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.

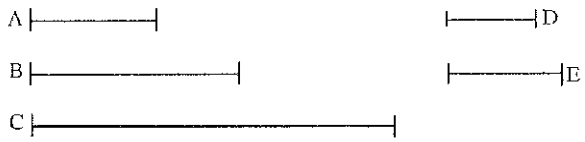
Pour ce qui est de la reconnaissance de la divisibilité par 7, une idée pourrait être d'effectuer mentalement la division euclidienne de l'entier par 7 et de voir si le reste est nul. Prenons le nombre 553924 et appliquons-lui l'algorithme de division usuel. Le reste de la division euclidienne de 55 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.

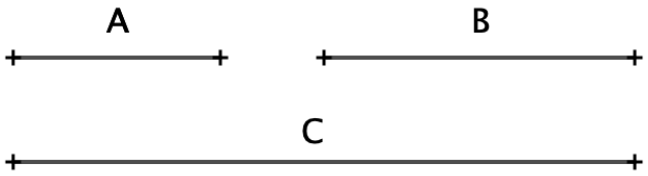
Ainsi, Euclide pose C le nombre obtenu en multipliant deux entiers A et B donnés et note D un diviseur premier de C dont il suppose qu'il ne divise pas A. Son objectif est de prouver, dans ce cas, que D divise B. La situation est parfaitement symétrique en échangeant les rôles de A et de B, ce qu'il 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)*

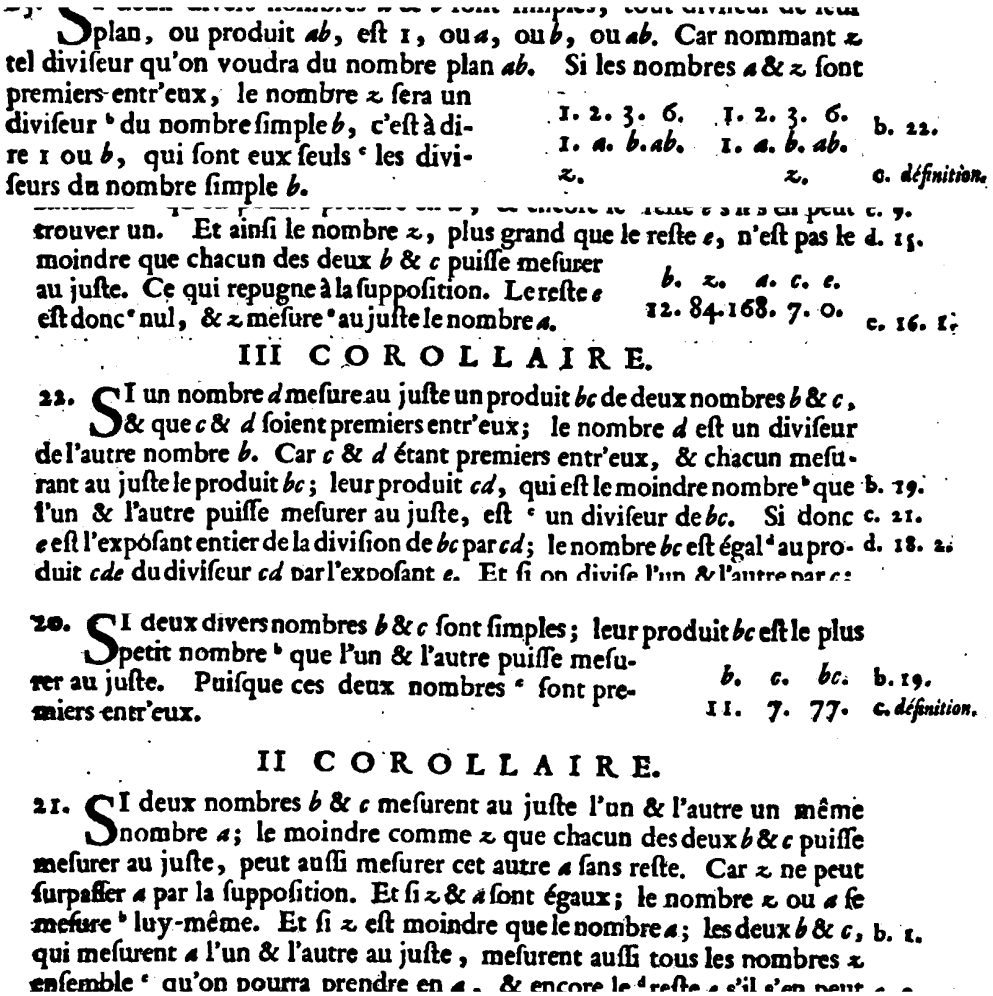
Dans ce texte nous reconnaissons d'abord le critère bien connu de divisibilité par 9 : « quand du nombre de l'addition des figures laissant tous les 9, il reste rien, qui est 0 ; alors ce nombre pourra se diviser par 9. » Forcadel parle de « l'addition des figures » là où nous dirions aujourd'hui « somme 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 $k \in \mathbb{Z}$.