LES DEMONSTRATIONS EN ARITHMETIQUE :

A propos de quelques preuves historiques du petit Théorème de Fermat

Martine BÜHLER, Anne MICHEL-PAJUS
Irem Paris 7 / Projet INRP

Un des aspects intéressants de l'arithmétique est que, sans avoir besoin d'un arsenal théorique important, on peut y faire de véritables démonstrations mathématiques, s'appuyant sur des raisonnements d'une certaine finesse.

On y travaille sur des objets familiers : les entiers. On y tient des raisonnements multiples et complexes ; on y obtient des résultats non triviaux mais faciles à comprendre, qu'on peut tester ou découvrir par expérimentation. L'arithmétique, présente dans les programmes de Terminale C de 1971, avait disparu au début des années quatre-vingts pour vingt ans et est revenue tant dans les programmes de collège (algorithme d'Euclide) que dans le programme de la spécialité « mathématiques » en Première et Terminale L, et Terminale S.

Ce retour s'accompagne d'une évolution notable, où est souligné l'intérêt d'une démarche expérimentale et plus généralement de la multiplicité des approches. Les textes historiques fournissent des exemples de cette diversité des points de vue. Il se trouve aussi que certains enseignants n'ont jamais étudié d'arithmétique au Lycée, et ne l'ont vue qu'en Théorie des nombres à l'Université, un point de vue fort éloigné de l'enseignement requis. L'analyse des preuves historiques nous semble une bonne approche pour un approfondissement de la réflexion.

Nous donnons au §1 les outils d'analyse que nous avons élaborés. Des preuves historiques du théorème de Fermat sont présentées au §2. Le §3 contient des commentaires et des compléments historiques, et le §4 des exemples de textes destinés aux élèves.

I. Les outils de démonstration et les démarches dans les manuels de Terminale S

I.1. *Le Théorème fondamental de divisibilité*

L'arsenal théorique, au-delà des propriétés élémentaires de divisibilité (par exemple, si un entier a divise à la fois b et c, alors a divise la somme $b + c$) et de l'algorithme d'Euclide, se réduit à un seul résultat fondamental, qu'on retrouve sous diverses formes équivalentes au cours de l'histoire, et que nous nommerons : théorème fondamental de divisibilité.

- « Proposition 32 d'Euclide » dite « Lemme d'Euclide » : si un nombre premier divise un produit, alors il divise l'un des facteurs du produit[1]. On le rencontre aussi sous sa forme contraposée : si un nombre premier p ne divise ni a ni b, alors il ne divise pas le produit ab.
- « Proposition 26 d'Euclide » : si deux nombres a et b sont premiers avec c, le produit ab sera aussi premier avec c.
- « Théorème de Gauss » : si un nombre divise un produit et est premier avec l'un des facteurs du produit, alors il divise l'autre.
- « Théorème fondamental de l'Arithmétique » : la décomposition d'un nombre entier en produit de facteurs premiers est unique. Notons que le théorème fondamental renvoie souvent aussi à l'existence de la décomposition, qui n'est pas concernée ici.

Le programme de Terminale S « spécialité mathématiques » y ajoute le théorème de Bachet-Bézout : « deux entiers a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$ ». Ce résultat est plus fort que le théorème fondamental.

Les manuels explorent plusieurs types de démarches pour présenter ces résultats. La plupart commencent par démontrer le théorème de Bachet-Bézout, soit par une procédure algorithmique permettant le calcul effectif des nombres u et v et utilisant l'algorithme d'Euclide, soit par un raisonnement plus abstrait (dont nous verrons des exemples plus loin). On en déduit ensuite le théorème de Gauss.

Un manuel s'intéresse d'abord aux propriétés du PGCD et en tire les théorèmes de Bachet-Bézout et Gauss de manière indépendante.

Les démarches sont assez diversifiées selon les manuels. Souvent le théorème de Bachet-Bézout y apparaît essentiel et, effectivement, il jouera un rôle important dans le développement ultérieur de l'algèbre. Mais ce n'est pas le cas dans la période que nous étudions ici, pour laquelle nous verrons que ce qui apparaît essentiel est le lemme d'Euclide ou le théorème de Gauss.

I.2. *Méthodes*

Nous avons aussi essayé de classer les méthodes que nous avons rencontrées dans les démonstrations arithmétiques étudiées. On les comprendra mieux à la lecture des textes, et nous les commenterons. Elles sont de deux types.

I.2.1 *Méthodes de tiroirs*

- « Principe des tiroirs » : Utilisation d'un nombre fini de tiroirs pour ranger des objets

1 La numérotation est celle de la traduction des *Eléments* de Peyrard [2]. Les propositions 26 et 32 dont il est question ici figurent dans le livre VII.

en nombre strictement supérieur : il y a donc au moins un tiroir contenant au moins deux objets. Ce résultat s'appelle « principe des tiroirs » (pigeonholes) ou « principe de Dirichlet ».

- « Disjonction des cas » : Partition des situations étudiées en un nombre fini de cas qu'on examine exhaustivement. C'est la méthode de « disjonction des cas ».
- « Mise en bijection » : Mise en bijection de deux ensembles finis de même cardinal.

I.2.2 *Méthodes d'escalier*

- « Descente finie » : Descente finie jusqu'à un entier convenable fournissant la conclusion soit directement soit par l'absurde.
- « Descente infinie » : Descente qui porte en elle-même sa contradiction parce qu'elle construit une suite infinie strictement décroissante d'entiers positifs. C'est la « méthode de descente infinie » de Fermat.
- « Raisonnement par récurrence »
- « méthode du plus petit élément » : Raisonnement utilisant le plus petit élément d'une partie non vide de N.

II. Quelques démonstrations historiques du Petit Théorème de Fermat

On rencontre ce théorème sous deux formes équivalentes :

> « Soit un nombre premier p et un entier a non divisible par p, alors p divise $a^{p-1} - 1$ »
>
> « Soit un nombre premier p et un entier quelconque a, alors p divise $a^p - a$ »

Il est énoncé sans démonstration par Fermat dans sa correspondance (en particulier dans la lettre à Frénicle du 18 octobre 1640). On en trouve une démonstration (publiée seulement en1863) dans les manuscrits de Leibniz.[2]

II.1 *EULER (1ère forme), LEGENDRE et GAUSS*

La première démonstration publiée, en 1736, est due à Euler. Celui-ci reprend la même idée en 1747, idée qu'on retrouve chez Legendre en 1798 [6]. Euler utilise le développement du binôme, une récurrence formalisée et le lemme d'Euclide. L'esprit de la démonstration est expliqué de façon concise par Gauss dans ses *Recherches Arithmétiques* en 1801 [5].

Commençons par le texte de Legendre (voir page suivante).

II.1.1 *LEGENDRE*

L'outil de départ est le développement du binôme.

Le lemme d'Euclide intervient dans le résultat sur la divisibilité des coefficients du binôme par l'entier premier p. Legendre démontre au début de son ouvrage le lemme d'Euclide, mais n'énonce jamais ni le théorème de Gauss, ni le théorème fondamental de l'arithmétique (existence et unicité de la décomposition en produit de facteurs premiers).

Pour conclure, Legendre utilise une descente finie jusqu'à l'entier convenable 0.

2 *Leibnizens Math. Schriften*, herausgegeben von G.J. Gerhardt, VII, 1863, 180-1 « nova algebrae promotio ». Traduite et commentée dans Mnémosyne 19.

§ I. *Théorèmes sur les nombres premiers.*

(129) Théorème. « Si c est un nombre premier, et N un nombre « quelconque non divisible par c, je dis que la quantité $N^{c-1}-1$ « sera divisible par c, de sorte qu'on aura $\frac{N^{c-1}-1}{c}$ = entier = e » (1).

Soit x un nombre entier quelconque, si on considère la formule connue

$$(1+x)^c = 1 + cx + \frac{c.c-1}{1.2}x^2 + \frac{c.c-1.c-2}{1.2.3}x^3 + \ldots + cx^{c-1} + x^c,$$

il est aisé de voir que tous les termes de cette suite, à l'exception du premier et du dernier, sont divisibles par c. En effet, soit M le coefficient de x^m; on aura $M = \frac{c.c-1.c-2.\ldots.c-m+1}{1.2.3.\ldots.m}$, ou $M.1.2.3\ldots m = c.c-1.c-2\ldots c-m+1$; et puisque le second membre est divisible par c, il faut que le premier le soit aussi. Mais l'exposant m, dans les termes dont il s'agit, ne surpasse pas $c-1$; donc c, qui est supposé un nombre premier, ne peut diviser le produit $1.2.3\ldots m$; donc il divise nécessairement M pour toute valeur de m depuis 1 jusqu'à $c-1$. Donc la quantité $(1+x)^c - 1 - x^c$ est divisible par c, quel que soit l'entier x.

Soit maintenant $1+x=N$, la quantité précédente deviendra $N^c-(N-1)^c-1$; et puisqu'elle est divisible par c, si on omet les multiples de c, on aura $N^c-1=(N-1)^c$, ou $N^c-N=(N-1)^c-(N-1)$. Mais en mettant $N-1$ à la place de N, et négligeant toujours les multiples de c, on aura semblablement $(N-1)^c-(N-1)=(N-2)^c-(N-2)$. Continuant ainsi de restes égaux en restes égaux, on parviendra nécessairement au reste $(N-N)^c-(N-N)$, lequel est évidemment zéro. Donc tous les restes précédents le sont; donc N^c-N est divisible par c.

Mais N^c-N est le produit de N par $N^{c-1}-1$, donc puisque N est supposé non divisible par c, il faudra que $N^{c-1}-1$ soit divisible par c; *ce qu'il fallait démontrer*

(1) Ce théorème, l'un des principaux de la théorie des nombres, est dû à Fermat; il a été démontré par Euler dans divers endroits des Mémoires de Pétersbourg, et notamment dans le tome I des *Novi commentarii*.

II.1.2 *EULER*

Dans la preuve d'origine, Euler utilise aussi la formule du binôme et le Lemme d'Euclide, mais comme il n'utilise pas l'« omission des multiples de c », la preuve est beaucoup plus longue. Pour la fin de la démonstration, il utilise une autre méthode que celle de Legendre :

corollaire 2

1. *C'est pourquoi, si on suppose que l'expression* $a^p - a$ *est divisible par p, l'expression* $(a+1)^p - a - 1$ *est aussi divisible par p, de la même manière sous la même hypothèse cette formule* $(a+2)^p - a - 2$ *et de là en continuant* $(a+3)^p - a - 3$ *etc. et généralement* $c^p - c$ *seront divisibles par p.*

théorème 3

2. Si p est un nombre premier, tout nombre de la forme $c^p - c$ sera divisible par p.

démonstration

Si […] on pose $a = 1$, comme $a^p - a = 0$ est divisible par p, il s'ensuit que ces formules également $2^p - 2$, $3^p - 3$, $4^p - 4$ etc . et généralement celle-ci $c^p - c$ seront divisibles par le nombre premier p. C.Q.F.D.

C'est une récurrence, que nous abrègerions peut-être aujourd'hui. Mais comme cette méthode n'était pas vraiment entrée dans les mœurs, Euler donne plus d'exemples que nécessaire — ce que nous faisons parfois avec nos élèves !

II.1.3 *GAUSS*

Nous avons une troisième formulation de cette preuve, résumée par Gauss dans ses Recherches Arithmétiques en 1801 [4]. Elle est très proche de celle d'Euler. Notons qu'il n'explique pas la première partie de la preuve, mais détaille l'induction.

Ce théorême remarquable, tant par son élégance que par sa grande utilité, s'appelle ordinairement *théorême de Fermat*, du nom de l'inventeur. (*Fermatii opera Math. Tolosæ* 1679. *Fol. p.* 163.) Fermat n'en a pas donné la démonstration, bien qu'il ait assuré qu'il l'avait trouvée. Euler en a le premier publié une dans la Dissertation intitulée : *Démonstration de quelques théorêmes relatifs aux nombres premiers.* (Comm. Ac. Pétrop. T. VIII) (*); elle est tirée du développement de $(a+1)^p$, qui fait voir par la forme des coefficiens, que $(a+1)^p - a^p - 1$ est toujours divisible par p, et que parconséquent $(a+1)^p - (a+1)$ le sera si $a^p - a$ l'est. Or comme $1^p - 1$ est divisible par p, $2^p - 2$ le sera donc ; et partant $3^p - 3$, et généralement $a^p - a$. Donc si p ne divise pas a, on aura aussi $a^{p-1} - 1$ divisible par p. Ce que nous venons de dire suffit pour faire connaître l'esprit de la démonstration.

II.2 *TANNERY*

On trouve une très jolie démonstration dans les conférences de Jules Tannery à l'Ecole Normale Supérieure en 1894 [1] Elle repose sur la méthode de mise en bijection :

Dans le cas où m est un nombre premier p, chaque nombre non divisible par p est premier à ce nombre : si donc dans l'expression ax où a n'est pas divisible par p on substitue $p - 1$ nombres x incongrus entre eux et à 0 (mod.p), on obtiendra $p - 1$ nombres congrus à ces mêmes nombres $x_1, x_2, \ldots x_{p-1}$ rangés dans un autre ordre ; le produit des nombres $ax_1, ax_2, \ldots ax_{p-1}$ est donc congru (mod p) au produit $x_1 x_2 \ldots x_{p-1}$, et comme le dernier produit est premier à p, on en conclut $a^{p-1} - 1 \equiv 0 \pmod{p}$.

C'est le célèbre *théorème de Fermat*, qui

joue, dans la théorie des nombres, un rôle essentiel et dont nous rencontrerons incidemment d'autres démonstrations ; observons qu'on en déduit immédiatement la proposition suivante : *quel que soit le nombre entier a et le nombre premier p, on a* $a^{p-1}-1 \equiv 0 \pmod{p}$.

Cette démonstration figure dans le document d'accompagnement des programmes de Terminale S et dans certains manuels. Notons l'emploi du mot « incongrus » pour deux nombres qui ne sont pas congrus modulo p.

La preuve repose sur une méthode de bijection. Elle révèle la puissance du Principe de Dirichlet, un principe qui apparaît si évident, et qui est utilisé ici sous son avatar de principe de bijection entre deux ensembles de même cardinal. Cette méthode évite tout recours à l'infini et la récurrence.

Le théorème Fondamental de divisibilité sert à montrer que $ax_1, ax_2, \ldots, ax_{p-1}$ sont tous différents et différents de 0 (mod p). Mais les règles de congruences évitent son explicitation.

La démonstration de Tannery est séduisante et élégante, par sa brièveté et la façon magistrale dont elle utilise les congruences. Son utilisation en classe, même si elle nécessite plus des six lignes de Tannery pour la faire comprendre à nos élèves de terminale, présente l'avantage qu'on peut appréhender cette démonstration dans sa totalité, sans avoir oublié à la fin de nos efforts les prémisses et le cheminement.

II.3 *EULER (2ème forme) et GAUSS*

En 1758 [3], Euler publie une démonstration du théorème de Fermat totalement différente, qui apparaît *a priori* plus longue et complexe, que nous détaillerons ci-dessous. Euler y utilise une classification des puissances de l'entier a selon leurs restes dans la division par le nombre premier p. La méthode consiste en des partitions en des nombres finis de tiroirs jusqu'à épuisement de l'ensemble considéré, couplée à l'utilisation du plus petit élément d'une partie non vide de **N**. Le théorème de base reste le lemme d'Euclide.

C'est cette démonstration que Gauss reprend dans ses *Recherches Arithmétiques* en 1801, mais avec un allègement dû au langage des congruences, et l'utilisation du « théorème de Gauss » qu'il démontre dans ce même ouvrage.

Pourquoi ce choix d'une démonstration *a priori* plus compliquée ?

Gauss reprend l'explication donnée par Euler lui-même : « *le développement de la puissance d'un binôme semble étranger à la théorie des nombres* ». La nouvelle démonstration respecte ainsi la « pureté de l'arithmétique ».

Reprenons cette démonstration : avant d'aborder la démonstration du théorème proprement dit, Euler explore les puissances de 7 modulo 641 :

> « Voici donc une méthode assez rapide pour trouver les restes qui proviennent de la division d'une puissance quelconque par un nombre quelconque. Par exemple si nous voulons chercher le reste qui provient de la division de 7^{160} par le nombre 641 :

Puissances	Restes	En effet puisque la première puissance 7 donne le reste 7 les puissances 7^2,7^3,7^4 donnent 49,343, et 478, c'est-à-dire –163, dont le carré 7^8 donne le reste 163^2 c'est-à-dire 288, et le carré de celui-ci 7^{16} donne le reste 288^2, c'est-à-dire 255. De même la puissance 7^{32} donne le reste 255^2 c'est-à-dire 284 et le reste de la puissance 7^{64} sera –110 et pour 7^{128} il vient 110^2 c'est-à-dire –79, reste qui multiplié par 284 donnera le reste de $7^{128+32} = 7^{160}$ qui sera 640 c'est-à-dire –1 .
7^1	7	
7^2	49	
7^3	343	
7^4	478	
7^8	288	
7^{16}	255	
7^{32}	284	
7^{64}	– 110	
7^{128}	– 79	
7^{160}	– 1	

Nous savions donc que, si la puissance 7^{160} était divisée par 641, le reste était 640 c'est-à-dire –1 , d'où nous concluons que le reste de la puissance 7^{320} est +1. Donc en général le reste de la puissance 7^{160n} divisée par 641 sera, soit +1 si n est un nombre pair, soit –1, si n est un nombre impair. »[3]

Après cette expérimentation sur des puissances particulières, Euler reprend son exploration dans le cas général. Rappelons que, étant donnés un nombre premier p et un nombre a non divisible par p, il s'agit de montrer que le reste de la division de a^{p-1} par p est 1. L'idée développée par Euler est de « classer » les puissances de a selon les $(p-1)$ restes non nuls possibles modulo p. Nous résumons ci-dessous les étapes de la démonstration.

Euler commence par montrer qu'il existe des puissances de a dont le reste est 1 : en effet, la suite a, a^2, a^3, a^4, … étant infinie et le nombre de restes non nuls possibles dans la division par p étant fini égal à $(p-1)$, il existe des puissances a^λ et a^μ , avec $\lambda < \mu$, présentant le même reste dans la division par p. Donc le nombre premier p divise $a^\mu - a^\lambda = a^{\mu-\lambda}(a^\lambda - 1)$. Comme p premier ne divise pas $a^{\mu-\lambda}$, p divise $a^\lambda - 1$, et le reste de la division de a^λ par p est bien 1.

On considère alors le plus petit entier λ strictement positif ayant cette propriété (le reste de la division de a^λ par p est 1) ; alors les λ puissances $1, a, a^2, a^3, \ldots, a^{\lambda-1}$ ont toutes des restes différents (non nuls) dans la division par p, sinon le raisonnement précédent donnerait un entier λ' plus petit que λ tel que p divise $a^{\lambda'} - 1$, ce qui est exclu. Si on obtient ainsi exactement les $(p-1)$ restes possibles non nuls modulo p, alors $\lambda = p - 1$ et le théorème est démontré.

Sinon, soit r un des restes non nuls qui n'a pas été obtenu . Notons que r est premier à p. On considère les λ nombres $r, ra, ra^2, ra^3, \ldots, ra^{\lambda-1}$; ces nombres ont tous des restes différents dans la division par p (sinon p diviserait $ra^\nu - ra^\mu = ra^{\nu-\mu}(a^\mu - 1)$ et donc $a^\mu - 1$ avec $\mu < \lambda$). De même, ra^μ et a^ν ne peuvent pas avoir le même reste sinon p diviserait $r - a^{\nu-\mu}$ ce qui est contradictoire avec le fait que r n'a pas été obtenu comme reste dans la division d'une puissance de a par p. En ajoutant ces restes aux précédents, nous obtenons ainsi 2λ restes non nuls différents modulo p ; si nous les avons tous, alors $(p-1) = 2\lambda$.

Sinon, on considère un reste s non encore obtenu et les nombres $s, sa, sa^2, sa^3, \ldots, sa^{\lambda-1}$. On montre de même que tous ces nombres ont des restes différents entre eux

3 Ce texte a été utilisé pour un devoir à la maison donné à des élèves « spécialistes » de Terminale S, assez tôt dans l'année, bien avant d'aborder le théorème de Fermat. Le texte de cet exercice se trouve au paragraphe IV.

et différents des restes obtenus précédemment. Si on a obtenu tous les restes non nuls possibles, alors $p - 1 = 3\lambda$.

Sinon, on continue… Le nombre de restes étant fini, le procédé doit s'arrêter . Quand on a obtenu tous les restes possibles, le même raisonnement prouve qu'il existe un entier t tel que : $p - 1 = t\lambda$.

Alors $a^{p-1} - 1 = a^{t\lambda} - 1 = (a^{\lambda})^{t} - 1$, or $x^{t} - 1$ est divisible par $x - 1$ pour tout entier x, car $x^{t} - 1 = (x-1)(x^{t-1} + x^{t-2} + ... + x + 1)$. Donc $a^{p-1} - 1$ est divisible par $a^{\lambda} - 1$. Comme p divise $a^{\lambda} - 1$, p divise aussi $a^{p-1} - 1$ et le théorème est démontré.

Ce raisonnement, en termes modernes, revient à faire une partition du groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ formée des classes d'équivalences selon le sous-groupe cyclique engendré par a. Ce type d'idée permet de démontrer le théorème de Lagrange : l'ordre d'un sous-groupe d'un groupe fini divise l'ordre de ce groupe.

Mais l'intérêt de cette démonstration n'est pas seulement d'ouvrir la voie à des développements ultérieurs ; malgré sa complexité, elle apparaît aussi comme relativement naturelle et résultant d'une exploration expérimentale des puissances d'un nombre.

En effet, la démonstration de Tannery, si convaincante et élégante, ne donne pas les raisons profondes de notre théorème. En ce sens, le détour par la démonstration d'Euler, reprise par Gauss, étudiant dans le détail le comportement des puissances d'un entier modulo p, est plus éclairante.

II.4 *FERMAT*

C'est d'ailleurs bien en termes de puissances que Fermat avait énoncé son théorème dans sa lettre à Frénicle du 18 octobre 1640 :

4. Il me semble après cela qu'il importe de vous dire le fondement sur lequel j'appuie les démonstrations de tout ce qui concerne les progressions géométriques, qui est tel :

Tout nombre premier mesure[4] *infailliblement une des puissances moins* 1 *de quelque progression que ce soit, et l'exposant de la dite puissance est sous multiple du nombre premier* –1 *; et après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.*

Exemple : *soit la progression donnée*

1	2	3	4	5	6
3	9	27	81	243	729

etc. avec ses exposants en dessus.

Prenez, par exemple, le nombre premier 13. *Il mesure la troisième puissance moins* 1, *de laquelle* 3, *exposant, est sous-multiple de* 12, *qui est moindre de l'unité que le nombre* 13, *et parce que l'exposant de* 729, *qui est* 6, *est multiple du premier exposant, qui est* 3, *il s'ensuit que* 13 *mesure aussi la dite puissance* 729 – 1.

Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

Il s'agit bien là semble-t-il de travailler sur les puissances d'un entier. Et le résultat

4 « mesure » signifie « divise ».

est plus précis que celui généralement appelé « théorème de Fermat », puisqu'on s'intéresse au plus petit entier λ tel que le nombre premier p divise $a^{\lambda}-1$. On aimerait connaître le cheminement de la pensée de Fermat, pour en arriver à ce qu'il appelle « le fondement sur lequel j'appuie les démonstrations de tout ce qui concerne les progressions géométriques »

Tous les auteurs insistent sur l'importance du théorème de Fermat et Euler se glorifie d'en donner la première démonstration en 1736. Le théorème de Fermat intervient de manière essentielle dans la recherche de la forme des diviseurs des nombres de Mersenne (2^n-1) et de Fermat ($2^{2^n}+1$), ainsi que pour d'autres problèmes comme la décomposition de nombres entiers en somme de carrés. Il existe également des réciproques partielles de ce théorème donnant des tests de primalité. Ainsi l'étude expérimentale des puissances d'un entier amène à la découverte, puis la démonstration d'un théorème intervenant dans diverses questions, dont certaines se révèlent actuellement primordiales : la primalité et le théorème lui-même étant à la base des méthodes modernes de cryptographie comme le système R.S.A..

III Commentaires et compléments

III.1 *Sur le théorème de Gauss et le calcul des congruences*

Il est bien connu que l'ouvrage de Gauss a joué un rôle central dans le développement de l'arithmétique. Euler et Legendre suivent la tradition euclidienne, même si Legendre donne une nouvelle preuve du Lemme d'Euclide dans sa *Théorie des Nombres* (1798).

De fait, Gauss ne fut pas le premier à publier le théorème de Gauss. Nous le trouvons dans *Les Nouveaux Elements de Mathematiques* de Jean Prestet, 2éme édition, 1689. Ce livre suscita peu d'intérêt car les mathématiciens de l'époque s'intéressaient plus à l' « Analyse Infinitésimale » qu'à l' « Analyse finie ».

Quoi qu'il en soit, Gauss commença à travailler le sujet dès 1795 « sans aucune idée de tout ce qui avait été fait sur le sujet », comme il l'explique dans sa préface. Il commence (Section I) par établir la théorie des congruences, puis (Section II) le théorème de Gauss, démontré par la méthode du plus petit élément et une preuve par l'absurde. Il explique pourquoi il démontre ce théorème : « 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, dans ce cas très simple, l'esprit de la méthode que nous appliquerons par la suite à des points bien difficiles. »

Gauss prouve ensuite l'unicité de la décomposition en nombres premiers. Il étudie les restes des puissances dans la Section III (où nous trouvons la preuve du petit Théorème de Fermat).

Gauss avait construit tous les outils, mais ce n'est sans doute pas un hasard s'il a fallu près d'un siècle après la publication du livre de Gauss pour qu'apparaisse une démonstration comme celle de Tannery, aussi brève que percutante. Il a fallu tout ce temps pour que la théorie des congruences, utilisée implicitement par Legendre en 1798, puis forma-

lisée par Gauss en 1801, soit complètement dominée.

Pour les professeurs, il est utile de prouver l'équivalence logique des différentes formes du théorème de divisibilité.

Le programme de Terminale S inclut le théorème de Bachet-Bézout. Ce dernier est plus fort que notre théorème fondamental de divisibilité. Son principe est donné par Bachet dans ses "*Problèmes plaisants et délectables*"(1624), et repris par Bézout dans son " *Cours d'Algèbre*" (1766). Toutefois, nous ne l'avons pas rencontré chez les auteurs étudiés. [5]

III.2 *Sur les méthodes*

La méthode de Dirichlet repose sur un concept que les élèves admettent sans difficultés, mais ne pensent pas à utiliser d'eux-mêmes. Nous pouvons leur montrer qu'elle permet de démontrer des résultats non triviaux. La disjonction des cas est très utile quand on travaille modulo un entier. Quand les élèves l'ont bien comprise, ils l'apprécient beaucoup et l'utilisent spontanément pour résoudre des exercices.

Par exemple, l'exercice de baccalauréat de Juin 2005 en Inde demandait de déterminer les nombres y tels que les nombres $x' = \frac{4y+4}{5}$ et $y' = \frac{2-3y}{5}$ soient des entiers. On peut faire une disjonction des cas modulo 5. Le tableau suivant :

y mod5	0	1	2	3	4
$4y+4$ mod5	4	3	2	1	0
$2-3y$ mod5	2	4	1	3	0

donne immédiatement le résultat : x' et y' sont entiers si et seulement si y est congru à 4 modulo 5.

La méthode de mise en bijection est également très utile lorsqu'on travaille modulo p. Lorsqu'on a p nombres distincts deux à deux strictement inférieurs à p $\{x_0, x_1, ..., x_{p-1}\}$ alors cela signifie que l'on a les p restes possibles dans la division par p, à l'ordre près, $\{0,1,...,p-1\}$.

La diversité des méthodes d'escalier mérite un examen plus approfondi. Nous pouvons nous demander, sur le plan historique et épistémologique, pourquoi les mathématiciens utilisent l'une ou l'autre.

L'origine de la méthode par récurrence est généralement attribuée à Pascal (même si on la rencontre avant, chez Maurolycus, par exemple). Toutefois son utilisation n'est pas encore naturelle à l'époque d'Euler, et même de Gauss. Cette méthode est au programme en secondaire actuellement, et l'on comprend pourquoi elle n'est pas si facile pour les élèves.

Fermat préfère sa méthode de descente infinie bien qu'elle soit fortement critiquée par Wallis et d'autres. Plus tard, Euler et Gauss, bien qu'ils lisent Fermat très attentivement, ne la reprennent pas. La méthode de descente finie évite le recours à l'infini, souvent au prix d'un raisonnement par l'absurde (ce n'est pas le cas dans la démonstration de Legendre). Notons que cette méthode se traduit directement en algorithme.

La méthode du plus petit élément évite aussi l'infini et donne une élégante et concise rédaction. C'est pourquoi elle rencontre un certain succès chez les étudiants en Post-Bac.

5 Voir [9]

La preuve de l'équivalence de ces méthodes est un bon exercice de logique.

IV. *L'arithmétique dans nos classes.*

L'étude des textes nous permet de mieux comprendre les différentes méthodes de démonstration, leur intérêt, leurs liens. Par exemple, les lettres de Fermat et les textes d'Euler montrent l'intérêt d'une exploration des puissances d'un entier donné avant des développements futurs et la présentation du théorème de Fermat.

Nous vous proposons d'abord un devoir à la maison pour Terminales S, utilisant le début de la seconde preuve d'Euler. Euler y étudie les restes des puissances de 7 dans la division par 641.[6] Il est intéressant de montrer aux élèves une démarche exploratoire de la part d'un mathématicien et de les faire travailler sur ce texte. Notons que le langage d'Euler n'est pas tout à fait le nôtre, et, pour travailler avec des nombres les plus petits possibles en valeur absolue, il accepte des restes négatifs (entre –320 et +320).

La version donnée ici est une version exploitant les possibilités d'exploration sur tableur (partie III), donnée aux élèves en octobre 2007.

Un devoir à la maison en terminale S spécialité maths

Dans un article publié en 1758*, Euler s'intéresse aux restes des puissances de* 7 *modulo* 641.

Préambule : lire le texte ci-dessous en vérifiant tous les calculs d'Euler. Vous écrirez sur la copie tous les calculs nécessaires à cette vérification, sans justification. Tous les calculs d'Euler sont-ils nécessaires pour obtenir le reste de 7^{160} (expliquez votre réponse) ?

« Voici donc une méthode assez rapide pour trouver les restes qui proviennent de la division d'une puissance quelconque par un nombre quelconque. Par exemple si nous voulons chercher le reste qui provient de la division de 7^{160} par le nombre 641 :

Puissances	Restes
7^1	7
7^2	49
7^3	343
7^4	478
7^8	288
7^{16}	255
7^{32}	284
7^{64}	– 110
7^{128}	– 79
7^{160}	– 1

En effet puisque la première puissance 7 donne le reste 7 les puissances 7^2,7^3,7^4 donnent 49,343, et 478, c'est-à-dire –163, dont le carré 7^8 donne le reste 163^2 c'est-à-dire 288, et le carré de celui-ci 7^{16} donne le reste 288^2, c'est-à-dire 255. De même la puissance 7^{32} donne le reste 255^2 c'est-à-dire 284 et le reste de la puissance 7^{64} sera –110 et pour 7^{128} il vient 110^2 c'est-à-dire –79, reste qui multiplié par 284 donnera le reste de $7^{128+32} = 7^{160}$ qui sera 640 c'est-à-dire –1 .

6 Nous soupçonnons Euler d'avoir choisi d'étudier les puissances de 7 modulo 641 parce que 641 est un facteur premier qu'il a rencontré dans son étude des nombres de Fermat.

Nous savions donc que, si la puissance 7^{160} était divisée par 641, le reste était 640 c'est-à-dire –1, d'où nous concluons que le reste de la puissance 7^{320} est +1. Donc en général le reste de la puissance 7^{160n} divisée par 641 sera soit +1 si n est un nombre pair, soit –1, si n est un nombre impair. »

Partie I : étude du texte d'Euler.

1. Justifiez le remplacement de 478 par –163 et expliquez l'intérêt pratique de cette démarche.
2. Citez le résultat du cours utilisé pour le calcul du reste de 7^8.
3. Justifiez le résultat donné pour le reste de la division de 7^{320} par 641 ainsi que celui de la division de 7^{160n} par 641 ?
4. Quel est le reste de la division de 7^{320n} par 641 ? Déterminer, en utilisant les résultats d'Euler et sans calculs supplémentaires, le reste de la division de 7^{648} par 641.
5. On appelle r_n le reste de la division de 7^N par 641. Montrer que cette suite est périodique.
6. Donner une méthode pour le calcul du reste de la division de 7^N par 641.

Partie II : et pour d'autres modules que 641 ?

1. Calculer les restes de 7, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7 dans la division par 63.
2. Montrer que la suite (r_n) des restes de la division de 7^N (pour N entier strictement positif) par 63 est périodique. Quel est le reste de la division de 7^9par 63 ?
3. On considère un nombre entier strictement positif m. La suite des restes de la division de 7^N par m est-elle toujours périodique ?
4. Euler constate que le reste de la division de 7^{320} par 641 est égal à 1. Existe-t-il un entier h strictement positif tel que le reste de la division de 7^h par m est égal à 1 pour tout entier m strictement positif ?

Vous justifierez soigneusement vos réponses aux questions 3 et 4.

Partie III : un résultat général

1. Programmez votre tableur pour obtenir les restes de 7^n dans la division par différents entiers a. Pour cela, vous écrirez « n » dans la cellule A1 et vous obtiendrez dans la colonne A les entiers de 1 à 100 ; vous écrirez « a = » dans la cellule D1 et choisirez une valeur de a dans la cellule E1. Dans la colonne B, obtenez les restes de 7^n dans la division par a. Dans la colonne C, programmez un test pour écrire « gagné » lorsque ce reste est 1.
2. *Conjecture :* après avoir essayé suffisamment de valeurs de a pour avoir une idée convaincante, conjecturez une condition nécessaire et suffisante portant sur 7 et a pour qu'il existe un entier n strictement positif tel que $7^n \equiv 1 \pmod{a}$.

3. *Démontrez votre conjecture* (dans un sens) : commencez par montrer : s'il existe un entier n strictement positif tel que $7^n \equiv 1 \pmod{a}$, alors …

4. La réciproque est plus difficile. Commencez par démontrer que, sous la condition trouvée, il existe un nombre u tel $7u \equiv 1 \pmod{a}$. Justifier alors l'existence de deux entiers naturels distincts m et k (avec $k > m$) tels que $7^k \equiv 7^m \pmod{a}$. En multipliant cette congruence par u^m, concluez.

5. Pouvez-vous conjecturer ce qui se passe pour les restes de la division de b^n par un entier a dans le cas général ?

La lecture du texte permet de voir si les élèves ont bien compris les notions élémentaires sur les congruences ; la question 5 de la partie II étudie une question classique du cours de Terminale S (spécialité « mathématiques »). La partie II continue l'exploration des puissances de 7, modulo 63 cette fois-ci.

L'idée qu'on veut dégager est, d'une part la périodicité des restes des puissances de 7 modulo un entier m, d'autre part la condition sous laquelle il existe n entier non nul tel que $7^n \equiv 1 \pmod{m}$. Il est d'ailleurs assez simple sur un tableur d'explorer la situation avec divers nombres m et de conjecturer le résultat suivant :

$$\exists n \in N^* \quad tel\ que\ 7^n \equiv 1 \pmod{m} \Leftrightarrow PGCD(7,m) = 1$$

Le théorème de Bézout suffit à montrer l'implication dans un sens et la démonstration de celle-ci est à la portée des élèves. Cependant, la démonstration de la réciproque est plus subtile ; elle peut être comprise des élèves, mais plus difficilement trouvée au niveau TS.

Le principe des tiroirs montre qu'il existe n_1 et n_2 avec $n_1 > n_2$ tels que $7^{n_1} \equiv 7^{n_2} \pmod{m}$.

Comme PGCD(7,m)=1, il existe deux entiers relatifs u et v tels que $7u + mv = 1$, donc on a : $7u \equiv 1 \pmod{m}$. Si r est le reste de la division de u par 7, on a aussi : $7r \equiv 1 \pmod{m}$ avec cette fois-ci un entier naturel r (non nul). Comme $7^{n_1} \equiv 7^{n_2} \pmod{m}$, on a aussi : $7^{n_1} \times r^{n_2} \equiv 7^{n_2} \times r^{n_2} \equiv (7r)^{n_2} \equiv 1^{n_2} \equiv 1 \pmod{m}$; mais, comme $n_1 - n_2 > 0$, on peut écrire : $7^{n_1} \times r^{n_2} \equiv 7^{n_1-n_2} \times 7^{n_2} \times r^{n_2} \equiv 7^{n_1-n_2} \pmod{m}$ donc finalement $7^{n_1-n_2} \equiv 1 \pmod{m}$.

Ce qui est sous-jacent à cette démonstration, c'est la notion de groupe et l'utilisation de l'inverse de 7 dans le groupe des éléments inversibles de l'anneau $\mathbf{Z} / m\mathbf{Z}$, groupe habituellement noté $(\mathbf{Z} / m\mathbf{Z})^*$.

On peut aussi remarquer lors de l'exploration sur tableur que, lorsque m est premier, le plus petit entier n non nul tel que $7^n \equiv 1 \pmod{m}$ est un diviseur de $m - 1$, et donc que, dans ce cas, $7^{m-1} \equiv 1 \pmod{m}$, alors que, si m n'est pas premier, ce n'est pas toujours le cas. On pourra bien sûr revenir sur ces considérations au moment d'introduire et de démontrer le petit théorème de Fermat, et disposer immédiatement de contre-exemples montrant que sa réciproque est fausse.

Les élèves ont été intéressés par ce problème. Ils ont bien réussi la partie I ; les démonstrations de la partie II leur ont paru

plus ardues et ils ont posé des questions en cours à ce sujet. L'utilisation du principe des tiroirs, qu'ils comprennent pourtant bien, n'est pas si aisée.

L'exploration des puissances d'un entier a un côté fascinant, car outre qu'elle est facile à mener, elle fait sentir qu'on tient là des résultats généraux, une méthode infaillible pour déterminer les restes de a^n modulo un entier m.

Les différents types de démonstrations que nous avons rencontrées ainsi que le théorème Fondamental de divisibilité (souvent sous la forme « théorème de Gauss ») se retrouvent fréquemment dans la résolution d'exercices du baccalauréat, voire dans les exercices donnés au Concours général. Nous donnons ci-dessous un exercice donné en Juin 2006 (avec son corrigé, qui utilise un bon échantillon des méthodes que nous avons exposées) .

Le premier exercice du Concours général de Mathématiques 2006

Si n est un entier naturel strictement positif, on note $\overline{a_i a_{i-1}\ldots a_1 a_0}$ son écriture décimale. On a donc $n = 10^i a_i + 10^{i-1} a_{i-1} + \ldots + 10a_1 + a_0$, les entiers a_j, $0 \leq j \leq i$, sont compris entre 0 et 9 et $a_i \neq 0$. On désigne par q un entier compris, au sens large, entre 1 et 9, et on pose $p = 10q - 1$ et l'on considère la fonction

$$f_q(n) = \overline{a_i a_{i-1}\ldots a_1} + qa_0 \ .$$

Si $i = 0$, alors $f_q(n) = qn$. Enfin, l'entier q étant fixé, on associe à tout entier n la suite (n_k) définie par les relations :

$$n_0 = n \quad \text{et} \quad \forall\, k \in \mathbf{N},\ n_{k+1} = f_q(n_k) \ .$$

Par exemple, si $q = 5$, la suite associée à 4907 est 4907, 525, 77, 42, 14, 21, 7, 35, 28, 42, 14, …

1. Vérifier que $f_q(n) = \dfrac{n + pa_0}{p}$. En déduire que $f_q(p) = p$.

2. (a) Montrer que, si $m > p$ alors $f_q(m) < m$.
   (b) En déduire que pour tout entier n, il existe un entier j tel que $n_j \leq p$.

3. (a) Montrer que si $m < p$ alors $f_q(m) < p$.
   (b) En déduire que pour tout entier n, la suite (n_k) est périodique à partir d'un certain rang, c'est-à-dire qu'il existe k et T entiers tels que $n_{j+T} = n_j$, pour tout $j \geq k$.

4. Etablir que, pour tout entier n, $f_q(n)$ est congru à qn modulo p.

5. Pour quelles valeurs de q la fonction f_q a-t-elle des points fixes (c'est-à-dire des entiers m tels que $f_q(m) = m$) autres que p ? Quels sont alors ces points fixes ?

6. Montrer que, pour des choix convenables de q, l'étude de la suite (n_k) associée à un entier n fournit des critères de divisibilité de n par 9, 19, 29, 13, 49 et 7. Enoncer ces critères.

Corrigé :

Question 1.

$$f_q(n) = \frac{n - a_0}{10} + qa_0$$

$$f_q(n) = \frac{n + a_0(10q - 1)}{10}$$

$$f_q(n) = \frac{n + pa_0}{10}$$

Dans le cas où $p = n$, on remarque que, comme $p = 10q - 1$, on a : $p \equiv -1 \equiv 9 \pmod{10}$, donc le chiffre des unités de p est $a_0 = 9$. Donc :

$$f_p(p) = \frac{p + pa_0}{10} = \frac{p + 9p}{10} = p$$

Question 2.

a. Si $m > p$, alors $f_q(m) = \frac{m + pa_0}{10} < \frac{m + ma_0}{10}$.

Or $\frac{m + ma_0}{10} = m\frac{a_0 + 1}{10} \leq m$ car $a_0 \leq 9$. Donc on a bien $f_q(m) < m$.

b. La question 2.b se résout, soit par la méthode de descente infinie, soit par la méthode du plus petit élément.

Descente infinie : On suppose que pour tout entier j, on a : $n_j > p$. Alors, on a : pour tout entier j, $f_q(n_j) < n_j$ (d'après 2.a), c'est-à-dire $n_{j+1} < n_j$. La suite (n_j) est alors une suite infinie strictement décroissante d'entiers naturels. Ce qui est impossible. Donc il existe j dans **N** tel que $n_j \leq p$.

MPPE : On suppose que pour tout entier j, on a : $n_j > p$. Soit n_m le plus petit élément de l'ensemble des valeurs de la suite (n_k). Alors, comme $n_m > p$, on a : $f_q(m) < n_m$, c'est-à-dire $n_{m+1} < n_m$. Ce qui est contradictoire avec le fait que n_m est le plus petit des éléments de l'ensemble des valeurs de la suite.

Question3 . a.Si $m < p$, alors on a $f_q(m) = \frac{m + pa_0}{10} < \frac{p + pa_0}{10} \leq p$. Donc on a bien : $f_q(m) < p$.

b. La question 3.b se résout par une récurrence suivie d'un principe des tiroirs.

On sait par la question précédente qu'il existe un entier j tel que $n_j \leq p$. La récurrence, très rapide, sert à montrer que, pour tout $k \geq j$, $n_k \leq p$.

Comme la suite extraite (n_k), avec $k \geq j$, comprend une infinité de termes qui ne peuvent prendre qu'un nombre fini de valeurs $\{1, 2, 3, \ldots, p - 1\}$, il existe k et k', avec $k < k'$, tels que $n_k = n_{k'}$ *(principe des tiroirs)*. La suite est alors périodique de période $k' - k$ à partir du rang k.

Question 4. La question 4. utilise les théorèmes de Gauss et de Bézout.

$10f_q(n) = n + pa_0 \equiv n \pmod{p}$.

Comme $p = 10q - 1$, on a : $10q \equiv 1 \pmod{p}$et donc $10f_q(n) \equiv 10qn \pmod{p}$. Donc p divise $10(f_q(n) - qn)$. Or p et 10 sont premiers entre eux car $10q - p = 1$ (théorème de Bézout) ; donc, par le théorème de Gauss, p divise $f_q(n) - qn$.

Question 5. (utilisation de la disjonction des cas).

$$f_q(m) = m \Leftrightarrow m + pa_0 = 10m \Leftrightarrow 9m = pa_0$$

• Si $q = 1$, alors $p = 9$ et m fixe $\Leftrightarrow m = a_0$. Dans ce cas, il y a donc huit points fixes autres que p : 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 .

• Si $q = 4$, alors $p = 39$ et m fixe $\Leftrightarrow 3m = 13a_0$. Comme 3 est premier avec 13, 3 divise a_0 *(théorème de Gauss)*, donc $a_0 = 3$ ou 6, ce qui donne deux points fixes : $m = 13$ ou $m = 26$.

• Si $q = 7$, alors $p = 69$ et m fixe $\Leftrightarrow 3m = 23a_0$. Comme 3 est premier avec 23, 3 divise a_0 *(théorème de Gauss)*, donc $a_0 = 3$ ou 6, ce qui donne deux points fixes : $m = 23$ ou $m = 46$.

• Si q est différent de 1, de 4 et de 7, alors p et 9 sont premiers entre eux. Donc, si m est fixe, 9 divise a_0 , c'est-à-dire $a_0 = 9$ et $m = p$; dans ce cas, il n'y a pas de point fixe autre que p.

Question 6. $10 f_q(n) = n + pa_0$

Donc : p divise $n \Leftrightarrow p$ divise $10 f_q(n) \Leftrightarrow p$ divise $f_q(n)$, car p et 10 sont premiers entre eux *(théorème de Gauss)*.

Ainsi, dans la suite (n_k) associée à un entier n, ou bien tous les termes sont divisibles par p, ou bien aucun ne l'est.

Le choix de $q = 1$ donne ainsi un critère de divisibilité par $p = 9$: on écrit la suite (n_k) associée à un entier n, les termes finissent par être plus petit que p et il est ainsi aisé de savoir s'il sont divisibles par $p = 9$. Le premier terme de la suite étant n, ceci répond à la question de la divisibilité de n par 9.

De même, les choix de $q = 2$ ou 3 ou 5 donnent des critères de divisibilité par 19 ou 29 ou 49.

Pour $q = 5$, on a $p = 49 = 7 \times 7$ donc :

$$10 f_q(n) = n + 7^2 a_0$$

Donc : 7 divise $n \Leftrightarrow 7$ divise $10 f_q(n) \Leftrightarrow 7$ divise $f_q(n)$ car 7 et 10 sont premiers entre eux. Ainsi, le choix $q = 4$ donne également un critère de divisibilité par 7. Ainsi, pour l'exemple donné par l'énoncé ($n = 4907$), il est visible que les pls petits termes sont divisibles par 7, donc tous les termes de la suite le sont et en particulier 4907 est divisible par 7.

De même, le choix de $q = 4$ donne un critère de divisibilité par 13 car alors $p = 3 \times 13$.

Bibliographie

BATTIE Véronique. *Spécificités et potentialités de l'Arithmétique élémentaire pour l'apprentissage du raisonnement mathématique* (Thèse). Paris : Irem Paris 7, 2004.

BUHLER Martine et MICHEL-PAJUS Anne. « Sur différents types de démonstrations rencontrées spécifiquement en arithmétique » in *Mnémosyne* 19. Paris : Irem PARIS7.

CHABERT Jean-Luc *et al.*. *Histoire d'algorithmes*. Paris : Belin, 1994.

DELAHAYE Jean-Paul. *Merveilleux nombres premiers*. Paris : Belin-Pour la Science, 2000.

GOLDSTEIN Catherine. *Un théorème de Fermat et ses lecteurs*. Presses Universitaires de Vincennes, 1995

GOLDSTEIN Catherine. « Le métier des nombres aux XVIIème et XIXèmes siècles ». In *Eléments d'Histoire des Sciences*, Serres Michel (dir.). Paris : Larousse-Bordas, 1997.

I.R.E.M. Groupe Epistémologie et Histoire. *Mathématiques au fil des âges*. Paris : Gauthier-Villars, 1987.

Textes sources :

[1] BOREL Emile et DRACH Jules. *Introduction à l'étude de la Théorie des Nombres et de l'Algèbre*, d'après les conférences de Jules Tannery à l'Ecole Normale Supérieure. Paris : Librairie Nony et Cie, 1894.

[2] EUCLIDE. *Les Elements*, Traduction du grec par F. PEYRARD. Paris : C.F. Patris,1819. Réédition : Paris, Blanchard,1966.

[3] EULER Leonhard . « Théorèmes sur les restes laissés par la division des puissances ». In *Nouveaux mémoires de l'Académie de Saint Petersbourg* ,T.7, (1758/9, 1761, p.49-82). Réed. *L.Euleri Commentiones Arithmeticae* , T. 1. Rudio, Lipsiae et Berolini : 1915. Traduction libre.

[4] FERMAT Pierre de. *Œuvres,* T.II et III, Tannery et Henry (ed.). Paris : §§ 1896.

[5] GAUSS Friedrich, *Recherches Arithmétiques*, Traduction Poullet-Delisle. Paris : Courcier 1807. Réédition Paris : Blanchard,1979. (Edition latine : 1801).

[6] LEGENDRE André-Marie, *Théorie des Nombres*. Paris : Firmin-Didot, 1830. Réédition Paris : Blanchard, 1955.