peuvent être remplacées par une boule du bas à sa droite (dizaine supérieure)

Exemple : 23 +21 On écrit 23	
puis on ajoute 1 à 3 résultat intermédiaire : 24	

ADDITION : résultat sans modification

Somme simple et directe			
2+1		2+5	
2+2		2+6	
3+1		2+7	
3+5		8+1	
3+6		5+4	
1+1		12+26	
2+2		71+118	

Changement d'écriture utilisation des boules du haut :
5*1 =1*5

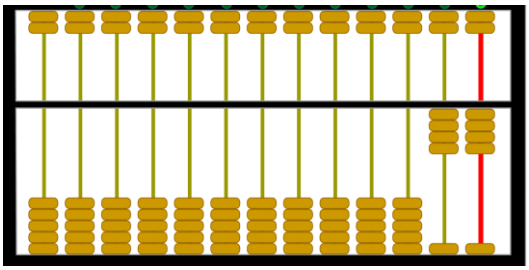
Somme simple et directe			
2+3		1+4	
4+1		3+2	
3+3		2+2+2	
4+4		3+3+3	

puis on ajoute 2 à 2

Impression et intérêt

Comment avez trouvé cette manipulation ?	c'est la suite logique de la manipulation précédente elle est simple et logique.
Quel intérêt y avez vous trouvé ?	elle permet de poursuivre notre apprentissage du boulier en assimilant la notion d'addition.
Cela vous a-t-il donné envie de continuer à faire des additions ?	oui, malgré le fait que ces calculs étaient faisables de tête, calculer au boulier est plus amusant et apporte une nouvelle logique
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous	
Très bien, on pratique la résolution d'addition au boulier et donne différemment.	

Résultat final : 44



Impression et intérêt

Comment avez trouvé cette manipulation ?	Cette manipulation est aussi interressante que la première.
Quel intérêt y avez vous trouvé ?	C'est plus amusant de faire des additions.
Cela vous a-t-il donné envie de continuer à faire des additions ?	Oui.
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous	

Impression et intérêt

Comment avez trouvé cette manipulation ?	Toujours instructive et c'est agréable d'apprendre des techniques que l'on connaissait pas.
Quel intérêt y avez vous trouvé ?	Instructif
Cela vous a-t-il donné envie de continuer à faire des additions ?	Non même si j'ai aimé le faire cette heure-ci.
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous	
Merci	

Addition utilisant tout le boulier

ADDITION : Changement d'écriture utilisation de la dizaine
4 = 5-1; 3 = 5-2 ; 2 = 5-3 ; 1 = 5-4

Somme simple et directe			
4+6		5+5	
3+7		2+8	
1+9		9+1	
5+5		4+4+4	
6+6		5+5+5	
7+7		6+6+6	
8+8		7+7+7	
9+9		8+8+8	
10+10		9+9+9	
11+11		11+11+11	
12+12		12+12+12	
13+13		13+13+13	
14+14		14+14+14	
15+15		17+17+17	
4+4		43+42	
4+3		54+42	
4+2		13+74	
3+3		40+24	
3+4		8204+473	
24+13		9003+374	
24+22		302+450	
14+22		1024+1102	

Impression et intérêt

Avez trouvé cette étape plus difficile manipulation ?	Oui manipuler les chiffres est de plus en plus difficile.
Avez vous trouvé la difficulté motivante ?	Ça nous motive à dépasser nos limites.
Cela vous a-t-il donné envie de continuer à voir la soustraction ?	Oui, on veut connaître toutes les méthodes de calculs avec le boulier chinois.
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous	

Impression et intérêt

Avez trouvé cette étape plus difficile manipulation ?	L'étape était plus intéressante
Avez vous trouvé la difficulté motivante ?	La difficulté m'a donnée envie de comprendre
Cela vous a-t-il donné envie de continuer à voir la soustraction ?	Oui mais j'ai envie de voir la multiplication
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous	

Impression et intérêt

Avez trouvé cette étape plus difficile manipulation ?	Oui suivant à droite
Avez vous trouvé la difficulté motivante ?	oui, car on a l'impression que tout est calculable, il faut juste faire l'effort
Cela vous a-t-il donné envie de continuer à voir la soustraction ?	oui, j'ai hâte d'aborder une nouvelle notion
Si vous avez d'autres remarques sur ce travail, positives ou négatives vous pouvez les écrire ci dessous	
c'était très bien, hâte de continuer	

Soustraction

Comme cela est dit en mathématique, la soustraction fonctionne comme l'addition
Dans les cas délicats ne demandent qu'une habitude de manipulation :

Exemple : 100 – 27

SOUSTRACTION :

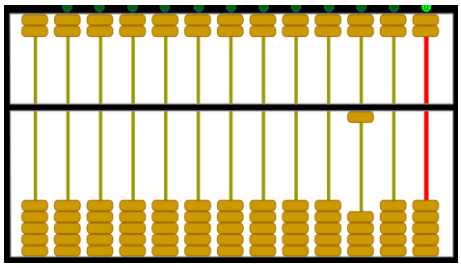
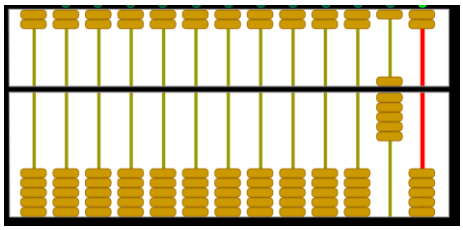
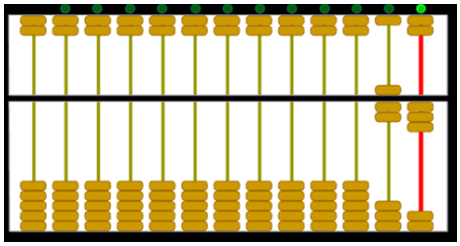
résultat sans modification

2-1		3-1	
3-2		4-2	
4-1		4-3	
24-12		32-21	
34-23		47-32	
297-156		348-247	
4867-2762		8246-6135	
3537-3532		9847-3725	
4862-3861		134249-23246	
4282-2222		44682-43562	

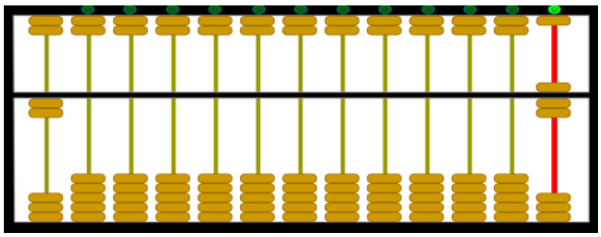
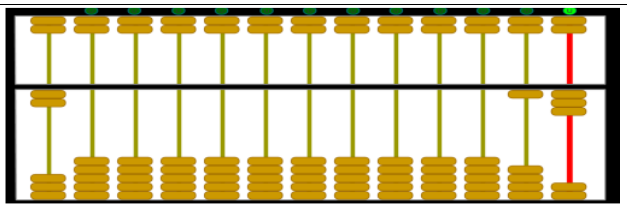
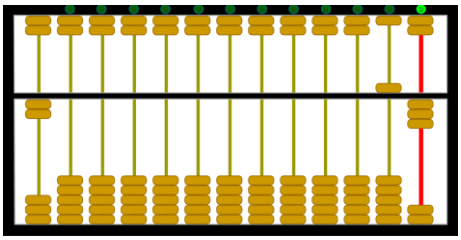
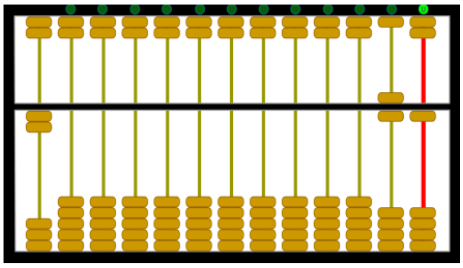
résultat avec modification :

-9 =-10+1 ;-8=-10+2 ;-7 = -10+3 ;-6 =-10+4
- 4 =-5 +1 ; -3 =-5+2 ;-2 = -5 +3 ;-1 = -5 +4 ;

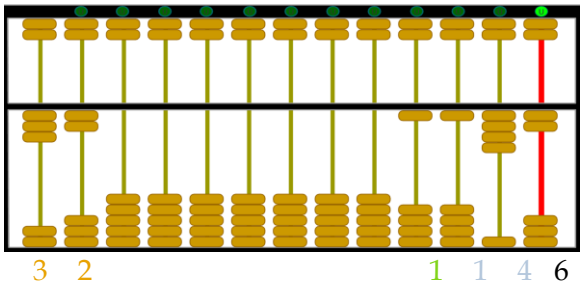
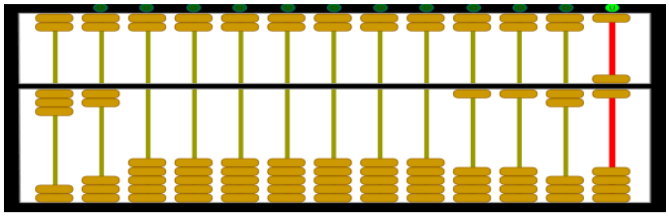
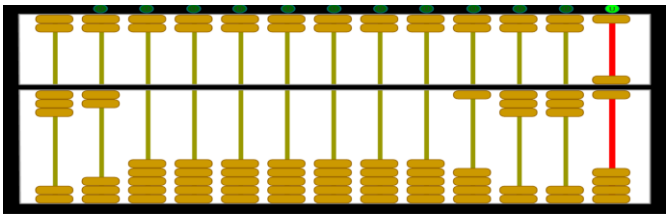
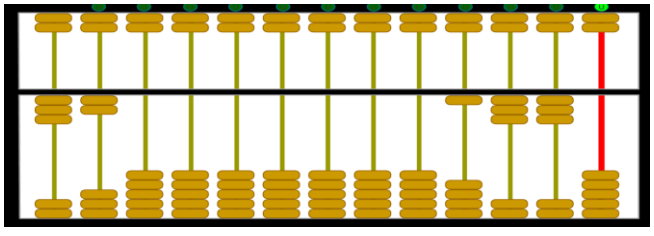
6-4		6-3	
7-4		7-3	
8-4		8-4	
68-34		78-34	
76-33		772-348	
26-18		9782-7849	
4762-2897		42327-37974	
5241-3756		54682-43862	
4762-3378		752-258*	
3648-2827			

<table>
<tr><td>Représentation
Avec cette notation, il est difficile de faire la soustraction</td><td>  </td></tr>
<tr><td>Donc on utilise le fait que : 100 = 1x 50 +5 x10</td><td>  </td></tr>
<tr><td>On constate aussi que - 27 = -30 + 3</td><td>  </td></tr>
<tr><td></td><td>Impression et intérêt
<table><tr><td>Comment avez trouvé cette manipulation ?</td><td>Plus compliqué que les autres</td></tr><tr><td>Quel intérêt y avez vous trouvé ?</td><td>C'est plus intéressant</td></tr><tr><td>Quelles sont les difficultés rencontrées par rapport à l'addition ?</td><td>aucune</td></tr><tr><td>Comment abordez vous ces deux opérations après ces manipulations ?</td><td>Elle paraissent plus évidentes</td></tr><tr><td colspan="2">Si vous avez d'autres remarques sur ce travail , positives ou négatives
vous pouvez les écrire ci dessous</td></tr><tr><td colspan="2"></td></tr></table></td></tr>
</table>

Division

Exemple 1 : Dividende : 7 ; quotient : 3 Diviseur : 2 ; reste : 1 7 | 2 1 | 3	
Règle 1 : le diviseur est inférieur au dividende : on utilise la table de multiplication, le quotient se place avant le dividende, le reste remplace le dividende.	
Exemple 2 : Divisons 13 par 2	
Méthode On ne peut diviser 1 par 2 ; on passe à la dizaine : ici 10.	le quotient est : 5 le reste est : 0
Règle 2 : Le dividende est inférieur au diviseur. Le quotient remplace le dividende. Le reste s'écrit directement à sa droite.	
On continue la division en prenant le reste 3 qui devient le dividende : 3 > 2 , donc le quotient 1 s'ajoutera à 5 (à la gauche du dividende, ici 3) et il reste 1 (3-2x1) remplace le dividende (ici 3)	

Division avec deux chiffres au diviseur

Exemple : 446 divisé par 32 Pour le chiffre des dizaines du dividende, les règles de positionnement du quotient sont les mêmes que pour la division à un chiffre.	
1er calcul : 44 divisé par 32 1ère étape : On utilise le chiffre des dizaines du diviseur et du dividende : 4 > 3 quotient = 1 : positionné avant la colonne du 4 ; reste = 1 : remplace le 4 ; ici le reste intermédiaire : 14 < 32 remarque : si le reste intermédiaire est supérieur à la dizaine (ici 30) on prend systématiquement comme quotient 9.	 3 2 1 1 4 6
2ième étape : on utilise le chiffre des unités du diviseur : ici 2. On soustrait 1 x 2 à 14 donc 12. remarque : il faut pour cette 2ième étape, toujours regarder les 2 chiffres après le quotient de la 1er étape.	 3 2 1 1 2 6
2ième calcul : on divise 126 par 32. 1ère étape : on utilise le chiffre des dizaines du diviseur et 1 pour le dividende : 1 < 3 donc (comme pour la division à un chiffre), on passe à 10 ; quotient : 3 reste 1	 3 2 1 3 3 6
2ième étape : on utilise le chiffre des unités du diviseur : ici 2. On soustrait 3 x 2 à 36 donc 30 **Conclusion** : quotient : 13 reste : 30	 3 2 1 3 3 0

CRYPTOLOGIE

PAGE Aurel
Chercheur
INRIA
aurel.page@inria.fr

Résumé
Cet atelier au colloque de l'IREM était basé sur un atelier que j'ai proposé de nombreuses fois à la Fête de la Science, dans le cadre du Parcours scientifique bordelais au centre Inria de Bordeaux, à des classes allant de la 3ème à la terminale en variant légèrement les sujets abordés. Ce texte retranscrit le contenu des différentes variantes de cet atelier, avec plus de détails.

I - BASES DE LA CRYPTOLOGIE

« À quoi vous fait penser le mot cryptologie ? » La plupart du temps, cette question suscite l'évocation des codes secrets et des téléphones portables. Lorsqu'on suggère le sigle HTTPS (HyperText Transfer Protocol Secure) et le symbole de cadenas des navigateurs web, tout le monde se souvient des sites internet à connexion sécurisée. Les cartes bleues et paiement sécurisés ou le vote électronique sont mentionnés plus rarement.

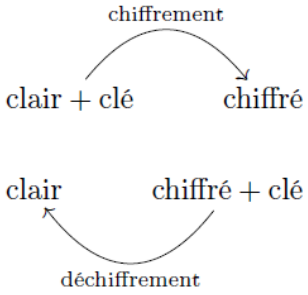
La cryptologie est **la science du secret** : le préfixe crypto- signifie « caché » et le suffixe -logie « science » ou « discours ». Elle regroupe l'ensemble des techniques permettant de transmettre ou conserver une information à destination de certaines personnes, et de la dissimuler aux autres. Elle possède deux composantes :

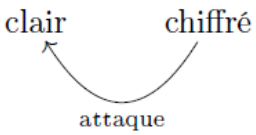
— La *cryptographie* : c'est la partie **défensive**, qui consiste à concevoir les procédés de dissimulation : le suffixe -graphie signifie « écriture » dans ce contexte.

— La *cryptanalyse* : c'est la partie **offensive**, qui consiste à essayer d'attaquer et de casser les procédés cryptographiques : le suffixe -lyse ou -analyse signifie « action de délier » ou « dissolution ».

Les deux composantes de cette discipline scientifique sont complémentaires et indissociables : il est souvent impossible de démontrer la sécurité d'un procédé cryptographique, mais on s'en convainc lorsque le procédé a résisté aux attaques de toute la communauté des experts pendant des années.

Vocabulaire de base de la cryptologie Dans le cadre de l'envoi sécurisé de messages, on peut résumer le procédé général ainsi :





Cela nous permet d'introduire un peu de vocabulaire :

- Le message sous une forme ordinaire, lisible par n'importe qui, est appelé le *clair*.
- Le message sous une forme illisible, indéchiffrable, est appelé le *chiffré*.
- Le procédé transformant le clair en chiffré s'appelle le *chiffrement*.
- Le procédé transformant le chiffré en clair s'appelle le *déchiffrement*.
- La *clé* est une information supplémentaire, secrète, qui est nécessaire pour procéder au chiffrement ou au déchiffrement.
- Lorsqu'on peut retrouver le clair à partir du chiffré sans la clé, on dit qu'on a une *attaque* contre ce procédé de chiffrement.

Remarquons que les terme de « code, codage, codé » sont réservés à un autre usage dans le jargon informatique et ne désignent pas une information cachée, contrairement à leur sens dans le langage courant.

Envoi sécurisé de messages On peut utiliser un tel procédé de chiffrement pour s'envoyer des messages de la manière suivante :

- Assia et Boaz se mettent d'accord sur une clé secrète commune.
- Assia chiffre son message à l'aide de leur clé.
- Assia envoie le chiffré à Boaz via un canal non sécurisé.
- Boaz reçoit le chiffré d'Assia et le déchiffre à l'aide de leur clé.
- Si l'indiscret Cyrille intercepte le chiffré, il ne peut pas retrouver le clair car il ne possède pas la clé.

Remarque : la même clé marche dans les deux sens, d'Assia vers Boaz ou de Boaz vers Assia. On parle de *cryptographie symétrique*, mais nous en reparlerons plus tard.

Les chiffres de substitution L'un des plus anciens procédés cryptographiques, utilisé au moins depuis l'Antiquité, consiste à remplacer chaque lettre par une autre dans l'alphabet : c'est ce qu'on appelle un *chiffre de substitution*.

Une version simple consiste à choisir un décalage dans l'alphabet (chiffre dit *de César*), par exemple :

$$a \to C, \quad b \to D, \quad c \to E, \quad \text{etc.}$$

Ici la clé est le décalage choisi (2 dans notre exemple), et permet de procéder au chiffrement comme suit :

$$\text{cesar (clair)} + \text{décalage } 2 \text{ (clé)} \dashrightarrow \text{EGUCT (chiffré)}$$

Le chiffre de César est-il sûr ? On s'aperçoit rapidement que non, car il y a seulement 26 clés différentes possibles. Si on possède un chiffré sans la clé, on peut essayer toutes les clés possibles, et un seul déchiffrement donnera un clair ayant du sens : on aura retrouvé le clair ainsi que la clé. Cette attaque est toujours considérée en premier dans l'analyse d'un procédé cryptographique, on l'appelle *attaque par énumération exhaustive*.

Un chiffre de substitution arbitraire est-il vulnérable face à une attaque par énumération exhaustive ? Pour répondre à cette question, il nous faut compter le nombre total de clés possibles. Le choix d'une clé consiste à choisir, pour chaque lettre, par quelle lettre de l'alphabet on la remplace. Pour la lettre 'a', on a 26 choix possibles. Pour chacun de ces 26 choix, il reste 25 choix possibles pour la lettre 'b' : on ne veut pas chiffrer 'a' et 'b' par la même lettre, car cela rendrait le déchiffrement impossible, même avec la clé. On arrive donc à 26×25 choix pour 'a' et 'b' combinés. En continuant ainsi pour toutes les lettres de l'alphabet, on compte un total de

$$26 \times 25 \times 24 \times \cdots \times 3 \times 2 \times 1 = 26! \approx 10^{27}$$

possibilités pour la clé (le symbole ! désigne la factorielle). Est-ce suffisant pour être protégé ? Pour cela il faut estimer la puissance de calcul disponible. Un ordinateur effectue de l'ordre de un milliard d'opérations par secondes. Le nombre d'ordinateurs en circulation est proche du nombre d'humains sur Terre (avec une répartition inégale), environ dix milliards. Le nombre de secondes dans une année est $3600 \times 24 \times 366 \approx 10^8$. Un an de calcul par l'humanité toute entière correspond donc environ à

$$10^9 \times 10^{10} \times 10^8 = 10^{9+10+8} = 10^{27} \text{opérations.}$$

On obtient une estimation similaire en remplaçant tous les ordinateurs personnels du monde par une dizaine des plus gros supercalculateurs du monde, d'une puissance d'environ un exaflop/s (10^{18} opérations par seconde). On peut donc estimer qu'il faudrait à l'humanité au moins 1 an de calcul pour tester toutes les clés possibles, ce qui paraît déjà être une bonne sécurité. Les crypto- systèmes réellement utilisés sont considérés comme sûrs si les meilleurs attaques connues nécessitent 10^{40} voire 10^{80} opérations suivant le niveau de sécurité visé.

II - ATTAQUE PAR ANALYSE DE FRÉQUENCES

Il faut attendre le IXe siècle pour qu'Al-Kindi, un savant arabe, propose une véritable technique de cryptanalyse contre les chiffres de substitution. Son attaque repose sur la remarque fondamentale suivante : dans une langue donnée, toutes les lettres n'apparaissent pas avec la même fréquence. Par exemple, en français, les fréquences approximatives sont les suivantes (en %) :

e	s	a	n	t	i	r	u	l	o
17.8	8.2	7.7	7.6	7.3	7.2	6.8	6.1	5.9	5.3

Si le chiffré est suffisamment long, on peut mesurer la fréquence d'apparition de chaque symbole, et s'en servir pour réduire le nombre de possibilités à un petit nombre. Les participants à l'activité ont utilisé cette technique pour retrouver le clair (et la clé) correspondant au chiffré suivant :

« U'PISYTFVQ ZY UD TREMFPHRDMKVY YCF ZY XDCAJYR JW XYCCDHY D U'DVZY Z'JWY TUY. PW TPWWDVF JWY XYFKPZY ZY TKVQQRYXYWF VWTDCCDIUY XDVC MDC FRYC MRDFVAJY. TYFFY FYTKWVAJY C'DMMYUUY UY XDCAJY SYFDIUY YF D YFY VWOYW- FYY MDR OYRWDX. YUUY TPWCVCFY D JFVUVCYR JWY TUY ZY UD XYXY UPWHJYJR AJY UY XYCCDHY D YWOPEYR. CV U'DFFDA- JDWF YCCDVY FPJFYC UYC TUYC MPCCVIUYC VU

OPVF FPJC UYC XYCCDHYC MPCCVIUYC. VU W'E D DJTJWY DFFDAJY MPJR RYFRP- JOYR UY XYCCDHY VWVFVDU XYXY DOYT JW FYXMC ZY TDUTJU VWQVWV. UY MRYXVYR MRPIUYXY ZY TYFFY FYTKWVAJY YCF UD HYWYRDFVPW Z'JWY TUY MDRQDVFYXYWF DUYDFPVRY. UY ZYJNVYXY YCF AJ'VU YCF ZVQQVTVUY Z'YWOPEYR JWY TUY FRYC UPWHJY ZY QDTPW CYTJRVCYY. UY FRPVCVYXY YCF AJ'VU WY QDJF MDC JFVUVCYR UD XYXY TUY MPJR ZYJN XYCCDHYC. »

Le texte chiffré était divisé en 9 phrases, réparties entre des groupes de 2 ou 3 participants. Chaque groupe comptait les occurrences des lettres, et les mesures étaient mises en commun de sorte à obtenir des fréquences globales sur le texte entier. Pour rendre l'activité réalisable en un temps court (20-30 minutes), seules les lettres fréquentes (C, D, F, J, U, V, W, Y) étaient comptées, le texte était préparé pour avoir des fréquences proches de la théorie, et la ponctuation et les espaces étaient conservés. De plus, après un temps de recherche indépendante, les groupes mettaient en commun les lettres qu'ils avaient trouvées, ce qui permettait à tout le monde de bénéficier des mots faciles à trouver de certaines phrases et de l'efficacité de certains groupes. La technique peut aussi être utilisée à la main sur des textes courts et sans ces aides, mais nécessite alors généralement quelques heures de tâtonnement. Les participants finissaient par reconstruire le texte clair suivant (ici reproduit sans majuscules ni accent puisqu'elles n'étaient pas prises en compte dans le chiffrement) :

« L'objectif de la cryptographie est de masquer un message à l'aide d'une clé. On connait une méthode de chiffrement incassable mais pas très pratique. Cette technique s'appelle le masque jetable et a été inventée par Vernam. Elle consiste à utiliser une clé de la même longueur que le message à envoyer. Si l'attaquant essaie toutes les clés possibles il voit tous les messages possibles. Il n'y a aucune attaque pour retrouver le message initial même avec un temps de calcul infini. Le premier problème de cette technique est la génération d'une clé parfaitement aléatoire. Le deuxième est qu'il est difficile d'envoyer une clé très longue de façon sécurisée. Le troisième est qu'il ne faut pas utiliser la même clé pour deux messages. »

Le texte évoque une autre technique de chiffrement, le *masque jetable* ou *chiffre de Vernam*. Elle consiste à chiffrer les lettres par un décalage (comme avec un chiffre de César), mais en utilisant un décalage différent pour chaque lettre. Plus précisément, la clé consiste en une suite de décalages, un pour chaque lettre du clair. On peut démontrer que cette technique est incassable : en effet, étant donné un chiffré, tout clair possible provient de ce chiffré via exactement une clé ; le chiffré ne contient donc aucune information sur le clair en l'absence de la clé. Un problème majeur de cette technique est que pour l'utiliser, il faut échanger au préalable une clé de la même longueur que le message à chiffrer. Nous reviendrons sur ce problème de l'échange de clé.

III - INFLUENCE DE LA DEUXIÈME GUERRE MONDIALE

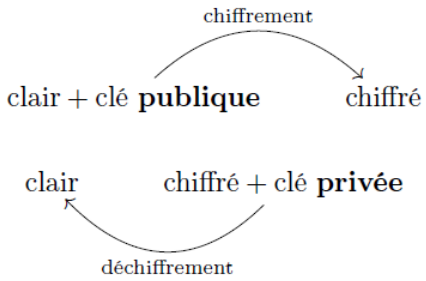
La cryptologie intéresse depuis longtemps les militaires. La deuxième guerre mondiale n'était pas une exception à cet égard : la cryptologie a joué un rôle clé dans son dénouement, et a connu des transformations majeures pendant cette période. Tout d'abord, une **automatisation** massive a été mise en place : du côté du chiffrement avec notamment les célèbres machines Enigma et Lorenz des allemands, mais aussi du côté de la cryptanalyse avec les « bombes » en Pologne puis à Bletchley Park, ancêtres de nos ordinateurs, qui permettaient d'analyser rapidement des milliers de possibilités. Un autre aspect important est celui de la

source de la confiance en la sécurité d'un procédé cryptographique. L'approche traditionnelle, qui semble de bon sens à première vue, a toujours été de **garder secret le procédé cryptographique** utilisé. Par exemple, durant la guerre, le fonctionnement des machines de chiffrement allemandes était gardé secret. Cependant, à plusieurs reprises des machines ou des manuels d'instructions ont été capturés, ce qui a permis aux services secrets de les étudier et de découvrir des faiblesses. A posteriori, il paraît illusoire d'avoir cru que ce type d'événement n'arriverait pas. Au contraire, dans la cryptographie moderne, les **procédés cryptographiques sont publics** et la sécurité doit dépendre seulement de la connaissance de la clé. C'est l'analyse scientifique et ouverte par la communauté des experts qui est la source de la confiance en la sécurité d'un cryptosystème.

Mais si la sécurité ne dépend que de la connaissance de la clé, une question reste en suspens, tout particulièrement à l'ère d'Internet : comment échange-t- on une clé avec une personne à l'autre bout de la planète, qu'on ne peut pas contacter physiquement ?

IV - CRYPTOGRAPHIE ASYMÉTRIQUE ET RSA

Principe La solution au problème du transfert de la clé a été résolue dans les années 70, avec l'invention par Diffie et Hellman de la cryptographie asymétrique. Leur idée est d'avoir deux clés différentes, une pour le chiffrement, et une pour le déchiffrement.



Le fonctionnement est le suivant. Supposons que Assia veut envoyer un message chiffré à Boaz.

- Boaz génère une paire de clés, l'une publique et l'autre privée.
- Boaz envoie sa clé publique à Assia via un canal non sécurisé.
- Assia **chiffre** son message à l'aide de la **clé publique**.
- Assia envoie le chiffré à Boaz via un canal non sécurisé.
- Boaz reçoit le chiffré d'Assia et le **déchiffre** à l'aide de sa **clé privée**.

La clé publique de Boaz peut être interceptée, mais cela n'a pas d'importance car elle ne permet pas de déchiffrer.

Dans leur article, Diffie et Hellman décrivent le principe d'un cryptosystème asymétrique, mais n'en proposent pas un concret. Le premier exemple est dû à Rivest, Shamir et Adleman, qui conçurent un système qui porte leur nom et est fréquemment utilisé : RSA.

Fonctionnement de RSA RSA est décrit comme un système de chiffrement qui **transforme un nombre en un autre nombre**. Il faut imaginer qu'on choisit un grand nombre N, et qu'on convient d'un encodage

public pour passer d'une suite de lettres à un nombre entre 0 et $N-1$ et inversement. Si le message à chiffrer est trop long, on le découpe en blocs qu'on chiffre indépendamment.

Par exemple pour $N = 24^2 = 576$ on peut encoder deux lettres dans chaque nombre entre 0 et $N-1$ par la règle : aa $\to 0$, ab $\to 1$, . . ., az $\to 25$, ba $\to 26$, bb $\to 27$, bc $\to 28$, . . ., zz $\to 575$. Insistons sur le fait que cet encodage est public et ne masque aucune information : il sert uniquement à transformer un problème de chiffrement de suites de lettres en un problème de chiffrement de nombres. On va donc définir un chiffrement sur les nombres entre 0 et $N-1$.

Le cryptosystème RSA est basé sur l'**arithmétique modulaire**. Cela consiste à choisir un entier N et à faire des opérations sur des nombres entiers, en éliminant systématiquement les multiples de N. Lorsqu'on calcule modulo N, on peut ainsi ramener tous les nombres dans l'intervalle $\{0, \ldots, N-1\}$.

Exemple : « arithmétique des horloges » modulo $N = 24$: 5h après 22h, il est 3h. On dit que $22 + 5 \equiv 3$ modulo 24.

Exemple : le calcul modulo $N = 10$ revient à ne garder que le dernier chiffre. $8 + 7 = 15 \equiv 5$ modulo 10.

L'arithmétique modulaire permet aussi de faire des multiplications.

Exemples : $5 \times 6 = 30 \equiv 6 \bmod 24$, $3 \times 8 = 24 \equiv 4 \bmod 10$.

Munis de cet outil, nous pouvons décrire le procédé de chiffrement.

- On choisit deux grands nombres premiers p et q, et on pose $N = pq$.
  Exemple : $p = 2$, $q = 5$ et $N = 10$.
- On choisit un entier e entre 1 et $(p-1)(q-1)$, premier avec $(p-1)(q-1)$.
  Exemple : $e = 3$ est premier avec $(p-1)(q-1) = 1 \times 4 = 4$.
- Avec l'algorithme d'Euclide, on calcule des entiers u, v tels que $eu + (p-1)(q-1)v = 1$.
  Exemple : $u = 3$, $v = -2$ vérifient $eu + (p-1)(q-1)v = 3 \times 3 - 4 \times 2 = 1$.
- La **clé publique** est (N, e) et la **clé privée** est u.
- Soit $m \in \{0, \ldots, N-1\}$ le clair à chiffrer. Le chiffré correspondant est $c \equiv m^e \bmod N$. On peut effectuer l'opération de chiffrement en connaissant uniquement la clé publique.
  Exemple : $m = 3$, d'où $c = m^e = 3^3 = 27 \equiv 7 \bmod 10$.
- Le déchiffrement du chiffré c consiste à calculer $c^u \bmod N$. Une conséquence du petit théorème de Fermat et du théorème des restes chinois est que pour tout message m qui n'est divisible ni par p ni par q, on a $c^u = (m^e)^u = m^{eu} \equiv m \bmod N$.
  Exemple : $c^u = 7^3 = 7 \times 49 \equiv 7 \times 9 = 63 \equiv 3 \bmod N$. On retrouve bien le message $m = 3$.

Pourquoi RSA est-il difficile à attaquer ? Étant donnés e et N, on ne sait trouver la clé privée u que si on sait trouver les facteurs premiers p et q de N.

- Il est **facile** de calculer $N = pq$ à partir de p et q (**multiplication**).
  Exemple : $859 \times 9001 = ?$ Vous pouvez effectuer cette multiplication à la main.
- Il est **difficile** de retrouver p et q à partir de N (**factorisation**).

Exemple : 3252911 = ? × ? Pour factoriser ce nombre naïvement, il faudrait essayer de le diviser par tous les nombres premiers jusqu'à 1800, cela donnerait 278 divisions à effectuer, ce qui serait très long!

Bien entendu, nous connaissons de meilleurs algorithmes que d'essayer toutes les divisions possibles, mais ils restent beaucoup plus lents qu'une multiplication. Actuellement les records de factorisation atteignent des nombres de 250 chiffres, alors qu'on peut sans problème multiplier des entiers de milliards de chiffres.

V- CRYPTOGRAPHIE POST-QUANTIQUE

Une partie de la recherche actuelle en cryptographie est consacrée au post-quantique. Malheureusement, l'ordinateur quantique est souvent une source de grande confusion. Essayons de clarifier les choses.

Qu'est-ce que l'ordinateur quantique ? C'est un modèle de calcul (une abstraction) inspiré des lois de la mécanique quantique, et qu'on espère pouvoir réaliser par un dispositif physique. On peut imaginer un ordinateur quantique comme un ordinateur ordinaire (classique) auquel est branché un appareil qui possède un état interne, inaccessible directement, mais sur lequel on peut faire certaines opérations. Les ordinateurs quantiques déjà construits ne sont que des approximations de ce modèle.

Quel est le lien avec la cryptographie ? L'algorithme quantique de Shor résout rapidement deux problèmes difficiles très utilisés en cryptographie : la factorisation et le problème du logarithme discret. Les ordinateurs quantiques existants sont très loin de pouvoir appliquer cet algorithme à des problèmes de taille cryptographique.

Mythe : un ordinateur quantique peut résoudre des problèmes que les ordinateurs classiques ne pourraient jamais résoudre, même avec un temps de calcul infini. C'est faux. Un ordinateur quantique peut être simulé par un ordinateur classique, mais avec un temps et une mémoire exponentiellement plus grands. Ils résolvent donc les mêmes problèmes, mais pas nécessairement avec la même efficacité.

Mythe : un ordinateur quantique résout des problèmes difficiles en essayant toutes les solutions en parallèle. C'est faux. L'état d'un ordinateur quantique peut encoder toutes les solutions possibles et leur appliquer certaines opérations, mais on ne peut pas accéder à cette information, on peut seulement obtenir une solution aléatoire. Toute la difficulté dans la conception d'algorithmes quantiques consiste à amplifier la probabilité d'obtenir une bonne solution en utilisant les opérations permises par la mécanique quantique.

Qu'est-ce que la cryptographie post-quantique ? Il s'agit de concevoir des procédés cryptographiques utilisables sur un ordinateur classique, mais qu'on pense résistants même à un attaquant disposant d'un ordinateur quantique.

VI - AUTRES APPLICATIONS DE LA CRYPTOGRAPHIE

Pour terminer, rappelons que la cryptographie moderne ne se limite pas au chiffrement des messages. Elle a de nombreuses autres applications, parmi lesquelles :

- le vote électronique ;
- les monnaies décentralisées ;

- le calcul sur des données chiffrées ;
- la signature, qui permet d'assurer l'authenticité (l'auteur est bien celui qui le prétend) et l'intégrité (non-modification) d'une donnée ;
- la mise en gage, dans laquelle une personne garde une information secrète temporairement puis la révèle, sans pouvoir la modifier entre-temps ;
- le partage de secret, dans lequel plusieurs personnes protègent une donnée, mais ne peuvent y accéder qu'ensemble ;
- les preuves zero-knowledge (l'expression française « preuve à divulgation nulle de connaissance » est très lourde), qui consistent à démontrer qu'on détient une information sans la révéler ;
- etc.

La cryptologie, qui est d'une importance cruciale pour notre mode de vie actuel, est une discipline scientifique florissante, qui a aussi le charme de faire émerger de très intéressants problèmes mathématiques, notamment en arithmétique.

ATELIERS MATHS ET JEUX

Groupe Maths et Jeux
IREM d'Aquitaine
Responsable du groupe : Anne-Claire Muller
Anne-claire.muller@ac-bordeaux.fr
https://maths-et-jeux.hubside.fr/

1. Le groupe IREM Maths et Jeux

Au sein de l'IREM d'Aquitaine, le groupe "Maths et Jeux" travaille sur l'utilisation des jeux comme outils pédagogiques pour l'apprentissage des mathématiques.

Les membres de ce groupe sont des enseignants du premier et du second degré, qui partagent un intérêt commun pour l'exploration des différentes manières dont les jeux peuvent être intégrés dans l'enseignement des mathématiques. Ils mettent l'accent sur la conception, l'adaptation et la mise en œuvre de jeux mathématiques afin de rendre l'apprentissage des mathématiques plus attrayant, interactif et efficace pour les élèves.

Le groupe "Maths et Jeux" de l'IREM d'Aquitaine développe des ressources pédagogiques, des jeux et des matériaux didactiques pour les enseignants et les élèves.

En résumé, le groupe "Maths et Jeux" de l'IREM d'Aquitaine se focalise sur l'exploration des possibilités d'intégration des jeux dans l'enseignement des mathématiques, dans le but d'améliorer l'expérience d'apprentissage des élèves et de promouvoir une approche ludique et engageante des mathématiques.

« ***Le jeu est la forme la plus élevée de la recherche.*** » ***Albert Einstein***

I - ATELIER AJ1 : LES JEUX DU COMMERCE

Animateurs : Jean-Marc OROZCO et Thimothé LICITRI
Niveau : cycle 3 au lycée

Le groupe Maths et Jeux a pour objectif de trouver des jeux du commerce qui permettent à nos élèves de développer des compétences mathématiques ou des compétences plus transversales. Nous vous avons proposé d'explorer et jouer à des jeux tels que Skyjo, Quarto, Can't stop et Paquet de Chips ! Vous constatez que les mathématiques constituent le fondement de nombreux jeux de société !

Nous avons présenté des jeux du commerce en indiquant leur possible utilisation en club maths ou en classe. Les contraintes sont différentes : temps, nombre d'élèves, objectifs.

Pour une utilisation en classe, nous conseillons par exemple, de jouer au même jeu avec plusieurs exemplaires.

Les participants de l'atelier ont pu découvrir de nombreux jeux et ainsi envisager de les utiliser en classe ou pour la formation des futurs enseignants.

Une partie des jeux présentés pendant l'atelier sont disponibles sur le diaporama de présentation, d'autres sur le site du groupe. Vous y trouvez notamment le top 10 de nos jeux préférés, parmi lesquels : Skyjo, 6 qui prend, Lobo 77 et Opération Amon Ré faisant travailler la numération et le calcul. Les jeux Paquet de chips, et Can't Stop font travailler les probabilités. Les jeux Recto Verso et Genius square font travailler la géométrie et la vue dans le plan ou l'espace. Enfin, le jeu MARI fait travailler l'algorithmique et la programmation. Ces jeux sont principalement destinés à des élèves du primaire et du collège. Quelques jeux peuvent être utilisés au lycée, comme le jeu 4, 6, suite, qui fait travailler la notion de suites numériques.

Nous proposons une liste de jeux très complète classée par niveau listant les principales compétences travaillées pour chacun des jeux.

II - ATELIER AJ2 : LES JEUX REVISITES

Animatrice : Laurence ALTHUISIUS

Niveau : cycle 3 au lycée

Le groupe Maths et Jeux a également pour but de revisiter des jeux de société afin de développer des compétences mathématiques. Vous trouverez de nombreux jeux créés par les membres du groupe pour leurs propres élèves, tels que le Sunny Numbers adapté à tous les niveaux, le Fracto et le Math-hoo. Tous ces jeux ont été développés à partir de jeux de société populaires existants !

Pendant l'atelier, nous avons présenté :

- **Le groupe IREM maths et jeux**, nos objectifs et notre travail.
- Les différents jeux créés par les collègues : Sunny Numbers est un jeu faisant travailler la numération et le calcul, revisité à partir du jeu de plateau Lucky Numbers que nous avons décliné dans tous les niveaux : nombres décimaux pour le premier degré, nombres relatifs et fractions pour le collège, et sens de variations des fonctions pour le lycée. Nous avons présenté un jeu de cartes Math-Hoo revisité à partir du jeu Hula-Hoo. Il travaille également la numération et le calcul pour des élèves de début de collège.
- **Les jeux revisités créés par des lycéens à l'occasion de la semaine des maths** sur le thème Maths à la carte (Trivial, Uno, 7 familles...). Ces jeux font travailler différents points du programme : fractions, puissances, racines carrées, dérivées…Ils sont utilisés en remédiation ou en appui pour faciliter l'assimilation des notions.
- **Des devoirs maison revisités**. Nous avons présenté des jeux utilisés en bilan de période pour faire réviser des élèves de lycée. Parmi eux, un Cluedo donné en devoir maison pour retravailler les notions de pourcentages et le premier degré en seconde, mais aussi un labyrinthe donné en

terminale, pour réviser toutes les notions vues jusqu'en décembre, et enfin un pixel art donné en seconde, pour réviser les notions vues au premier trimestre. Nous avons également présenté un pixel art collaboratif donné en fin d'année de seconde pour réviser les équations, probabilités et statistiques qui, une fois finalisé, permettait d'obtenir un portrait de Maryam Mirzakhani.

- **Des jeux revisités plus spécifiquement sur le thème de l'arithmétique** : Primo, qui est un jeu créé par l'IREM de Caen, le jeu Juniper Green, le jeu des potions décomposées…

Nous avons ensuite proposé aux participants de jouer à 4 jeux : potions recomposées, Primo, Math-hou, et Sunny Numbers. Ces jeux sont utilisés en classe sur des temps courts (10 à 15 minutes) pour favoriser la mémorisation de notions clés, comme le calcul littéral, le calcul fractionnaire, sur les puissances, de façon à donner un côté plus ludique et agréable à des séances sur l'apprentissage de la technique de calculs mathématiques.

Les jeux proposés dans l'atelier sont téléchargeables sur le diaporama de présentation.

III - ATELIER AJ3 : LE JEU « TURING MACHINE »

Animateur : Alexandre AUDOIN

Niveau : lycée

Avez-vous déjà entendu parler du Turing Machine ? Il s'agit d'un jeu de déduction sorti sur le marché à la fin de l'année 2022, dont le but est de trouver quatre chiffres en posant des questions à des cartes à connotation arithmétique. Le but est de mettre vos compétences mentales à l'épreuve en affrontant d'autres participants !

L'idée est de proposer aux participants l'utilisation d'un jeu comme outil pédagogique de réflexion logique. Chacun a pu tester ce jeu en collaboration dans un premier temps par groupes de 4, puis, sur une seconde partie en opposition, dans l'objectif d'optimiser la recherche du code secret en utilisant le minimum de tests possibles.

Turing Machine est un **jeu de déduction compétitif fascinant**. Il permet d'interroger un proto-ordinateur fonctionnant sans électricité ni électronique, qui ouvre la voie à une nouvelle génération de jeux de déduction.

Le but ? Trouver le code secret avant les autres joueurs, en interrogeant astucieusement la machine. Avec Turing Machine, vous utilisez un **ordinateur mécanique au matériel original composé de cartes perforées**.

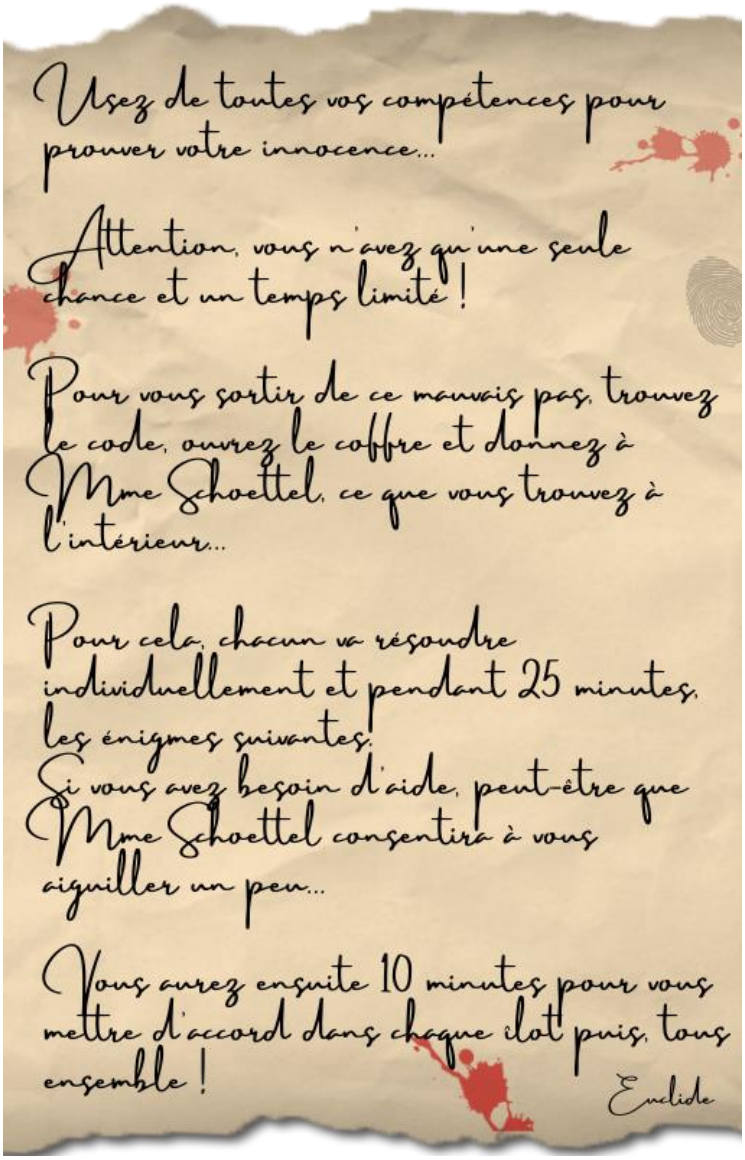
Grâce à TuringMachine.info, ce sont plus de **7 millions de problèmes générés en ligne**, allant de combinaisons simples à des combinaisons incroyablement complexes, qui vont alimenter la « rejouabilité » presque infinie de Turing Machine.

Maintenant c'est à vous de le faire vivre à vos élèves dans vos établissements. Ce jeu permet non seulement de faire travailler la logique à vos élèves mais également d'aborder l'arithmétique sous un angle original, puisque la plupart des vérificateurs font appels à ces notions.

IV - ATELIER AJ4 : L'ESCAPE GAME « LES MYSTERES DE LA DIVISIBILITE »

Animatrices : Ambre SCHOETTEL

et Marlène DARNIS



Niveau : collège et lycée

Un cambriolage a eu lieu au collège Cheverus de Bordeaux ! Un ordinateur contenant des informations sensibles a été dérobé. Rejoignez l'agent Euclide et aidez-le à résoudre l'enquête !

Vous trouverez ici une version collège et une version lycée avec tous les documents prêts à l'emploi : parchemin, livret élève, vidéo et corrigé.

L'atelier "Escape game : Les mystères de la divisibilité" a débuté par une présentation rapide de l'escape game et par la diffusion de la vidéo qui a été proposée aux élèves. Cette vidéo a permis aux 20 personnes présentes (mais normalement, aux élèves) de rentrer directement dans l'activité et de comprendre ce qui les amène à réaliser ces énigmes... L'ensemble du groupe a terminé les énigmes niveau collège en 15 min environ et a enchaîné sur les énigmes niveau lycée (qu'ils n'ont pas terminées).

Pour réaliser cet escape game avec vos élèves, voici quelques conseils et un retour d'expérience :

Matériel à prévoir :

- Cadenas code à 4 chiffres
- Boîte fermée par le cadenas

- Clé USB à mettre à l'intérieur de la boîte, avec dessus une vidéo permettant d'innocenter les élèves (ou autre si vous le souhaitez)
- Vidéo « Flash info »
- Livrets imprimés pour les élèves (prévoir plusieurs exemplaires au cas où ils commettent des erreurs à l'énigme 1)
- Parchemin imprimé

Mise en place de cette activité :

Avant la séance, l'enseignant doit installer, au fond de la salle, la boîte fermée, les livrets et le parchemin.

La vidéo « Flash info » est montrée aux élèves dès leur entrée en classe. Une fois la vidéo terminée, l'enseignant demande à un élève de lui ramener le matériel, lit le parchemin qui donne les consignes et distribue le livret à chacun.

Les élèves se lancent dans l'activité, le minuteur démarre et le reste de la séance est rythmée grâce à la vidéo qui annonce la fin de la recherche individuelle, le début du travail collectif et la fin de ce dernier.

L'enseignant fait ensuite une mise en commun avec les élèves afin qu'ils se mettent d'accord sur **un seul code** et conclut la séance avec un bilan.

Difficultés potentielles :

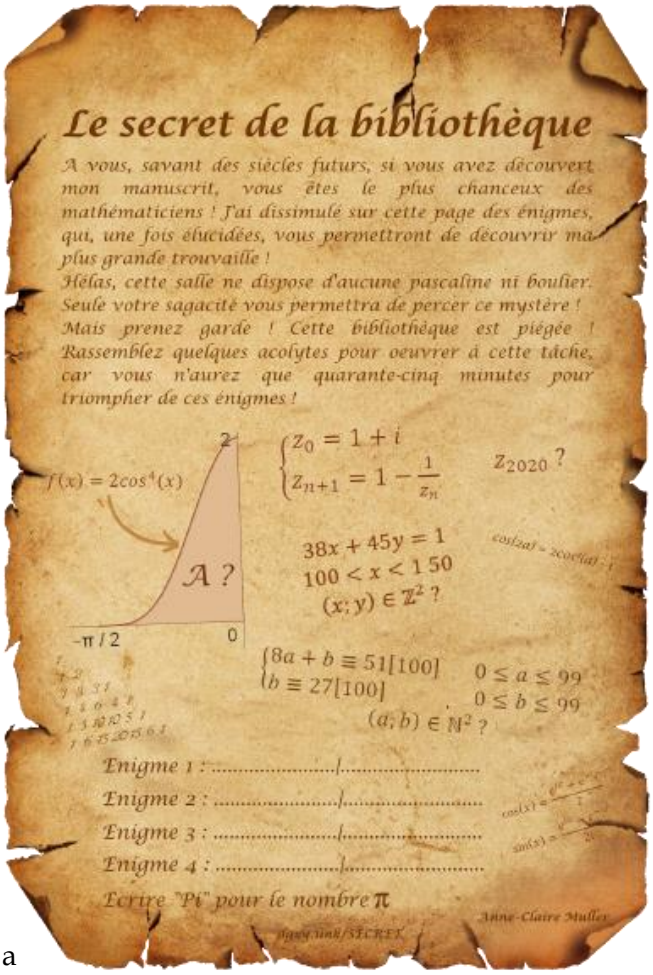
- Pour l'énigme 1, il faut veiller à ce que les élèves colorient bien les cases afin que le code apparaisse clairement à la fin. Les élèves n'ont pas rencontré de difficultés particulières si ce n'est d'oublier de vérifier **tous** les critères à chaque fois.
- Pour l'énigme 2, les élèves ont tendance à s'arrêter au « 2 » puisqu'un code couleur apparaît pour la première fois, il faut alors bien insister sur le fait **de continuer le chemin tant qu'ils le peuvent**.
- L'énigme 3 est l'énigme qui a posé le plus de soucis, les élèves confondent «chiffres» et «nombres» puis ne tiennent pas compte du rang indiqué dans chaque phrase et obtiennent ainsi un code faux (ils ne mettent pas les chiffres au bon endroit). Pour gagner du temps sur la résolution de cette énigme, il est possible de leur autoriser la calculatrice pour la seconde étape de cette énigme.

Pour éviter de perdre du temps, il est plus judicieux de placer les élèves en îlots, afin que la transition entre le travail individuel et collectif se fasse rapidement.

V - ATELIER AJ5 : L'ESCAPE GAME « LE SECRET DE LA BIBLIOTHEQUE»

Animatrice : Anne-Claire MULLER

Niveau : lycée (maths expertes)



Au sein d'une bibliothèque, vous faites une découverte surprenante : un vieux manuscrit renfermant une série d'énigmes arithmétiques. Un secret d'une grande importance sera révélé si vous parvenez à les résoudre ! Relevez le défi et tentez à votre tour de percer ce mystère captivant ! Vous trouverez ici tous les éléments de l'escape game : parchemin, les Genially (l'un avec timer et l'autre sans) et le corrigé.

Cet escape game d'un niveau de terminale mathématiques expertes est semi-numérique et doté d'un timer car il est possible de le résoudre en temps limité (45 minutes) pour ajouter un peu d'enjeu ! Les énigmes sont sur un parchemin mais les réponses doivent être entrées sur un Genially. Chaque bonne réponse donne accès à un indice. Les 4 indices réunis permettent de résoudre l'énigme finale qui donne accès au message cherché.

L'atelier « Escape game : le secret de la bibliothèque » a débuté par la présentation du Genially de mise en situation. Chaque participant a pris possession de son parchemin contenant les 4 énigmes à résoudre, ainsi qu'un lien raccourci permettant d'accéder à un Genially. Une fois expliqué, le principe de ce Genially qui permet d'entrer les réponses des énigmes et de les valider, les participants ont débloqué la 5ème énigme : la résolution d'un système de 4 équations à 4 inconnues que les participants ont tenu à résoudre à la main, ce qui n'est pas attendu pour les élèves. À ce moment de l'escape game, on peut mettre à disposition des calculatrices, car la résolution attendue est une résolution matricielle du système. À la fin du temps imparti, nous avons évoqué les outils numériques utilisés pour concevoir ce jeu : Canva et Genially.

Quelques jours plus tôt, mes élèves de maths expertes avaient testé cet escape game et réussi à résoudre les énigmes dans le temps imparti. Pour cela, ils s'étaient réparti les différentes énigmes par centre d'intérêt, car les énigmes abordaient des thèmes différents du programme de maths expertes. J'ai notamment confié l'énigme de l'aire, qui demande à linéariser un cosinus, à un groupe en particulier, car c'est le travail le plus long de l'escape game. Au final, tout le monde a trouvé son énigme et mon petit message d'encouragement, ce qui a permis de finir cette année sur une note à la fois ludique et émouvante !

À la fin, comme il restait un peu de temps, j'ai présenté un Cluedo créé par Carine RUBY pour des élèves de l'option maths expertes. Ce dernier porte sur les premiers chapitres de maths expertes : la forme algébrique des nombres complexes et le début de l'arithmétique. Ce Cluedo utilise les notions de division euclidienne et de congruence. Il utilise notamment les codes cryptés à l'aide de la méthode de Vigenere. J'ai fait part de mon retour d'expérience, puisque je l'ai testé en 2022. Ce travail est prévu pour durer 2 heures, ce qui est un peu long pour des élèves. J'avais mis en compétition 3 équipes qui se sont alors réparties le travail en atelier pour qu'il soit faisable en 1 heure mais le travail était quand même trop dense. J'ai donc créé une version faisable en une heure en réduisant le nombre d'énigmes tout en gardant le concept de travail collaboratif par équipe pour résoudre les énigmes.

Maths Experts

Cluedo

Qui a assassiné Monsieur Burns ?

Le shérif Wiggum découvre le corps sans vie du riche industriel Charles Montgomery Burns et l'histoire de fou commence à springfield !

Dans un accès d'incompétence notoire, Wiggum identifie six suspects : Homer, Marge, Lisa, Bart, Krusty le clown et Waylon Smithers !

Il vous donne **deux heures** pour résoudre l'énigme grâce à des indices mathématiques que seuls des experts comme vous réussiront à déchiffrer.

Qui a commis cet affreux meurtre ?
Dans quelle pièce ? Avec quelle arme ?

Afin de résoudre cette affaire au plus vite, le shérif Wiggum vous demande de former trois équipes indépendantes de six experts.
Dans chacune des trois équipes, vous devrez collaborer avec d'autres experts pour rédiger un rapport détaillé de votre enquête, en faisant figurer tous les calculs effectués, ainsi que vos conclusions.
L'équipe la plus rapide pour résoudre l'enquête sera récompensée !

good luck!

Création : Carine Ruby

Page 1

VI - ANNEXES

- Diaporama des ateliers
- Site du groupe Maths et Jeux

Titre : Actes du colloque « Raisonner en arithmétique. Est-ce incongru ? »

Talence les 15, 16 et 17 juin à Talence

Directeurs de publication : Foulquier Laurianne, Judas Christian, Lambert Patricia

Mots-clés : Arithmétique, collège, lycée, raisonnements, informatique, cryptographie, histoire des mathématiques, algorithmique, logique, nombres et numération

Dépôt légal : 2025

Nombre de pages : 324 pages A4

Editeur :

ISBN :

Public concerné : Professeurs de mathématiques, professeurs des écoles, formateurs en mathématiques chargés de la formation des professeurs de mathématiques et des professeurs des écoles

Prix :

Actes du colloque « Raisonner en arithmétique. Est-ce incongru ? »

Depuis les programmes de collège (septembre 2016) et de lycée (janvier 2019), l'arithmétique a retrouvé une place plus importante à ces deux niveaux d'enseignement. Ce retour mérite une réflexion de la part de tous les acteurs de la communauté éducative afin de mieux accompagner les collègues et les élèves, le réseau des IREM s'y engage pleinement.

Le préambule des programmes de mathématiques du cycle 4 souligne l'importance de la formation au raisonnement et le rôle particulier que peut y jouer l'arithmétique. Ce travail contribue fortement à la formation de la personne et du citoyen (domaine 3 du socle). La notion de preuve est toujours un objectif central dans le secondaire :
« Le programme du cycle 4 permet d'initier l'élève à différents types de raisonnement, le raisonnement déductif, mais aussi le raisonnement par disjonction de cas ou par l'absurde » pour préparer le passage à la démonstration qui est un enjeu fondamental du programme de seconde. C'est aussi l'occasion, pour les élèves, d'enrichir leurs connaissances sur les nombres.

De nombreuses recherches ont montré les potentialités de l'arithmétique pour mener un tel travail, la géométrie n'étant pas le seul domaine pertinent pour raisonner, conjecturer, prouver. En effet, la familiarité des élèves avec les nombres facilite leur engagement dans la tâche et il est aisé de proposer des exercices d'arithmétique conduisant à formuler une conjecture qui ne soit pas une évidence. Il y a alors un véritable enjeu à prouver cette conjecture. De nombreux groupes IREM et chercheurs ont déjà exploré cette thématique. Ainsi, ce colloque sera l'occasion de proposer une synthèse de ces travaux.

Il s'adresse à tous les acteurs du premier et second degré jusqu'à l'université. Il abordera quelques-unes des questions qui se posent aux enseignants et aux formateurs : Quels enjeux d'apprentissage de l'arithmétique du cycle 3 à l'université ? Comment permet-elle d'engager les élèves dans un processus de preuve ? Quelles compétences mathématiques sont travaillées à travers son apprentissage ? Quelle(s) articulation(s) entre arithmétique et logique ? Quel apport de l'histoire des mathématiques concernant les usages de l'arithmétique ? Quels transferts en classe ? Quelle place pour l'algorithmique et la programmation ? Les propositions d' ateliers aborderont l'une ou plusieurs de ces questions et pourront adopter le point de vue des savoirs en jeu, des apprentissages des élèves, des pratiques ou de la formation des professeurs.

L'un des objectifs de ce colloque est ainsi de donner aux différents acteurs une vision d'ensemble de l'enseignement de l'arithmétique à travers des conférences, communications et ateliers.

Les conférences proposées autour des thèmes arithmétique et cryptographie (Daniel PERRIN), arithmétique et didactique (Véronique BATTIE), arithmétique et raisonnement (René CORI), arithmétique et algorithmique/programmation (Jean-Michel Muller) et arithmétique et histoire des mathématiques (Marc MOYON) viendront nourrir cette réflexion.

irem

ISBN