Sur différents types de démonstrations rencontrées spécifiquement en arithmétique.

Martine Bühler et Anne Michel-Pajus

[De] Qual ieu ay fach, las flors venes pilhar
Lo rest laysar, si non fassa par vos [1]

Un des aspects intéressants de l'arithmétique est qu'elle porte sur des objets, les entiers, facilement accessibles par l'intuition. Sans avoir besoin d'un grand arsenal théorique, on peut y faire de véritables démonstrations mathématiques, s'appuyant sur des raisonnements d'une certaine finesse, et obtenir des résultats non triviaux. Ceci donne à l'arithmétique un caractère formateur spécifique dans l'apprentissage de la démonstration.

Nous avons limité notre analyse à des textes qui proposent explicitement une démonstration ; ce qui exclut plusieurs siècles d'arithmétique que nous nous contenterons de survoler, en limitant notre étude à des textes écrits entre le 18ème et le 20ème siècle.

Nous avons par ailleurs choisi comme point de départ le « petit théorème de Fermat » parce qu'il figure dans les nouveaux programmes de Terminale S (spécialité) et les textes présentés ne dépassent généralement pas ce niveau.

La première partie repère brièvement les méthodes de démonstration choisies dans quelques documents pédagogiques récents.

Dans un second temps nous présentons une mise en perspective plus large de certaines questions que nous serons amenées à évoquer, et nous détaillons nos outils d'analyse : les quatre types d'occurrence du Théorème Fondamental de l'Arithmétique d'une part, une classification des types de raisonnement, d'autre part.

La troisième partie propose l'analyse, selon notre grille, de trois extraits de démonstrations du « petit théorème de Fermat ».

La quatrième partie regroupe des textes autour de la « méthode de descente infinie » de Fermat et de ses variantes.

La cinquième partie reprend l'étude des différentes formes du théorème fondamental, mais sous un point de vue historique, en pointant leur introduction et les démonstrations d'implications entre quatre énoncés de ce théorème.

Ainsi, le bagage théorique de base peut se limiter à une seule propriété, mais celle-ci apparaît sous des formes différentes selon les points de vue. Certaines façons de raisonner se retrouvent tout au long de l'histoire, sous des formes plus ou moins formalisées. Nous proposons dans cet article une classification de cette multiplicité d'approches, que nous espérons éclairante pour les enseignants.

[1] [De] ce que j'ai fait, venez piller les fleurs, Laissez le reste, s'il n'est fait pour vous.
Concours : la première personne qui nous donnera la référence exacte de cette citation (extraite d'un ouvrage de mathématiques) gagne le prochain numéro de *Mnémosyne*…

I. Les choix des programmes et des manuels de Terminale S (spécialité mathématiques) en 2002

Le programme comporte entre autres résultats l'existence et l'unicité de la décomposition en produit de facteurs premiers (dont l'unicité « pourra être admise »), et les théorèmes de Bézout et Gauss (avec comme « application : petit théorème de Fermat »). Le document d'accompagnement des programmes ne donne pas de clés pour les démonstrations des théorèmes de Bézout et Gauss, mais relie le résultat de Bézout à la recherche des points à coordonnées entières sur une droite. Par contre, trois démonstrations sont proposées pour le petit théorème de Fermat : celle de Tannery (voir supra page 28), celle utilisant le développement du binôme (avec une descente jusqu'à un entier convenable comme dans le cours de Legendre), et une démonstration combinatoire dénombrant les différents coloriages possibles d'un polygone régulier à p sommets (voir annexe 5).

Dans les manuels que nous avons consultés, nous avons trouvé trois types de démarches. Dans certains manuels (Collection Math x, Didier ; collection Hyperbole, Nathan), on commence par démontrer, par remontée de l'algorithme d'Euclide, que, si d = PGCD(a,b), alors il existe u et v entiers relatifs tels que $au + bv = d$, puis que l'ensemble des nombres de la forme $au + bv$, avec u et v entiers relatifs, est l'ensemble des multiples de d. On en tire comme cas particulier le théorème de Bézout (a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au + bv = 1$), puis, comme conséquence du théorème de Bézout, le théorème de Gauss : si a divise bc et si a est premier avec b, alors il existe des entiers relatifs u et v tels que $au + bv = 1$, donc $acu + bcv = c$; comme a divise acu et bc, alors a divise c.

D'autres manuels (Collection Indice, Bordas ; collection Transmath, Nathan ; collection Terracher, Hachette) démontrent le théorème de Bézout par une méthode combinant l'utilisation du plus petit élément d'une partie non vide de N et division euclidienne. On considère deux nombres entiers a et b premiers entre eux. L'ensemble E des nombres entiers naturels non nuls de la forme $au + bv$, avec u et v entiers relatifs, n'est pas vide, car il contient les multiples strictement positifs de a et b. Il admet donc un plus petit élément d, qui est strictement positif. On effectue la division euclidienne de a par d : $a = dq + r$ où $0 \leq r < d$ et on sait que $d = au_0 + bv_0$, avec u_0 et v_0 entiers relatifs. On a alors : $r = a - dq = au + bv$ avec $u = 1 - u_0q$ et $v = -v_0q$. Comme d est le plus petit élément strictement positif de E, $r = 0$, donc d divise a. On démontre de même que d divise b. Donc $d = 1$. On vient de montrer que, si deux nombres entiers a et b sont premiers entre eux, il existe u et v entiers relatifs tels que $au + bv = 1$. La réciproque est évidente. On en tire le théorème de Gauss comme ci-dessus.

Enfin, un dernier manuel (Collection Fractale, Bordas) s'intéresse d'abord aux propriétés du PGCD. Il énonce sans démonstration les propriétés suivantes :

si a et b sont des entiers et k un entier naturel non nul, alors PGCD(ka,kb) = kPGCD(a,b).

si d est un entier naturel diviseur commun de a et b, $PGCD(\frac{a}{d},\frac{b}{d}) = \frac{1}{d} PGCD(a,b)$.

D'où on tire que tout diviseur commun de a et b divise leur PGCD.

On donne ensuite la propriété suivante : si d = PGCD(a,b), alors il existe u et v entiers relatifs tels que $au + bv = d$. La propriété est montrée sur un exemple numérique considéré comme générique, en remontant l'algorithme d'Euclide. On en tire le théorème de Bézout.

La démonstration du théorème de Gauss est indépendante du théorème de Bézout : si a et b sont deux nombres premiers entre eux tels que a divise bc, alors PGCD(ac,bc) = cPGCD(a,b) = c. Comme a est un diviseur commun de ac et bc, il divise leur PGCD, c'est-à-dire c.

On remarque des démarches très diversifiées dans les différents manuels, ce qui montre l'intérêt des différentes approches. Ce qui apparaît essentiel est le théorème de Bézout. Ce théorème jouera un rôle important dans le développement ultérieur de l'algèbre, en liaison avec la notion d'anneau principal, mais pas dans la période que nous étudions ici. C'est pourquoi il n'apparaît pas dans l'étude des textes proposée ici.

II. 1. Un survol historique de travaux en arithmétique

Les considérations sur pair-impair, multiples, nombres premiers nous viennent probablement de l'école de Pythagore. Cependant, on ne possède aucun texte des Pythagoriciens. On connaît ce courant par l'œuvre des néo pythagoriciens Nicomaque de Gérase et Théon de Smyrne (II^{ème} siècle après J.-C.). Le premier a écrit une *Introduction Arithmétique*[2], dans laquelle on trouve des considérations sur pair-impair, nombres figurés, crible d'Eratosthène. Le second a également écrit une *Arithmétique*[3] destinée à assister la lecture des textes de Platon. Chez aucun des deux on ne trouve de véritable démonstration au sens d'une suite de propositions logiquement articulées les unes aux autres comme celles qu'on trouve chez Euclide, Apollonius ou Archimède. Par contre, on y voit très nettement un effort original, soit pour expliquer la formation ou les propriétés de certaines séries de nombres à partir de dispositions géométriques des unités composant un entier en figures[4], soit pour subordonner la formation de certaines séries de nombres à d'autres séries considérées comme plus simples ou plus fondamentales.[5] Cette tradition a eu une influence extrêmement grande sur la pensée antique et médiévale : dans la tradition grecque elle-même, elle a contribué chez les néoplatoniciens tardifs comme Jamblique, Syrianus ou Proclus à leur définition de la « mathématique générale », notion qui a eu à son tour une grande importance à la Renaissance. Le moyen-âge latin a étudié ce type d'arithmétique au travers de la traduction très influente que Boèce a donné de Nicomaque ; dans le Moyen-Age arabe, ce texte a également été traduit assez tôt et a donné lieu à des développements originaux, qui visaient notamment à fonder par des démonstrations géométriques certaines démarches néopythagoriciennes.[6]

La civilisation chinoise a laissé des travaux arithmétiques, dont le célèbre théorème des restes, dont le nom vient du problème 26 du chapitre 3 du *Sunzi Suanjing* (Manuel Mathématique du Maître Sun) datant environ du quatrième siècle de notre ère. On y trouve des règles de résolution sans explicitation des démonstrations au sens euclidien du terme, mais avec des commentaires sur leur raison d'être, leur validité, etc..[7]

Les *Eléments* d'Euclide (III^{ème} siècle avant J.C.) restent une source importante sur les connaissances des Grecs en arithmétique. Ce traité est essentiellement géométrique, mais contient néanmoins trois livres consacrés à l'arithmétique, présentant des définitions et des

[2] Nicomaque de Gérase, *Introduction Arithmétique* , Trad. J. Bertier, Vrin, 1978

[3] J.Dupuis, *Ce qui est utile en mathématiques pour la lecture de Platon*, Bruxelles, 1966

[4] C'est ce qu'on appelle couramment les nombres figurés. Pour comprendre l'esprit de l'exposé de Théon de Smyrne sur ce sujet, on pourra se reporter à l'extrait traduit dans ce même numéro dans les 'bonnes vieilles pages'.

[5] Ce type de conception de l'arithmétique, qui n'est pas vraiment dissociable du sens philosophique étendu que ces auteurs lui donnaient initialement, est un des grands ancêtres antiques de la pensée mathématique moderne et du rôle prépondérant qu'y joue l'arithmétique des nombres entiers.

[6] Sur ce point voir le résumé sur le développement de l'arithmétique arabe dans *Histoire des Sciences Arabes*, vol.2, dir. R. Rashed, Seuil 1997, pp.21-29 et 85-91, et la traduction de quelques textes significatifs des efforts de démonstration dans R. Rashed, *Entre arithmétique et algèbre*, Belles Lettres 1984, *L'induction mathématique : al-Karaji, as-Samaw'al*, pp.71 seq.

[7] Voir *Les neuf chapitres* édités et commentés par K. Chemla et G. Shuchun, Dunod 2004 et J.C. Martzloff, *Histoire des mathématiques chinoises*, Masson, 1987.

propositions sur les nombres, avec des démonstrations fondées sur un raisonnement hypothetico-déductif.

Diophante d'Alexandrie, dont on connaît peu de choses (il a vécu entre le II^{ème} siècle avant J.-C. et le IV^{ème} siècle après J.-C.), a écrit une œuvre originale. Ses *Arithmétiques* comportaient au départ 13 livres[8], qui présentent des problèmes sur les nombres et des méthodes novatrices pour les résoudre. Ils ont été traduits en arabe par un algébriste, ce qui explique la manière dont les arabes ont majoritairement lu Diophante et utilisé l'outil algébrique pour résoudre les problèmes diophantiens. Un autre courant, initié en particulier par al-Khazin, a développé une arithmétique entière sans algèbre.

On retrouve ces deux tendances aux XVI^{ème} et XVII^{ème} siècles en Occident. Diophante, longtemps oublié en Occident, est redécouvert à la Renaissance par six des treize livres des *Arithmétiques*. Bombelli incorpore des problèmes de Diophante dans l'édition de *l'Algebra* de 1572. En Allemagne, à la même époque, Xylander publie une traduction en latin de Diophante (1575). La nouvelle algèbre de Viète emprunte beaucoup à Diophante. Enfin, Bachet de Méziriac donne en 1621 une édition bilingue en grec et en latin de ces six livres retrouvés. C'est cette édition que lit et annote Fermat, donnant ainsi un nouvel élan à l'arithmétique. Mais ce renouveau est le fait de toute une époque[16bis]. Notons que Fermat n'a jamais écrit de traité d'arithmétique ; c'est dans sa correspondance qu'il faut chercher ses travaux en arithmétique.

Au XVIII^{ème} siècle, Euler, qui s'intéresse à tous les domaines des mathématiques, publie dans les *Commentaires de l'Académie de Petersbourg* un certain nombre de démonstrations de résultats énoncés par Fermat. Au XIX^{ème} siècle, l'intérêt pour l'arithmétique est renouvelé par les travaux de Lagrange, Legendre et Gauss.

Et c'est ici que commencera notre histoire…

II.2. Nos outils d'analyse

En examinant les arguments de divisibilité, on s'aperçoit que les auteurs utilisent, explicitement ou non, un des quatre résultats fondamentaux (équivalents entre eux) suivants :

- « Proposition 32 d'Euclide » dite « Lemme d'Euclide » : [LE1] : si un nombre premier divise un produit, alors il divise l'un des facteurs du produit.[9]. On le rencontre aussi sous sa forme contraposée [LE2] : si un nombre premier *p* ne divise ni *a* ni *b*, alors il ne divise pas le produit *ab*.
- « Proposition 26 d'Euclide » [PE] : si deux nombres *a* et *b* sont premiers avec *c*, le produit *ab* sera aussi premier avec *c*.
- « Théorème de Gauss » [TG] : 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 » [TF] : 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.

L'équivalence de ces quatre résultats est montrée dans l'Annexe 1a. Nous donnons dans l'annexe 1b un exemple d'anneau dans lequel ces propriétés ne sont pas vérifiées.

Il est intéressant de se demander lesquels des quatre énoncés du Théorème fondamental sont utilisés et/ou explicités et/ou démontrés dans les textes, de regarder leur ordre

[8] Voir *Mnémosyne* n°14 pages 43-51.

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

d'exposition, la façon dont ils apparaissent liés, et les méthodes mises en œuvre. Nous n'avons fait ce travail que pour quelques traités mais cette recherche suffit à montrer les différents points de vue des auteurs et leurs priorités. Un autre résultat fondamental fréquemment utilisé est la relation de division euclidienne, que nous ne questionnerons pas ici.

On s'aperçoit en cours de route que ces auteurs déploient une riche variété de méthodes. Nous tentons ci-dessous une classification sommaire de ces méthodes de raisonnements, telles qu'elles apparaissent à travers l'organisation des démonstrations.

- Méthodes de tiroirs.
  - [MPT] : Utilisation d'un nombre fini de tiroirs pour ranger des objets 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 ».
  - [MDC] : Partition des situations étudiées en un nombre fini de cas qu'on examine exhaustivement. C'est la méthode de « disjonction des cas ».
  - [MBi] : Mise en bijection de deux ensembles finis de même cardinal.

- Méthodes d'escalier.
  - [MDF] : Descente finie jusqu'à un entier convenable fournissant la conclusion soit directement soit par l'absurde.
  - [MDI] : 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.
  - [MIS] : Induction simple : on démontre le passage d'un entier particulier spécifié au suivant et cet exemple générique justifie la généralisation.
  - [MRG] : Raisonnement par récurrence généralisé.
  - [MPPE] : Raisonnement utilisant le plus petit élément d'une partie non vide de N (ou méthode du plancher !)

On trouvera dans l'annexe 2 une démonstration de l'équivalence logique des méthodes [MDI], [MRG] et [MPPE].

Nous présentons ci-après notre travail d'analyse selon cette double grille : méthodes, avatars du Théorème fondamental.

Pierre de Fermat

III. Un choix de textes autour de la démonstration du petit théorème de Fermat

III.1. Un texte de Legendre.

Nous examinons d'abord un extrait de la *Théorie des nombres* de Legendre [6]. La première édition date de 1798 ; celle que nous avons utilisée est une réédition par Blanchard en 1955 de l'édition de 1830.

§ 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*.

La démonstration de Legendre reprend la première démonstration donnée par Euler en 1736 dans les *Mémoires de Pétersbourg*, comme le rappelle Legendre dans la note. Elle repose sur le développement du binôme ; Legendre montre que le nombre premier *c* divise tous les coefficients du développement à l'exception du premier et du dernier. Le fait que les coefficients sont des entiers est implicite : dans la démonstration qu'Euler donne en 1736, il précise que ces coefficients sont entiers car il reconnaît en eux des nombres figurés.

Pour Legendre, cela semble un résultat bien connu. L'argument de divisibilité mis en jeu est le lemme d'Euclide [LE1], sans ambiguïté possible. Au début de son traité, Legendre démontre d'ailleurs ce lemme (nous en verrons la démonstration plus bas), mais n'énonce pas le théorème de Gauss. L'unicité de la décomposition en facteurs premiers n'est pas non plus explicitement énoncée. La démonstration se termine à l'aide d'une méthode d'escalier, menant par descente finie à l'entier convenable 0 [MDF]. Notons qu'il utilise pour ce faire un calcul « en omettant les multiples de *c* », c'est-à-dire pour nous un calcul de congruences.

III.2. Un texte d'Euler

Le deuxième texte étudié est le début d'un article d'Euler(1758) [3] où celui-ci propose une démonstration du petit théorème de Fermat (il ne s'agit pas de sa première démonstration, comme nous venons de le lire) .

Si *p* est un nombre premier ne divisant pas le nombre *a*, alors *p* divise $a^{p-1}-1$.

Pour faciliter la lecture, nous avons découpé et réorganisé le texte. La démonstration complète est expliquée en termes modernes dans l'Annexe 3, accompagnée d'un texte de Gauss, la reprenant de façon plus concise.

THEOREME 1

1. Si p est un nombre premier et si a est premier avec p, il ne se trouve aucun terme de la progression géométrique

$$1, a, a^2, a^3, a^4, a^5, a^6, etc$$

qui soit divisible par le nombre p.

DEMONSTRATION Cela est évident d'après le livre VII d'Euclide, Prop. 26, où il est démontré que, si deux nombres *a* et *b* sont premiers avec *p*, le produit *ab* aussi sera premier avec *p* ; et donc, puisque *a* est premier avec *p*, en posant $b=a$, le carré a^2 sera premier avec *p* ; et en continuant, a^3, en posant $b=a^2$; de même, a^4, en posant $b=a^3$, etc. Ainsi donc aucune puissance de *a* ne sera divisible par le nombre premier *p*.

Euler utilise donc ici explicitement [PE] et une induction simple [MIS].

Le théorème 3, que nous regarderons page suivante, démontre l'existence de puissances de *a* qui ont pour reste 1 dans la division par *p*. L'utilisation du résultat fondamental y est ambiguë, c'est pourquoi nous examinerons d'abord les théorèmes 4 et 5

THEOREME 4.

16. Si la puissance a^{μ} divisée par p laisse le reste = r et que le reste de la puissance supérieure $a^{\mu+\nu}$ est = rs, le reste de la puissance a^{ν}, par laquelle la seconde surpasse la première, sera = s.

[…]

SCHOLIE

19. La démonstration de ce théorème peut aussi se faire ainsi. Puisque a^{μ} divisé par *p* laisse *r*, on aura $a^{\mu} = mp + r$ et de la même façon $a^{\mu+\nu} = np + rs$; donc on aura $a^{\mu+\nu} - a^{\mu}s = np - mps = (n - ms)p$ et donc le nombre $a^{\mu+\nu} - a^{\mu}s = a^{\mu}(a^{\nu} - s)$ sera divisible par *p* ; et l'un des facteurs a^{μ} n'est pas divisible par *p*. Donc l'autre $a^{\nu} - s$ sera divisible par *p*, et en conséquence la puissance a^{ν} divisée par *p* donnera le reste = *s*.

Notons que, dans tout le texte, Euler se réfère à ses propositions précédentes, et donc, même s'il ne le précise pas à chaque énoncé, le nombre *p* est premier. Ainsi , Euler utilise ici clairement [LE1].

THEOREME 5

20. *Si a^{λ} est la plus petite puissance après l'unité qui, divisée par p, laisse l'unité, alors aucune des autres puissances ne laisse le même reste = 1, sauf celles que l'on trouve dans la progression géométrique*

$$1,\ a^{\lambda},\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ a^{5\lambda} \text{ etc.}$$

DEMONSTRATION

Supposons en effet qu'une autre puissance a^{μ} quelconque donne aussi le reste = 1 si on la divise par *p*, et puisqu'on a $\mu > \lambda$ et que cependant μ n'est égal à aucun multiple de λ, on peut produire l'exposant μ de sorte que $\mu = \nu\lambda + \delta$ avec $\delta < \lambda$ et l'on n'aura pas $\delta = 0$. C'est pourquoi, puisque la puissance $a^{n\lambda}$, aussi bien que $a^{\mu} = a^{n\lambda+\delta}$, laisse l'unité quand elle est divisée par *p*, d'après le §18, cette puissance a^{δ} aussi aura l'unité pour reste et donc a^{λ} ne serait pas la plus petite puissance ayant cette propriété, contrairement à l'hypothèse. C'est pourquoi si a^{λ} est la plus petite puissance présentant le reste 1, aucune autre puissance ne sera dotée de la même propriété, si ce n'est celles dont les exposants sont multiples de λ.

C'est une démonstration du type [MPPE] : λ est le plus petit élément de l'ensemble des entiers naturels *n* vérifiant une certaine propriété (ici a^n a pour reste 1 dans la division par *p*) et, en utilisant une division euclidienne, Euler prouve par l'absurde que les seuls éléments de l'ensemble sont les multiples de λ .

Revenons maintenant au théorème 3 :

THEOREME 3

12. *Si le nombre a est premier avec p et que l'on forme la progression géométrique*

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7 \text{ etc}$$

il y a de nombreux termes, qui divisés par p, laissent pour reste 1 et les exposants de ces termes forment une progression arithmétique.

DEMONSTRATION

Parce que le nombre de termes est infini, mais que les différents restes ne peuvent se former en nombre supérieur à $p-1$, il est nécessaire que plusieurs, ou plutôt, une infinité de termes produisent le même reste *r*. Soit a^{μ} et a^{ν} deux termes de ce type laissant le même reste *r*, alors $a^{\mu}-a^{\nu}$ sera divisible par *p*. Mais $a^{\mu}-a^{\nu}=a^{\nu}(a^{\mu-\nu}-1)$, et puisque ce produit est divisible par *p*, mais que un facteur a^{ν} est premier avec *p*, il est nécessaire que l'autre facteur $a^{\mu-\nu}-1$ soit divisible par *p* ; d'où la puissance $a^{\mu-\nu}$ divisée par *p* aura le reste = 1. Soit $\mu-\nu=\lambda$, tel que le reste de la puissance a^{λ} soit = 1, pour toutes les puissances $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, $a^{5\lambda}$ etc. pareillement le reste sera aussi = 1. C'est pourquoi l'unité sera le reste de toutes les puissances

$$1,\ a^{\lambda},\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ a^{5\lambda},\ a^{6\lambda}\ \text{etc.}$$

dont les exposants sont en progression arithmétique.

Euler utilise ici le principe des tiroirs, [MPT], et aussi un résultat qui semble être le théorème de Gauss. Or, la seule référence dans toute cette partie du texte à des résultats arithmétiques connus des lecteurs de l'époque est le recours à la proposition 26 d'Euclide [PE] dans la démonstration du théorème 1 ; le théorème de Gauss, même s'il peut être logiquement déduit des propositions euclidiennes, n'est pas explicité dans les *Eléments*. D'autre part, comme nous l'avons dit plus haut, Euler considère toujours que le nombre *p* est premier et, pour un nombre premier, « *p* ne divise pas *a* » est équivalent à « *p* est premier avec *a* », ce qu'Euclide démontre. Il est probable qu'Euler pense ici au lemme d'Euclide plutôt qu'au théorème de Gauss.

La suite du texte montre que le plus petit λ tel que *p* divise $a^{\lambda-1}$ est un diviseur de *p*-1, d'où l'on déduit le petit théorème de Fermat (cf Annexe 3).

Cette démonstration du petit théorème de Fermat, s'appuyant sur l'étude des puissances d'un nombre modulo *p*, est reprise par Gauss dans la Section Troisième de ses *Recherches Arithmétiques* [5]. Dans la première section, Gauss introduit le langage des congruences[7] et démontre les propriétés utiles sur congruences et opérations. La section seconde contient la démonstration de ce que nous appelons le « théorème de Gauss » [TG] ; nous l'examinerons en détail dans la partie IV.

La section troisième commence par une démonstration du théorème de Fermat semblable à celle donnée par Euler dans le texte étudié ici. Elle utilise des propriétés arithmétiques et les puissances du nombre *a*. Nous donnons en annexe 3 un résumé de cette démonstration et le texte de Gauss.

Gauss suggère les raisons qui ont poussé Euler à chercher une démonstration différente de celle trouvée en 1736.

> Lambert en a donné une semblable, (*Acta eruditorum*. 1769, p. 109.). Mais comme le développement de la puissance d'un binome semble étranger à la théorie des nombres, Euler (Comm. nov. Petrop. T. VIII, p. 70.) donna une autre démonstration qui est conforme à celle que nous venons d'exposer. Dans la suite il s'en présentera encore d'autres : ici nous nous contenterons d'en donner encore une déduite du même principe que celle d'Euler. La proposition suivante, dont le théorême en question n'est qu'un cas particulier, nous sera utile pour d'autres recherches.

[7] Rappelons qu'on dit que *a* est congru à *b* modulo un entier *m* (ce qu'on note $a \equiv b \pmod{m}$) lorsque *m* divise l'entier *b* – *a* ; les congruences sont compatibles avec l'addition et la multiplication.

III.3. Un texte de Tannery

Il s'agit d'une nouvelle démonstration du théorème de Fermat, donnée par Jules Tannery dans ses conférences à l'Ecole Normale Supérieure, semblable à celle donnée actuellement par certains manuels de Terminale Scientifique (spécialité). Le texte est tiré de l'*Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure* par Emile Borel et Jules Drach (1894) [1].

On trouve au début du traité la définition et les propriétés des congruences modulo un entier *m*, utilisées dans la démonstration suivante :

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 $x_1, x_2, ...x_{p-1}$ rangés dans un autre ordre ; le produit des nombres $ax_1, ax_2, ...ax_{p-1}$ est donc congru (mod.*p*) au produit $x_1x_2...x_{p-1}$, et comme le dernier produit est premier à *p*, on en conclut $a^{p-1}-1 \equiv 0$ (mod.*p*).

C'est le célèbre *théorème de Fermat*, qui joue, dans la théorie des nombres, un rôle essentiel[10] 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* $a^p - a \equiv 0$ (mod.*p*).

Le début de la démonstration utilise le théorème de Gauss [TG] et la méthode des tiroirs [MBi]: lorsqu'on considère $p-1$ nombres $x_1, x_2, ...x_{p-1}$ incongrus entre eux et à 0 (mod.*p*), alors ces $p-1$ nombres sont, à l'ordre près, les $p-1$ différents restes non nuls possibles modulo p ; il y a bien ici une bijection. Le nombre *p* ne peut pas diviser $ax_j - ax_i = a(x_j - x_i)$ pour $i \neq j$ car il est premier avec *a* et devrait donc diviser $x_j - x_i$ d'après le théorème de Gauss [TG] démontré plus haut dans le traité (voir infra pages 44). Donc les $p-1$ nombres $ax_1, ax_2, ...ax_{p-1}$ sont distincts deux à deux modulo *p* et sont égaux dans leur ensemble aux $p-1$ différents restes non nuls possibles modulo *p*. On a ainsi $ax_1ax_2...ax_{p-1} \equiv x_1x_2...x_{p-1}$ (mod.*p*).

Donc le nombre premier *p* divise $ax_1ax_2...ax_{p-1} - x_1x_2...x_{p-1} = (a^{p-1}-1)(x_1x_2...x_{p-1})$ et comme le nombre *p* est premier à $x_1x_2...x_{p-1}$, *p* divise $a^{p-1}-1$ ([TG] à nouveau).

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

[10] 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 ($2^{2^n}+1$) ; un article sur le sujet est en préparation pour un numéro ultérieur de *Mnémosyne*. Il existe également des réciproques partielles de ce théorème donnant des tests de primalité.

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.

Elle nous séduit aussi par la puissance qu'elle révèle du principe des tiroirs, principe qui paraît si évident, et qui est ici utilisé par son avatar de la mise en bijection de deux ensembles de même cardinal.

Ce n'est sans doute pas un hasard si ce type de démonstration, aussi brève et percutante, apparaît presque un siècle après la publication du livre de Gauss. Nous avons vu Legendre utiliser la théorie des congruences implicitement, puis Gauss la formaliser explicitement. Elle est à la fin du dix-neuvième siècle complètement digérée.

Mais, si elle est convaincante et élégante, cette démonstration 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. Elle montre comment les $p - 1$ résidus non nuls modulo p se répartissent en « classes » définies à l'aide des puissances modulo p d'un entier a, classes qui ont toutes le même cardinal. C'est d'ailleurs bien en termes de puissances que Fermat énonce 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 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.

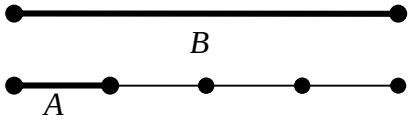
Il s'agit bien là semble-t-il de travailler sur les puissances d'un entier. Et le résultat est plus précis que celui généralement appelé « théorème de Fermat », puisqu'on s'intéresse au plus petit entier λ tel que le nombre premier p divise $a^{\lambda} - 1$. On aimerait connaître le cheminement de la 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 »

IV. Quelques textes autour des méthodes de descente infinie, de plancher et de récurrence.

IV.1.Un texte d'Euclide, extrait du livre VII des *Éléments* [2].

La proposition qu'on va découvrir est un des tout premiers énoncés du principe sur lequel se fonde ce que Fermat baptisera plus tard, comme nous le verrons ensuite (IV.2.2), la « méthode de descente infinie ». Elle fait partie de la série des livres VII, VIII et IX des *Eléments* d'Euclide, qu'on appelle parfois ses « livres arithmétiques ». L'arithmétique dont il s'agit, cependant, repose fondamentalement sur une représentation géométrique des nombres,

qu'Euclide conçoit le plus souvent comme des *droites*.[11] Les algorithmes arithmétiques sont donc pensés chez lui sur la base de procédures géométriques, comme celle de *mesure* d'une droite par une autre : que la *droite* A *mesure*[12] la droite B veut dire qu'on peut adjoindre[13] entre elles un certain nombre de *droites* égales à A pour *composer*[14] la droite B.



A *mesure* B

B est *composé* de droites égales à A.

C'est sur cette base qu'on peut comprendre la définition qu'Euclide donne d'un *nombre composé*, ainsi que par exemple celle de la multiplication d'un nombre par un autre.

Déf VII.14 : Un nombre composé est celui [qui est] mesuré par un certain nombre.

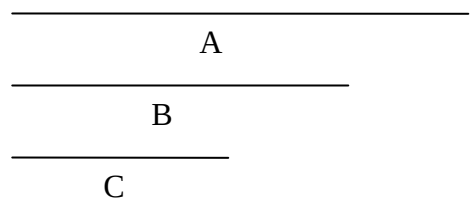
Déf VII.16 : Un nombre est dit multiplier un nombre quand, autant il y a d'unités en lui, autant de fois le multiplié est ajouté [à lui-même], et qu'il est produit un certain [nombre].

Notons qu'ici, comme à l'école primaire, le nombre qui multiplie n'a pas le même statut que celui qui est « multiplié » – en fait ajouté à lui-même autant de fois qu'il y a d'unités dans le multiplicateur. Dans le schéma ci-dessus, si A et B représentent des nombres, on peut faire correspondre à la *multitude* des *droites* égales à A qui, ajoutées, composent B, le *nombre* quatre, et dire que quatre, multipliant A, *produit* le nombre B.

Nous sommes maintenant armés pour découvrir la proposition 31 du livre VII, qui montre, dans notre langage, que tout nombre composé (non premier) est *divisible* par « un certain » (c'est-à-dire au moins un) nombre premier.

Prop. VII. 31 : *Tout nombre composé est mesuré par un certain nombre premier.*

Soit un nombre composé A. Je dis que A est mesuré par un certain nombre premier.



En effet, puisque A est composé, un certain nombre le mesurera. Qu'il le mesure et que ce soit B. Et si B est premier, ce qui était prescrit aura été fait.[15] S'il est composé, un certain nombre le mesurera. Qu'il le mesure et que ce soit C. Et puisque C mesure B et que B mesure A, le [nombre] C mesure donc aussi A.

Et, d'une part si C est premier, ce qui était prescrit aura été fait, d'autre part s'il est composé, un certain nombre le mesurera. Alors l'investigation étant poursuivie de cette façon, un certain nombre premier sera trouvé qui mesurera [A]. Car s'il ne s'en trouvait pas, des nombres en quantité illimitée mesureraient le nombre A, dont chacun serait plus petit que le précédent ; ce qui est impossible dans les nombres. Donc un certain nombre premier sera trouvé qui mesurera le [nombre] précédent et qui mesurera aussi A.

Donc tout nombre composé est mesuré par un certain nombre premier. Ce qu'il fallait démontrer.

[11] Le mot *droite* est pour nous un faux ami : dans le langage euclidien en effet, il renvoie à une ligne droite limitée des deux côtés, c'est-à-dire à ce que nous appelons un *segment* de droite.

[12] *mesurer* se dit en grec *metrein* ou *katametrein*, de la même racine que *metron*, mesure, d'où nous vient notre *mètre*. De fait notre opération de *mesure* à l'aide d'un *mètre* renvoie assez bien au concept euclidien.

[13] On pourrait dire encore *ajouter*, à condition de bien entendre par là *ad-jouxter*, ou faire se jouxter bout à bout : l'ajout (géométrique) n'est donc pas l'addition (arithmétique).

[14] La *composition* se dit en grec *sunthesis*, de *suntithêmi*, *poser ensemble*, d'où nous vient *synthèse*. Ce terme technique renvoie donc en général à l'*ajout* de deux objets géométriques.

[15] Ce langage évoque en fait une résolution de problèmes, comme si l'énoncé était : *Etant donné un nombre composé, trouver un nombre premier qui le mesure.*

L'argument essentiel de cette proposition revient à ce que nous formulerions ainsi : il n'y a pas de suite infinie strictement décroissante d'entiers naturels. Il faut noter par ailleurs que la démonstration repose en fait sur l'analyse d'un algorithme qu'on pourrait imaginer se poursuivre indéfiniment, au cas où aucun diviseur premier n'était trouvé. Cet algorithme n'est pas décrit 'en général' au sens où nous l'entendons, c'est-à-dire en décrivant le passage d'une étape *quelconque* à la suivante, mais il est décrit sur les deux ou trois premiers pas, qui permettent de concevoir comment on *pourrait* poursuivre. Ce type de raisonnement à l'aide d'un exemple générique est resté courant pendant longtemps, comme nous avons eu l'occasion de le voir chez Euler (cf. texte III.2).

IV.2. Quelques échanges épistolaires du XVIIème

Au XVII^{ème} siècle, Fermat s'empare de cette propriété des nombres entiers pour en faire une « route tout à fait singulière », qu'il appelle *méthode de descente infinie*. Fermat occupe en effet une place singulière au XVII^{ème} siècle : les méthodes générales données par l'algèbre pour résoudre de nombreux problèmes détournent un certain nombre de mathématiciens des problèmes arithmétiques, qui semblent particuliers et peu susceptibles de généralité. Ainsi, Descartes se plaint à Mersenne [7] des questions incessantes qu'il lui pose sur les nombres en arguant qu'il a autre chose à faire.

IV.2.1. Un extrait de lettre de Descartes

DESCARTES à MERSENNE
3 JUIN 1638

Au reste, mon Reverend Pere, je vous crie mercy, et j'ay les mains si lasses d'escrire cette lettre, que je suis contraint de vous supplier et vous conjurer de ne me plus envoyer aucunes questions, de quelque qualité qu'elles puissent estre ; car, lorsque je les ay, il est malaysé que je m'abstiene de les chercher, principalement si je sçay qu'elles vienent, comme celles-cy, de quelque personne de merite. Et m'estant proposé une estude pour laquelle tout le tems de ma vie, quelque longue qu'elle puisse estre, ne sçaurait suffire, je ferois tres mal d'en employer aucune partie à des choses qui n'y servent point. Mais, outre cela, pour ce qui est des nombres, je n'ay jamais pretendu d'y rien sçavoir, et je m'y suis si peu exercé que je puis dire avec verité que, bien que j'aye autrefois appris la division et l'extraction de la racine quarrée, il y a toutefois plus de 18 ans que je ne les sçay plus, et si j'avois besoin de m'en servir, il faudroit que je les estudiasse dans quelque livre d'Arithmetique, ou que je taschasse à les inventer, tout de mesme que si je ne les avois jamais sceuës.

Mais Fermat est à la fois algébriste et arithméticien ; or, en algèbre, on perd la spécificité des nombres entiers. Fermat cherche un moyen de la récupérer tout en utilisant la force du calcul algébrique[16].

Il s'intéresse aux triangles « rectangles en nombres », qui posent le même problème que les triplets pythagoriciens, c'est-à-dire les triplets (a,b,c) vérifiant $c^2 = a^2 + b^2$ et pouvant donc être les côtés d'un triangle rectangle.[17]

[16] Voir C.Goldstein, le métier des nombres au 18ème et 19ème siècles, in *Eléments d'Histoire des sciences*, sous la direction de Michel Serres, Larousse 1997, pp 411-443.

[17] Voir dans la brochure n°79 de l'IREM Paris VII un problème à partir d'un texte de Diophante à ce sujet.

IV.2.2 Des extraits de lettres de Fermat et de Wallis

FERMAT à CARCAVI[18]
AOUT 1659.

RELATION DES NOUVELLES DÉCOUVERTES EN LA SCIENCE DES NOMBRES .

1. Et pour ce que les méthodes ordinaires, qui sont dans les Livres, étoient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir. J'appelai cette manière de démontrer la *descente infinie* ou *indéfinie,* etc. ; je ne m'en servis au commencement que pour démontrer les propositions négatives, comme, par exemple:

Qu'il n'y a aucun nombre, moindre de l'unité qu'un multiple de 3, qui soit composé d'un carré et du triple d'un autre carré ;

Fermat affirme ici qu'il n'existe pas de nombre de la forme *3n-1*, avec *n* entier, égal à a^2+3b^2, avec *a*, *b* et *n* entiers.

Qu'il n'y a aucun triangle rectangle en nombres dont l'aire soit un nombre quarré.

La preuve se fait par *απαγωγην εις αδυνατον*[19] en cette manière:

S'il y avoit aucun triangle rectangle en nombres entiers qui eût son aire égale à un quarré, il y auroit un autre triangle moindre que celui-là qui auroit la même propriété. S'il y en avoit un second, moindre que le premier, qui eût la même propriété, il y en auroit, par un pareil raisonnement, un troisième, moindre que ce second, qui auroit la même propriété, et enfin un quatrième, un cinquième, etc. à l'infini en descendant. Or est-il qu'étant donné un nombre, il n'y en a point infinis en descendant moindres que celui-là (j'entends parler toujours des nombres entiers). D'où on conclut qu'il est donc impossible qu'il y ait aucun triangle rectangle dont l'aire soit quarrée.

On infère de là qu'il n'y en a non plus en fractions dont l'aire soit quarrée; car, s'il y en avoit en fractions, il y en auroit en nombres entiers, ce qui ne peut pas être, comme il peut se prouver par la *descente*.

Je n'ajoute pas la raison d'où j'infère que, s'il y avoit un triangle rectangle de cette nature, il y en aurait un autre de même nature, moindre que le premier, parce que le discours en seroit trop long et que c'est là tout le mystère de ma méthode. Je serai bien aise que les Pascal et les Roberval et tant d'autres savans la cherchent sur mon indication.

Fermat expose ici le principe de la méthode en l'appliquant apparemment à une suite de triangles ; mais ces triangles « en nombres entiers » fournissent en fait trois suites de nombres (les mesures de leurs trois côtés). C'est l'impossibilité de construire ces suites infinies strictement décroissantes d'entiers qui lui permet de conclure. Notons que Fermat ne précise pas ce qu'il entend par « triangle moindre » qu'un autre. Le lecteur sera peut-être déçu de ne pas voir ici comment on obtient ce fameux deuxième « triangle moindre que celui-là qui auroit la même propriété ». En fait, dans une autre lettre, Fermat donne une démonstration

[18] (Corresp, Huygens n° 651, (1) Publiée pour la première fois par M, Charles Henry *(Recherches,* p. 113-116) d'après une copie de la main de Huygens. Cette pièce avait été envoyée depuis peu par Fermat à Carcavi, lorsque celui-ci la communiqua à Huygens, le 14 août 1659.

[19] Littéralement : conduite jusqu'à l'impossible. Il s'agit d'un terme consacré depuis Aristote. Fermat utilise plus bas le terme : déduction à l'impossible.

explicite ; Frénicle de Bessy en donne une également. Ces démonstrations sont longues et difficiles, aussi renvoyons-nous le lecteur intéressé à l'ouvrage de Catherine Goldstein *Un théorème de Fermat et ses lecteurs* cité en bibliographie [15] : les textes de Fermat et Frénicle y sont donnés et abondamment commentés.

On voit ici Fermat s'intéresser à la démonstration de l'impossibilité de certaines propriétés, position fort moderne, mais peu prisée à l'époque. Ainsi, Wallis écrit-il [4], p.438:

WALLIS à DIGBY

Il ne m'a certes pas été désagréable, sur le désir exprimé par votre très noble correspondant [Fermat], d'engager une, deux fois la lutte avec lui et de descendre dans son arène ; mais cet illustre savant n'attend pas, sans doute, que je continue toujours le même exercice, et que, comme si je n'avais rien autre chose à faire, j'aborde sans cesse de nouvelles questions, perpétuellement renaissantes.

J'en dis autant pour ses récentes propositions négatives, que : en dehors de 25, il n'y a aucun nombre carré entier, qui augmenté de 2, fasse un cube ; ni, en dehors de 4 et 121, aucun qui, augmenté de 4, fasse un cube. Si cela est vrai ou non, je ne m'en soucie pas extrêmement, alors que je ne vois pas quelle grande conséquence peut en dépendre. Je ne m'appliquerai donc pas à le rechercher. En tout cas, je ne vois point pourquoi il en fait montre comme de choses d'une hardiesse étonnante et qui doivent stupéfier soit M. Frenicle, soit aussi les Anglais ; car de telles déterminations négatives sont très fréquentes et nous sont familières. Les siennes n'avancent rien de mieux ou de plus fort que si je disais :

Il n'y a pas (en entiers) de *cubocube* (j'entends une sixième puissance) ou même de carré, qui ajouté à 62, fasse un carré.

Ou : en dehors de 4, il n'y a aucun carré qui, ajouté au nombre 12 fasse un bicarré.

Ou : en dehors de 16, il n'y a pas de bicarré qui, ajouté à 9, fasse un carré.

…

Il est facile d'imaginer d'innombrables déterminations négatives de la sorte.

Fermat est conscient de ces réserves et affirme qu'il peut appliquer sa méthodes à «des questions affirmatives» dans le paragraphe suivant de sa lettre à Carcavi d'Août 1659. Nous n'avons malheureusement pas trouvé le détail de ses démonstrations !!!

2. Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y venir est beaucoup plus malaisé, que celui dont je me sers aux négatives. De sorte que lorsqu'il me fallut démontrer que *tout nombre premier qui surpasse de l'unité un multiple de* 4, *est composé de deux quarrés* , je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquoient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité. Le progrès de mon raisonnement en ces questions affirmatives est tel: si un nombre Premier pris à discrétion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux quarrés, il y a là un nombre premier de même nature, moindre que le donné, et ensuite un troisième encore moindre, etc. en descendant à l'infini jusques à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivroit n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux quarrés.

IV.3.Un texte de Legendre [6].

Examinons maintenant une variante de cette méthode dans une démonstration du lemme d'Euclide .

VI. « Tout nombre premier qui ne divise ni l'un ni l'autre des facteurs A et B, ne peut diviser leur produit A B. »

Cette proposition étant l'une des plus importantes de la théorie des nombres, nous donnerons à sa démonstration tout le développement nécessaire.

Soit, s'il est possible, θ un nombre premier qui ne divise ni A ni B, mais qui divise le produit A B, on pourra supposer qu'en divisant A par θ on a le quotient *m* (qui pourrait être zéro) et le reste A'; on aura donc A = *m*θ + A', et semblablement B = *n*θ + B'.

Donc AB = *m n* θ^2+ *n* A'θ + *m* B' θ + A' B'. Cette quantité, d'après l'hypothèse, doit être divisible par θ, et comme les trois premiers termes sont divisibles par θ, il faudra que le quatrième A' B' soit également divisible par θ; ainsi nous pourrons faire A' B'=C' θ.

Dans ce premier résultat, nous remarquerons 1° que A' et B' ne sont zéro ni l'un ni l'autre, parce que A et B sont supposés non divisibles par θ; 2° que A' et B', comme restes de la division par θ, sont moindres que θ; 3° qu'aucun des nombres A′ et B' ne peut être égal à l'unité ; car si on avait A' = 1, le produit A'B' se réduirait à B' ; or B' étant < θ, il est impossible qu'on ait B' = C'θ .

Nous avons donc deux nombres entiers, A', B', tous deux plus grands que l'unité, et tous deux moindres que θ, dont le produit est divisible par θ, de sorte qu'on a A' B' = C'θ. Voyons les conséquences qui en résultent.

Puisque A' est moindre que θ, on peut diviser θ par A'; soit *p* le quotient et A" le reste, on aura θ = *p* A' +A"; donc θ B'= *p* A'B' +A"B'.

Le premier membre est divisible par θ, il faut donc que le second le soit aussi. Mais la partie A'B' est divisible d'elle-même par θ, puisque A'B' = C'θ; donc 1'autre partie A"B' doit être encore divisible par θ.

Le nombre A", comme reste de la division par A', est moindre que A', il ne peut d'ailleurs être zéro; car si cela était, il serait divisible par A' et ne serait plus un nombre premier. Donc du produit A'B', supposé divisible par θ, on tire un autre produit A"B' divisible encore par θ, et qui est plus petit que A'B' sans être zéro.

En suivant le même raisonnement, on déduira du produit A"B' un autre produit A'"B' ou A"B", encore plus petit, et qui sera toujours divisible par θ sans être zéro.

Et en continuant la suite de ces produits décroissants, ou parviendra nécessairement à un nombre moindre que θ. Or il est impossible qu'un nombre moindre que θ, et qui n'est pas zéro, soit divisible par θ; donc l'hypothèse d'où l'on est parti ne saurait avoir lieu.

Donc si les nombres A et B ne sont divisibles, ni 1'un ni l'autre par θ , leur produit AB ne pourra non plus être divisible par θ.

Legendre, à partir d'un nombre A' tel que le nombre premier θ divise A'B' avec 1 <A'< θ, en fabrique un deuxième (par division euclidienne de θ par A') strictement plus petit et ayant les mêmes propriétés. Fermat eût conclu immédiatement à l'impossibilité par sa méthode de descente, mais Legendre précise que les produits A'B' allant en décroissant strictement finiront par se trouver inférieurs à θ et donc non divisibles par ce nombre θ. Il s'agit donc d'une descente finie jusqu'à un entier convenable [MDF].

A la fin du dix-neuvième siècle, cette particularité des entiers naturels (il n'existe pas de suite infinie strictement décroissante d'entiers naturels) prendra le statut d'axiome du bon

ordre[20] : toute partie non vide de *N* admet un plus petit élément. Ceci induit une autre forme de la méthode dont nous donnons un exemple ci-dessous : pour démontrer qu'il n'existe pas d'entier possédant une propriété P, on considère l'ensemble E des entiers naturels possédant P. Si cet ensemble est non vide, il possède un plus petit élément *m*. La méthode consiste alors à trouver un entier possédant la propriété P strictement inférieur à *m*. On aboutit ainsi à une contradiction prouvant que E est l'ensemble vide.

Nous avons rencontré en (III.1) une autre utilisation de cette méthode par Legendre pour la démonstration du théorème de Fermat. Nous examinons maintenant une autre variante de la méthode de descente infinie dans un texte de Tannery sous la forme « méthode du plus petit élément » [MPPE].

IV.4. Un texte de Tannery [1].

Tannery démontre ici en utilisant la méthode du plus petit élément [MPPE] que 2 ne peut pas être résidu quadratique modulo un nombre premier *p* de la forme $8n \pm 3$ (autrement dit, il n'existe pas d'entier *x* tel que $x^2 \equiv 2 \bmod p$).

Rappelons que, lorsqu'on travaille mod *p*, on peut se contenter de travailler avec des entiers inférieurs à *p*. Par ailleurs un certain nombre d'affirmations de Tannery peuvent se démontrer aisément par la méthode de disjonction des cas . Par exemple : il n'existe pas de carré congru à 2 mod 3. En effet, tout nombre entier est congru à 0, 1 ou 2 , mod 3, donc son carré est congru à 0 ou 1. Le même type de raisonnement permet de voir que le carré de tout nombre impair est de la forme $8n \pm 3$.

> […] Supposons maintenant que *p* soit de la forme $8n \pm 3$; il faut montrer que la congruence
>
> $x^2 - 2 \equiv 0$ (mod. *p)* est impossible. On le vérifie sans peine pour *p* = 3. Si donc la proposition n'était pas vraie, il existerait un nombre premier *p* de la forme $8n \pm 3$, tel que la proposition soit en défaut pour ce nombre, tout en étant vraie pour tous les nombres premiers de même forme inférieurs à *p.* Il suffit donc de démontrer l'impossibilité d'une telle chose. Si le nombre *p* existait, la congruence $x^2 \equiv 2$ (mod. *p), p* = 8*n* + 3 ou 8*n*+ 5, aurait deux solutions inférieures à *p*; l'une d'elles serait un nombre impair[21]; désignons-la par *x.* Nous allons faire voir que, *x* étant impair et inférieur à *p,* $x^2 - 2$ ne pourrait être divisible par *p* sans être divisible par un nombre premier de même forme et inférieur à *p.* En effet, le carré de tout nombre impair étant de la forme 8*n* + 1, x^2 - 2 est de la forme *8n* - 1 et ne peut par suite être égal à *p* ; on a donc x^2 - 2 = *p f, f* étant plus grand que 1. *f* est d'ailleurs inférieur à *p,* puisque *x* est inférieur à *p*; tous les facteurs premiers de *f* sont donc inférieurs à *p* ; il suffit donc de montrer que l'un au moins de ces facteurs est de la forme 8*n* +3 ou 8*n*+ 5. Or, si tous ces facteurs étaient de la forme $8n \pm 1$ (ils sont nécessairement impairs), leur produit *f* serait de la forme $8n \pm 1$ et le produit *pf* ne pourrait être de la forme 8*n*-1, ce qui est contraire à ce qu'on vient de voir.

[20] Voir I.R.E.M., *Histoires de problèmes, histoire des mathématiques*, Ellipses, 1997, pages 7-32.

[21] Si *a* vérifie $a^2 \equiv 2 \bmod p$ alors on a $(p-a)^2 \equiv 2 \bmod p$. Comme *p* est impair, *a* ou *p-a* est une solution impaire de la congruence.

IV.5. Un texte d'Euler

Comme nous le justifions dans l'Annexe 2, les trois méthodes : descente infinie, méthode du plus petit élément, démonstration par récurrence, sont logiquement équivalentes. Le nom « raisonnement par récurrence » a été donné par Poincaré en 1902, mais le principe de la démonstration par récurrence apparaîtrait dans le *Livre Arithmétique* de Maurolycus en 1557 ; il est clairement énoncé [8] par Pascal[22] dans son *Traité du Triangle Arithmétique* :

> Quoique cette proposition ait une infinité de cas, j'en donnerai une démonstration bien courte en supposant deux lemmes.
>
> Le 1, qui est évident de soi-même, que cette proportion se rencontre dans la seconde base […]
>
> Le 2, que si cette proportion se trouve dans une base quelconque, elle se trouve nécessairement dans la base suivante.
>
> D'où il se voit qu'elle est nécessairement dans toutes les bases : car elle est dans la seconde base par le premier lemme ; donc par le second elle est dans la troisième base, donc dans la quatrième, et à l'infini.

Dans le corpus que nous étudions, nous rencontrons la démonstration par récurrence, par exemple dans la première démonstration par Euler du petit théorème de Fermat, citée en note par Legendre (II.1.1).

Voici le texte d'Euler :

> 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 (*porro*) $(a+3)^p - a - 3$ 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.

Cette démonstration peut-elle être réellement qualifiée de démonstration par récurrence (MRG)?

Contrairement au résultat de Pascal qui, pour démontrer une propriété universelle, annonce qu'il suffit de démontrer deux lemmes (d'initialisation et d'hérédité) il n'est pas question, ici, d'une théorisation de la démonstration par récurrence.

Cependant, la démonstration de ce que nous appelons l'hérédité est faite par Euler indépendamment du rang (ce que Pascal ne fait pas dans la suite du texte cité plus haut), telle que nous la ferions actuellement.

Cependant, Euler éprouve le besoin de se justifier en effectuant une sorte d'induction. Il recommence d'ailleurs dans sa démonstration du théorème 3, ainsi que nous le faisons couramment lorsque nous voulons convaincre nos élèves et guider leurs premiers pas vers la

[22] Voir I.R.E.M., *Histoires de problèmes, histoire des mathématiques*, Ellipses, 1997, pages 7-32.

compréhension du théorème de récurrence. La compréhension profonde de ce théorème suppose des connaissances que n'ont pas nos élèves et il semble donc important de leur faire « sentir » le principe. Il n'en demeure pas moins une extrême rigueur dans la formulation des démonstrations, celles-ci s'appuyant sur les deux hypothèses d'initialisation et d'hérédité. Ce n'est évidemment pas une préoccupation d'Euler, la notion de rigueur variant avec le temps. Le principe de récurrence n'a d'ailleurs pu être théorisé qu'après l'axiomatisation des entiers. Mais nous trouvons bien les éléments essentiels d'une telle démonstration, agrémentés d'une esquisse d'induction qui peut permettre d'emporter l'adhésion des lecteurs.

V. Les différents avatars du théorème fondamental

V.1. Dans les *Éléments* d'Euclide [2bis].

Comme on l'a vu, l'arithmétique occupe trois livres des *Eléments* : les livres VII, VIII et IX. Les résultats qui nous intéressent figurent au livre VII, qui dégage des résultats importants sur les nombres premiers et les nombres premiers entre eux. Ces résultats s'appuient, assez étrangement pour nous, sur les proportions entre nombres entiers.

En effet une proportion est une relation à quatre termes, en l'occurrence des nombres, qui s'énonce sous la forme « A est à B comme C est à D » (par exemple 20 est à 5 comme 4 est à 1) et dont le maniement nous paraît peu commode. Pour les anciens au contraire, ces proportions constituent un *instrument de pensée* fondamental. Un exemple arithmétique permettra de saisir cet aspect de la pensée antique : on a vu plus haut ce que voulait dire qu'un nombre en multiplie un autre. Dans le cas particulier du schéma représenté dans la partie IV.1 « le nombre quatre, multipliant A, produit B » veut dire : « la multitude des droites égales à A qui, ajoutées ensemble, composent B, est *la même* que la multitude des unités dans le nombre quatre ». En langage euclidien, A est *la même partie* de B que l'unité l'est de quatre, ou encore B et quatre sont *équimultiples* de A et de l'unité respectivement. Une façon naturelle de dire ce qui précède est d'énoncer une *proportion* : A est à B comme l'unité est à quatre, ou inversement B est à A comme quatre est à l'unité.

Dans ces conditions, le théorème énonçant que deux nombres C et D se multipliant l'un l'autre, *les* produits obtenus (en effet on peut multiplier C par D, mais aussi D par C) sont égaux entre eux,[23] se ramène à une *opération élémentaire* sur les proportions : si P est un nombre, il est équivalent de dire que 1 est à C comme D est à P, ou que 1 est à D comme C est à P : c'est ce qu'on appelle l'*alternance* des termes moyens (C et D), démontrée par Euclide en VII.13 et qui est une des opérations *élémentaires* sur les proportions. Si P est le produit de C par D, il est donc encore le produit de D par C et réciproquement.[24]

L'exposé euclidien repose donc sur la démonstration préalable des propriétés opératoires des proportions (VII.11-14), dont fait partie l'alternance des termes moyens (VII.13) proposition que nous noterons désormais, de manière anachronique :

$$\frac{A}{B}=\frac{C}{D}\Rightarrow\frac{A}{C}=\frac{B}{D}$$

[23] C'est ce que nous appelons la *commutativité* du produit, que nous notons CD = DC. Chez Euclide c'est l'objet de la proposition VII.16.

[24] En réalité, ce résultat, qui fait l'objet de la proposition VII.16 (Heiberg-Vitrac) n'est pas démontré sur la base de VII.13 où est démontré l'alternance des termes moyens, mais de VII.15 qui n'est apparemment qu'un cas particulier de VII.13 ; la raison en est probablement que l'unité n'étant pas un nombre pour les anciens ne constitue par un terme 'légitime' dans un proportion. Euclide revient donc à une démonstration élémentaire qui s'appuie directement sur la définition VII16. Voir Vitrac [2bis] comm. ad VII.16, p.319-320.

De la même façon, nous confondrons désormais, pour simplifier, l'expression antique « A mesure B » avec l'expression moderne « A divise B ». [25]

Euclide démontre ensuite plusieurs résultats fondamentaux concernant spécifiquement les proportions de nombres entiers :

- Si C et D sont les plus petits nombres tels que $\frac{A}{B}=\frac{C}{D}$, alors C divise A et D divise B, avec le même quotient[26] (VII.20).
- Si C et D sont premiers entre eux et si $\frac{A}{B}=\frac{C}{D}$, alors C et D sont les plus petits nombres tels que $\frac{A}{B}=\frac{C}{D}$ (VII 21).
- Si C et D sont les plus petits nombres tels que $\frac{A}{B}=\frac{C}{D}$, alors ils sont premiers entre eux (VII.22).

Ces résultats fondamentaux de l'arithmétique euclidienne sont constamment utilisés dans les propositions ultérieures, comme on va le voir sur les exemples qui nous intéressent. Ainsi, voici comment Euclide démontre la proposition 24, que nous avons notée [PE] : *si deux nombres sont premiers avec un certain nombre, leur produit sera aussi premier avec ce même [nombre]*. En effet, si A et B sont premiers avec C et si AB n'est pas premier avec C, il existe E différent de l'unité qui divise (Euclide dit « mesure ») à la fois AB et C. Comme E mesure C et que A et C sont premiers entre eux, A et E le sont aussi.[27] En appelant F le nombre correspondant à la multitude des droites égales à E qui composent AB,[28] on a[29] que AB=FE, donc $\frac{B}{F}=\frac{E}{A}$. Comme A et E sont premiers entre eux, A divise F et E divise B (VII 20, 21) donc E est un diviseur commun à B et C, ce qui est contraire à l'hypothèse.

Notons qu'on peut isoler de cette démonstration l'argument suivant, qui se trouve démontré « au passage » : si le nombre E mesure le produit de A par B et qu'il est premier avec A, alors (en inventant F et en utilisant VII.20 et 21 de nouveau), on obtient que E mesure B. C'est ce que nous appelons le théorème de Gauss, moyennant la substitution de « divise » pour « mesure ». Pourtant, Euclide ne l'énonce nulle part comme une proposition indépendante et n'en fait donc pas un résultat fondamental.

Euclide démontre de la même manière la proposition VII.30 : *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, si un nombre premier A divise le produit BC, alors BC=DA pour un certain nombre D. Donc $\frac{A}{C}=\frac{B}{D}$. Si le nombre premier A ne divise pas C, alors A et C sont premiers entre eux, A et C sont les plus

[25] Gauss utilise également deux termes distincts en latin dans les *Disquisitiones* : *metiri* (mesurer) et *dividere* (diviser). Voir : *The shaping of arithmetic after K.F. Gauss'disquisitiones arithmeticae* ed. C. Goldstein, N.Schappacher et J. Schwermer, Springer 2007.

[26] Euclide n'emploie pas cette notion mais dit que C et D mesurent A et B respectivement 'autant de fois'.

[27] Sinon la plus grande commune mesure à A et E, différente de l'unité, mesurerait aussi A et C, qui ne seraient donc pas premiers entre eux : c'est l'objet chez Euclide de la proposition précédente (VII.23).

[28] Euclide applique ici l'opération qui permet de faire correspondre un nombre (ici F) à une multitude, la même qui nous a permis d'inventer le nombre « quatre » pour compter la multitude représentée en IV.1.

[29] C'est l'objet de la prop. VII.19 de prouver l'équivalence d'une proportion à l'égalité du produit des termes moyens et extrêmes.

petits nombres vérifiant $\frac{A}{C} = \frac{B}{D}$, donc A divise B. La formulation est là encore très proche du théorème de Gauss, mais n'en est qu'un cas particulier.

Actuellement, dans l'enseignement, et particulièrement pour l'enseignement de spécialité en Terminale S, c'est le chemin inverse qui est privilégié ; les résultats de divisibilité, comme le théorème de Gauss, sont obtenus d'abord et sont un outil fondamental pour les démonstrations. Une conséquence « mineure » est la validation de résultats sur les fractions irréductibles.

Enfin, comme on l'a vu plus haut, la proposition 33 donne un résultat qui pourrait mener à l'existence de la décomposition d'un entier en produit de deux nombres premiers : *Tout nombre composé est mesuré par quelque nombre premier*. Mais, ni l'existence, ni l'unicité de la décomposition d'un nombre entier en produit de nombres premiers ne sont énoncés explicitement dans les *Eléments*, même si on pourrait les déduire assez facilement du corpus des propositions démontrées par Euclide. De même, il n'y a aucune recherche systématique des diviseurs d'un nombre. Ce qui ne signifie pas que ces techniques n'étaient pas connues à l'époque. Jean Itard signale que Platon donne le nombre (59) de diviseurs stricts de 5040.

En vue de fixer un nombre qui convienne, décidons que le nombre des chefs de famille sera de 5040, qui, cultivant le territoire, en sont aussi les défenseurs. Que la terre ainsi que les résidences soient pareillement distribuées en un même nombre de sections, chacune étant l'unité distributive que sont en commun l'homme et son lot. Commençons donc par distribuer le nombre total, en deux portions, puis le même nombre en trois : en fait il est dans la nature du nombre en question de se laisser diviser en quatre, en cinq et, ainsi de suite jusqu'à dix. Partant, quiconque institue des lois doit à propos des nombres avoir, pour autant, réfléchi à la question de savoir *(a)* quel est le nombre, et comment constitué, qui sera le plus commodément utilisable pour toute organisation sociale : disons donc que c'est celui qui possède intrinsèquement le plus grand nombre de divisions et surtout de divisions qui se suivent. Tout nombre, c'est clair, pour tous les besoins est susceptible de tous les fractionnements que l'on voudra; mais ce nombre de 5040, pour la guerre aussi bien que pour tout ce que comporte la paix par rapport à l'ensemble des contrats et des partages, soit à propos de contribution ou de répartition d'avantages, ce nombre, dis-je, ne pourrait se fractionner en un nombre de fractionnements supérieur à cinquante-neuf ; mais, de 1 jusqu'à 10, ils se succèdent d'une façon continue. Au reste, voilà des propriétés dont une solide étude, et poursuivie à loisir, est obligatoire pour ceux à qui la loi prescrit de s'y consacrer.[30]

(c) Quant à nous du moins, c'est ce qu'à cette heure nous affirmons, nous ne pouvions choisir une exactitude supérieure à celle de ce nombre de 5040, puisque, jusqu'à 12 en commençant par 1, il possède toutes les possibilités de partage exact, hormis celui par 11. Encore cette exception admet-elle le plus simple des remèdes, puisqu'il suffit de mettre à part deux foyers familiaux pour lui rendre la santé d'une exacte divisibilité dans les deux sens.[31]

En bref, Euclide s'appuie sur les proportions pour démontrer [PE] et [LE1] indépendamment l'un de l'autre, mais n'énonce ni [TG] ni [TF]. Ce qui apparaît fondamental, ce sont les résultats sur les proportions, constamment utilisés dans les démonstrations. [LE1] est utilisé dans la proposition 14 du livre IX : *Si le plus petit nombre est mesuré par des nombres premiers, il ne sera mesuré par aucun nombre premier, si ce n'est par ceux qui le mesuraient d'abord*. Mais la plupart des résultats sont obtenus en revenant aux proportions, alors qu'un lecteur actuel préférerait sans doute utiliser [LE1].

[30] *Les Lois* dans *Œuvres complètes*, Tome II, Collection La Pléiade, Gallimard, 1943, Pages 793 et 794.
[31] Idem page 840

V.2. Les *Nouveaux Eléments de Mathématiques* de Jean Prestet (Paris 1689) [9].

Nous avons vu plus haut qu'Euler n'a pas énoncé explicitement le « théorème de Gauss ».

La question se pose alors de savoir quand on voit apparaître cet énoncé explicite dans un traité d'arithmétique. Catherine Goldstein a étudié[16]un traité de Prestet[32] dans lequel est énoncé ce théorème. Ce traité a connu plusieurs éditions : la première, en 1675, ne comportait pas l'énoncé du théorème de Gauss ; cette édition a eu une large audience car Prestet était soutenu par Malebranche et Leibniz. Cependant, dans les années quatre-vingts, le développement du calcul infinitésimal accapare l'attention des mathématiciens de l'époque, d'où un désintérêt pour « l'analyse finie ». La deuxième édition du livre de Prestet en 1689 ne rencontre pas le même succès que la première ; or c'est dans cette édition que Prestet énonce le théorème qui nous intéresse.

Le livre VI des *Nouveaux Eléments* de Prestet constitue un traité d'arithmétique élémentaire. Après avoir défini les objets de son étude (grandeur entière, diviseurs, nombres premiers, qu'il appelle aussi simples, etc.), Prestet énonce et démontre un certain nombre de résultats sur les nombres premiers ou premiers entre eux :

- Corollaire VIII : si un nombre premier *a* ne divise pas un nombre *z*, alors *a* et *z* sont premiers entre eux.
- Corollaire XI : tout nombre entier *z* est divisible par un nombre simple.

Il démontre ensuite le résultat fondamental suivant :

Théorème I : si deux nombres b et c sont premiers entre eux, bc est le plus petit nombre que l'un et l'autre puisse diviser au juste sans reste.

Autrement dit, dans ce cas, *bc* est le plus petit commun multiple des nombres *b* et *c*.

Ce théorème est démontré par une utilisation assez complexe de l'algorithme d'Euclide, avec descente et remontée. Décrivons d'abord la démonstration de Prestet, avec des termes actuels.

Soient *b* et *c* deux nombres premiers entre eux et *z* un multiple commun de *b* et *c*.

$b = cq + d$ avec $0 < d < c$. Soit *y* tel que $\frac{z}{b} = \frac{y}{d} = k$. Comme *z* est un multiple de *b*, *y* est un multiple de *d*. Or $z = bk = cqk + dk = cqk + y$; comme *z* est un multiple de *c*, *y* est un multiple de *c*. On réitère l'opération selon l'algorithme d'Euclide et on obtient :

$c = dq' + e$ avec $0 < e < d$. Soit *x* tel que $\frac{y}{c} = \frac{x}{e}$. Comme précédemment, *x* est un multiple de *d*.

On continue jusqu'à obtenir un reste égal à 1 (car *b* et *c* sont premiers entre eux).

$d = eq'' + f$ avec $f = 1$. Soit *v* tel que $\frac{x}{d} = \frac{v}{f}$. Alors *v* est multiple de *e*.

Donc *e* divise *v*, c'est-à-dire $\frac{v}{f}$ [parce que $f = 1$] donc $e \leq \frac{v}{f}$.

Donc $e \leq \frac{x}{d}$ et donc $d \leq \frac{x}{e}$.

De même $d \leq \frac{y}{c}$ et donc $c \leq \frac{y}{d}$.

[32]On trouvera une reproduction en fac-simile d'extraits significatifs de ce Traité et une présentation plus détaillée (par Michèle Grégoire) dans la rubrique « Bonnes Vieilles Pages » du numéro 16 de la Revue *Mnémosyne* , I.R.E.M. Paris 7, Juillet 2000.

Donc $c \leq \frac{z}{b}$.

Donc $bc \leq z$.

Ainsi bc est plus petit que tout multiple commun de b et c. Donc il est le plus petit multiple commun.

Notons que ce procédé permet d'obtenir le lien entre PPCM et PGCD :

Posons $b = a_1, c = a_2$ et $z = y_1$. On construit les suites (a_n) et (y_n) comme ci-dessous :

$a_1 = q_1 a_2 + a_3$	$\frac{y_1}{a_1} = \frac{y_2}{a_3}$	y_2 *est multiple de* a_2
…	…	…
$a_{n-2} = q_{n-2} a_{n-1} + a_n$	$\frac{y_{n-2}}{a_{n-2}} = \frac{y_{n-1}}{a_n}$	y_{n-1} *est multiple de* a_{n-1}

En utilisant les relations $\frac{y_k}{y_{k+1}} = \frac{a_k}{a_{k+2}}$, en effectuant leur produit et en simplifiant, on aboutit à : $\frac{y_1}{y_{n-1}} = \frac{a_1 a_2}{a_{n-1} a_n}$ qu'on peut écrire : $y_1 = \frac{y_{n-1}}{a_{n-1}} \times \frac{a_1 a_2}{a_n}$. Puisque y_{n-1} est multiple de a_{n-1}, le premier rapport est un entier et, si on a poursuivi l'algorithme d'Euclide jusqu'au dernier reste non nul, a_n est le $PGCD(a_1, a_2)$. On a ainsi prouvé que tout multiple commun à a_1 et a_2 est un multiple du quotient (entier) $\frac{a_1 a_2}{PGCD(a_1 a_2)}$ qui, étant lui-même multiple commun à a_1 et a_2, est donc le plus petit.

Ce type de démonstration par descente et remontée de l'algorithme d'Euclide est aussi utilisé par Bézout pour démontrer le résultat qui porte son nom.[33]

• Corollaire II : si *b* et *c* divisent *a*, alors le plus petit commun multiple de *b* et *c* divise *a*.

Le principe de la démonstration est le suivant : si on appelle *z* ce plus petit commun multiple, $z \leq a$. Si $z = a$, alors la proposition est vraie. Sinon, $a = zq + r$ avec $0 \leq r < z$. Comme *b* et *c* divisent *z* et *a*, alors *b* et *c* divisent $z - aq = r < z$. Ceci est contradictoire avec le fait que *z* est le plus petit commun multiple (non nul), sauf si $r = 0$ (Démonstration du type [MPPE] avec utilisation de la division euclidienne).

• Corollaire III : si un nombre *d* mesure un produit *bc* et que *c* et *d* soient premiers entre eux , le nombre *d* est un diviseur de l'autre nombre *b*.

En effet, dans ce cas, par le théorème I, le plus petit commun multiple de *c* et *d* est le produit *cd*. Comme *bc* est un multiple à la fois de *d* (par hypothèse) et de *c*, alors, par le corollaire précédent, *bc* est un multiple du *PPCM (d, c)*, qui est *dc*. Donc $bc = cdk$; donc $b = dk$, c'est-à-dire *d* divise *b*. Prestet démontre que le résultat obtenu sur le PPCM de *b* et *c* , lorsque *b* et *c* sont premiers entre eux, entraîne le théorème de Gauss. La réciproque étant vraie, ce résultat constitue donc une cinquième forme du théorème fondamental.

Notons au passage que Prestet en tire la détermination de tous les diviseurs d'un nombre donné sous forme d'un produit de facteurs premiers, par généralisation de résultats sur *ab*, *abc*, *abcd*, *abcde*, *abcdef*, a^2, a^2b, a^2b^2, où *a*, *b*, *c*, *d*, *e*, *f* sont des nombres premiers distincts

[33] Voir à ce sujet *Histoire d'algorithmes* Chabert et al. Belin 1994 p139-145.

deux à deux. Il montre alors le lien entre le plus petit commun multiple de deux nombres et leur plus grand commun diviseur, en utilisant les résultats précédemment démontrés.

V.3. La *Théorie des Nombres* de Legendre [6].

C'est dans *l'Introduction contenant des notions générales des nombres* qu'on trouve nos résultats fondamentaux.

Legendre commence par la démonstration de la commutativité du produit par descente finie jusqu'à un entier convenable. Soit en effet deux nombres A et B avec A > B ; On a A=B+C et on en déduit AB=BB+CB et BA=BB+BC. Donc on aura AB=BA si l'on a BC=CB ; en continuant, on arrivera au cas où l'un des deux facteurs est l'unité ou bien les deux facteurs sont égaux. D'où le résultat. Legendre démontre presque aussitôt le lemme d'Euclide [LE2] comme on l'a vu plus haut. Il fait la remarque que l'irrationalité de $\sqrt{2}$ découle de cette proposition ainsi que de manière générale celle de $\sqrt[n]{b}$ lorsqu'il n'existe pas d'entier x tel que $x^n = b$

Legendre donne alors explicitement l'existence de la décomposition d'un nombre entier en produit de facteurs premiers, mais n'énonce pas l'unicité. Cependant, il utilise implicitement ce résultat dans la recherche de tous les diviseurs d'un nombre entier. Le théorème de Gauss n'est pas énoncé, ni utilisé, le résultat fondamental est le lemme d'Euclide.

Sa méthode de prédilection est la descente finie jusqu'à un entier convenable, utilisée pour la démonstration de la commutativité du produit, le lemme d'Euclide , le théorème de Fermat.

V.4. Les *Recherches Arithmétiques* de Gauss [5].

L'ouvrage paraît en 1801 ; Gauss explique dans sa préface qu'il a commencé à s'intéresser au sujet en 1795, sans « aucune idée de tout ce qui avait été fait sur le sujet », ce qui explique qu'on y voit « la Science prise presque dès son principe ». Il y rend hommage au traité de Legendre, paru alors que son propre livre est sous presse.

La Section Première introduit les congruences modulo un entier *m* et donne les propriétés de compatibilité avec les opérations arithmétiques ; il signale que les critères de divisibilité et les règles de « vérification des opérations arithmétiques » (preuves par 9 et 11) reposent sur ces résultats.

La Section Seconde, où est démontrée le « théorème de Gauss » [TG], commence par une démonstration du lemme d'Euclide.

Des Congruences du premier degré.

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.

Nous rencontrons ici l'utilisation du plus petit entier strictement positif possédant une propriété donnée [MPPE], couplée à un raisonnement par l'absurde.

Gauss précise la raison pour laquelle 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 parceque plusieurs auteurs modernes ont présenté des raisonnemens 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.

Il utilise ensuite ce résultat pour démontrer l'unicité de la décomposition en facteurs premiers [TF], qui lui sert à déterminer tous les diviseurs d'un entier donné (et donc leur nombre), ainsi que le plus grand commun diviseur de deux ou plusieurs entiers.

Enfin, il en tire des théorèmes de divisibilité :

- *Si les nombres a, b, c, etc. sont premiers avec k, leur produit l'est aussi* [PE]. En effet, le produit *abc*… n'a pas d'autres facteurs premiers que ceux de *a* ou *b* ou *c* etc.

- *Si les nombres a, b, c, etc. sont premiers entre eux, et que k soit divisible par chacun d'eux, il le sera aussi par leur produit*. Car si *p* est un diviseur premier du produit *abc*…avec l'exposant *n*, alors p^n divise l'un des facteurs *a* ou *b* ou *c* etc.(car ils sont premiers entre eux) et donc divise *k* ; il en est de même de tous les autres facteurs du produit qui divise donc *k*.
- *Si a est premier avec b et que ak soit divisible par b, k sera aussi divisible par b* [TG]. En effet, *ak* est divisible à la fois par *a* et *b*, qui sont premiers entre eux, donc *ak* est divisible par le produit *ab* (par la précédente). D'où : $ak = nab$ donc $k = nb$.

Nous donnons dans l'annexe 4 un large extrait du texte de Gauss. Remarquons qu'à ce stade, il ne resterait qu'à voir le lemme d'Euclide comme cas particulier du théorème de Gauss pour établir l'équivalence entre les quatre résultats fondamentaux[34]. Mais cela ne fait pas partie des préoccupations de Gauss.

La Section Troisième s'occupe des « résidus des puissances » et c'est là qu'on trouve une démonstration du petit théorème de Fermat (voir Annexe 3).

V.5. Les conférences de Jules Tannery à l'Ecole Normale Supérieure (1891-1892) [1].

E. Borel et J. Drach rédigent les conférences de J. Tannery et publient une *Introduction à la Théorie des Nombres et à l'Algèbre supérieure* en 1894. Le livre débute par un exposé sur les congruences et leurs propriétés. Il s'appuie sur le théorème de Gauss [TG] dont il donne une démonstration attribuée à Poinsot. Comme dans l'ouvrage de Prestet, on commence par montrer que le plus petit commun multiple de deux nombres *a* et *m* premiers entre eux est leur produit. Pour cela, on considère la suite des multiples de *a* : {0, *a*, 2*a*, 3*a*, …, *ma*, …} et on appelle *h* le plus petit nombre strictement positif tel que *ha* est aussi un multiple de *m*. Le nombre *ha* est donc le plus petit commun multiple de *a* et *m*. Dans la suite des multiples de *a*, *h* nombres consécutifs sont toujours incongrus deux à deux modulo *m* car, si $ka \equiv k'a$ (mod. *m*) avec $0 < k - k' < h$, alors *m* divise le produit $(k - k')a$, ce qui contredit le fait que *h* est le plus petit nombre strictement positif tel que *m* divise *ha*. Par contre, si *h* divise $k - k'$, alors *m* divise le produit $(k - k')a$, donc $ka \equiv k'a$ (mod. *m*). Donc, si on considère la suite des restes des multiples de *a* dans la division par *m*, ces restes se reproduisent de *h* en *h*, mais *h* restes consécutifs sont distincts deux à deux. Par conséquent, les seuls multiples de *m* parmi les multiples de *a* sont les multiples de *ha* (démonstration du type [MPPE]). En particulier, *ha* divise *ma*, donc *h* divise *m*. Par conséquent, $m = hd$ et $ha = mq = hdq$, c'est-à-dire : $a = dq$. Le nombre *d* est donc un diviseur commun à *a* et *m*, et comme *a* et *m* sont premiers entre eux, $d = 1$, donc $m = h$ et dans ce cas, le plus petit commun multiple de *a* et *m* est bien leur produit *ma*. On en tire le théorème de Gauss comme dans Prestet.

En guise de conclusion…

On voit dans les classes de Terminale S spécialité certains élèves s'approprier avec bonheur certaines des méthodes rencontrées. Par exemple, la méthode de disjonction des cas rencontre beaucoup de succès, y compris sur des énoncés de baccalauréat dont l'auteur ne pensait peut-être pas à ce type de résolution : on trouvera dans l'annexe 6 des exemples de sujets de baccalauréat utilisant certaines des méthodes dont on parle dans l'article.

L'enseignement de l'arithmétique, qui avait disparu des programmes, est réapparu et a beaucoup évolué, en intégrant notamment une plus grande diversité des méthodes de recherche, de raisonnement et de démonstration. On pourra à ce sujet comparer utilement le libellé des programmes de Terminale C de 1971 et le document d'accompagnement des programmes actuels, qui stipule que « la démarche mathématique comporte des phases

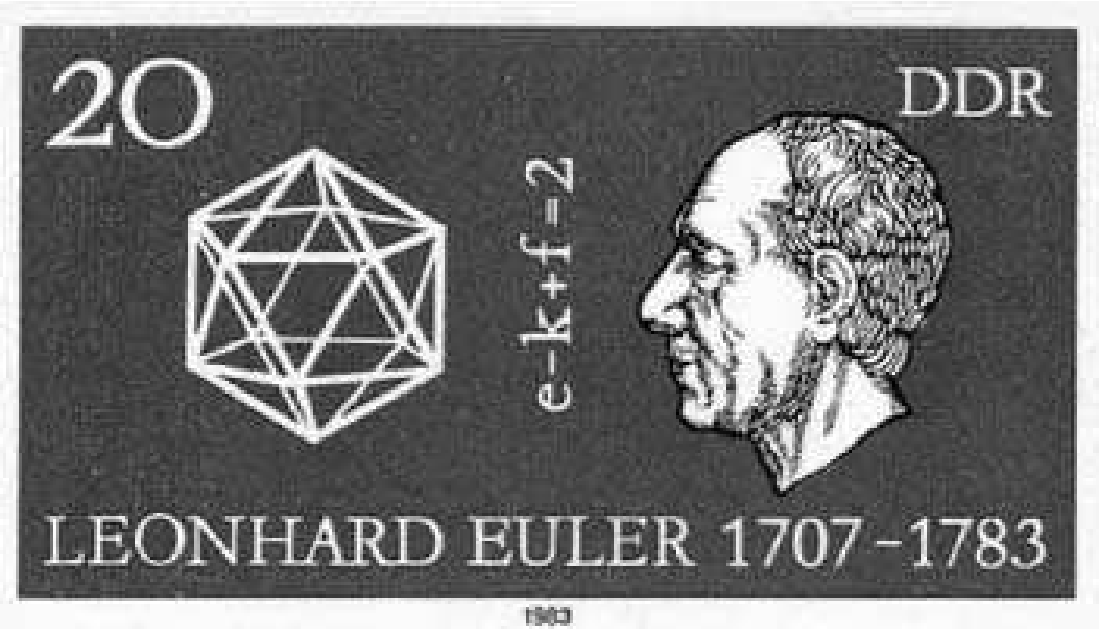
[34] Voir l'annexe 1.

expérimentales […] ; c'est particulièrement le cas en arithmétique ». Ce même document préconise de raisonner modulo 5 ou 7 (disjonction des cas) pour prouver que certaines équations diophantiennes n'ont pas de solution, un type de raisonnement absent des programmes antérieurs.

L'étude historique met en lumière des méthodes de démonstration permettant un évitement de l'infini et des difficultés qu'il entraîne : méthode du plus petit élément, répartition en classes d'équivalence par exemple. Ces méthodes, qui apparaissent assez naturellement dans le cadre des problèmes d'arithmétique sont riches de possibilités pour des développements ultérieurs en algèbre, que ce soit en tant que méthodes « standard » ou pour la construction d'objets théoriques sophistiqués.

Par exemple, la disjonction des cas couplée aux congruences, donne une première idée des classes d'équivalences, avant d'aborder $\mathbb{Z}/n\mathbb{Z}$ et les groupes finis..

L'examen des différentes méthodes de démonstration rencontrées dans les textes offre ainsi un réel intérêt pédagogique pour présenter la multiplicité des points de vue ; la démarche « expérimentale » des auteurs y est également sensible. Nous espérons que la classification que nous avons tentée est éclairante et utile.



Annexe 1
Une arithmétique sans théorème fondamental

On pratique l'arithmétique dans tout anneau commutatif unitaire intègre[35] . On donne alors les définitions suivantes :

L'ensemble des éléments inversibles de A est noté A* .

$A^* = \{a \in A ; \exists b \in A \ tel\ que\ ab = 1\}$

On dit que *a* divise *b* (ce qu'on note *a* / *b*) si et seulement s'il existe *c* dans A tel que *b* = *ac*.

Un élément *p* de A est dit irréductible si et seulement si $p \notin A^*$ et $[p = ab \Rightarrow a\ ou\ b \in A^*]$.

Deux éléments *a* et *b* sont dits premiers entre eux si et seulement si $[d / a\ et\ d / b \Rightarrow d \in A^*]$.

Par exemple, dans *Z*, les nombres inversibles sont +1 et –1 et les nombres irréductibles sont les nombres premiers avec leurs opposés.

On dit qu'un anneau A est factoriel lorsque :

- A est intègre
- Tout élément de A se décompose en produit de facteurs irréductibles.
- Cette décomposition est unique à élément inversible et permutation près.

Annexe 1a

Pour un anneau intègre A dans lequel tout élément se décompose en produit de facteurs irréductibles, il y a équivalence entre les propriétés suivantes :

(i) La décomposition est unique.

(ii) Lemme d'Euclide : si *p* est irréductible et si *p* divise *ab*, alors *p* divise *a* ou *b*.

(iii) *p* est irréductible si et seulement si l'idéal (*p*) est premier[36].

(iv) Théorème de Gauss : Si *a* et *b* sont premiers entre eux et si *a* divise *bc*, alors *a* divise *c*.

Remarque : on a toujours : si l'idéal (*p*) est premier, alors *p* est irréductible. En effet, si l'idéal (*p*) est premier, alors : si *p* = *ab*, alors *ab* est un élément de l'idéal (*p*) donc *a* ou *b* est dans l'idéal (*p*) (car cet idéal est premier) donc *a* = *kp* ou *b* = *kp*. Donc *p* = *ab* = *kbp* ou *kap* ; donc *kb* ou *ka* est égal à 1(car l'anneau A est intègre). On en déduit que *a* ou *b* est inversible. La propriété qui nous intéresse dans (iii) est donc la réciproque : si *p* est irréductible, alors l'idéal (*p*) est premier.

(ii) $\Rightarrow$ (iii) Supposons que *p* est irréductible et soit *ab* un élément de l'idéal (*p*). Alors *p* divise le produit *ab* et, par le lemme d'Euclide, *p* divise *a* ou *b*. Donc *a* ou *b* est dans l'idéal (*p*), qui est donc premier.

(iii) $\Rightarrow$ (ii) Si *p* est irréductible et divise le produit *ab*, alors *ab* est un élément de l'idéal (*p*), qui est premier. Donc *a* ou *b* est un élément de (*p*), donc *p* divise *a* ou *b*.

(ii) $\Rightarrow$ (i) Le Lemme d'Euclide entraîne l'unicité de la décomposition : c'est la démonstration habituelle, que nous voyons chez Gauss.

---

[35] Un anneau est unitaire s'il possède un élément neutre pour sa deuxième loi. Il est intègre si : « ab= 0 $\Rightarrow$a = 0 ou b = 0 »

[36] Un idéal (P) est dit premier ssi « ab $\in$ P $\Rightarrow$a $\in$ (P) ou b $\in$ (P) »

(i) $\Rightarrow$ (iv) L'unicité entraîne le théorème de Gauss ; cette démonstration se trouve dans les *Recherches Arithmétiques* de Gauss ; elle nécessite l'existence de la décomposition.

(iv)$\Rightarrow$ (ii) Le lemme d'Euclide est un cas particulier du théorème de Gauss.

Dans tout anneau principal (c'est-à-dire dans lequel tout idéal est principal, c'est-à-dire engendré par un seul élément), le théorème de Bézout est vrai, donc aussi le théorème de Gauss. Tout anneau principal est factoriel.

Tout anneau euclidien (possédant une division « euclidienne ») est principal.

Annexe 1b

Il existe des anneaux intègres dans lesquels la décomposition en produit d'éléments irréductibles existe mais n'est pas unique. L'exemple qui suit est tiré du *Cours d'algèbre* de Daniel Perrin [19].

$A = Z\left[i\sqrt{5}\right] = \left\{z \in C \,;\, il\ existe\ a\ et\ b\ dans\ Z\ tels\ que\ z = a + ib\sqrt{5}\right\}$

A est intègre (car inclus dans C).

On définit, pour tout z de A, $N(z) = |z|^2 = a^2 + 5b^2$.

Alors, si $z = z_1 z_2$, on a : $N(z_1 z_2) = N(z_1)N(z_2)$. Donc, si z_1 divise z, alors $N(z_1)$ divise $N(z)$. De plus, si $z_1 = a_1 + i\sqrt{5}b_1$ et $N(z_1) = 1$, alors $a_1^2 + 5b_1^2 = 1$ donc $a_1 = \pm 1$ et $b_1 = 0$; donc $z_1 = \pm 1$. On en déduit que, si $N(z)$ est premier, alors z est irréductible car, pour tout diviseur z_1 de z, $N(z_1)$ est un diviseur de $N(z)$, donc est égal à ± 1, donc aussi z_1 qui est alors inversible.

Le même type de considérations permet de démontrer que tout élément de A* admet au moins une décomposition en produit de facteurs irréductibles. En effet, si l'élément z est irréductible, la décomposition est toute trouvée. Sinon, il s'écrit : $z = z_1 z_2$, avec deux facteurs non inversibles ; si ces deux facteurs sont irréductibles, alors on a trouvé une décomposition convenable. Sinon, remarquons que $N(z_1) < N(z)$ (car, sinon, $N(z_2) = 1$ et z_2 serait inversible), ainsi que $N(z_2) < N(z)$, et recommençons le processus avec celui des deux facteurs qui n'est pas irréductible (éventuellement les deux). Le processus s'arrête car, sinon, la suite des $N(z_i)$ serait une suite strictement décroissante infinie d'entiers strictement positifs, ce qui est impossible. Or, lorsque le processus s'arrête, on a déterminé une décomposition de z en produit de facteurs irréductibles.

On a ainsi montré l'existence de la décomposition en produit de facteurs irréductibles de tout élément de A*. Mais A n'est pas factoriel : la décomposition n'est pas unique. Voici un contre-exemple :

On a : $9 = 3 \times 3 = \left(2 + i\sqrt{5}\right)\left(2 - i\sqrt{5}\right)$

Or 3 est irréductible. En effet, si $3 = z_1 z_2$ alors $N(3) = 9 = N(z_1)N(z_2)$. Donc $N(z_1)$ est égal à 1 ou 3 ou 9. Mais, si $N(z_1) = 3$, alors $a_1^2 + 5b_1^2 = 3$, ce qui est impossible. Donc $N(z_1)$ est égal à 1 ou à 9, c'est-à-dire que $N(z_1)$ ou $N(z_2)$ est égal à 1, donc l'un des deux facteurs de 3 est égal à 1. Donc 3 est irréductible.

De la même façon, $\left(2 \pm i\sqrt{5}\right)$ est irréductible car une décomposition en produit amène également à $N(2 \pm i\sqrt{5}) = 9 = N(z_1)N(z_2)$ et on peut faire le même raisonnement.

Ainsi le nombre 9 possède deux décompositions en produit de facteurs irréductibles essentiellement différentes.

Annexe 2

Equivalence des méthodes de descente infinie, récurrence et bon ordre

Nous nommons A l'ensemble des entiers naturels possédant une certaine propriété.

Sous forme logique, le principe de la méthode de descente infinie peut s'écrire :

MDI	$\{(n\in A)\Rightarrow(\exists n'<n \mid n'\in A)\}\Rightarrow A=\varnothing$

L'axiome de bon ordre : « Toute partie non vide de *N* admet un plus petit élément » peut s'exprimer de façon équivalente :

ABO	Si A est une partie de *N* qui n'admet pas de plus petit élément, alors $A=\varnothing$

La méthode de récurrence totale s'écrit :

MRT	$\{(0\in A)\text{ et }[(\forall n'\le n \quad n'\in A)\Rightarrow(n+1\in A)]\}\Rightarrow A=N$

Démonstration de MDI $\Rightarrow$ ABO

Soit A une partie de *N* qui n'admet pas de plus petit élément.

Dans ce cas $\{(n\in A)\Rightarrow(\exists n'<n \mid n'\in A)\}$ est vérifiée et donc, d'après MDI, $A=\varnothing$

Démonstration de ABO $\Rightarrow$ MRT

Nous supposons que A est telle que $\{(0\in A)et[(\forall n'\le n \quad n'\in A)\Rightarrow(n+1\in A)]\}$

La conclusion cherchée est $A = N$, c'est-à-dire $B = CA = \varnothing$.

Par l'absurde, si B n'est pas vide, d'après ABO elle admet un plus petit élément n_0.

Puisque $0\in A$, $0\notin B$, et donc $n_0\ge 1$ et $n_0-1\in N$. De plus $\forall n'\le n_0-1 \quad n'\in A$ (car n_0 est le plus petit élément de *B*) donc $n_0\in A$. Ce qui est exclu par $n_0\in B$. Donc *B* est vide et $A = N$.

Démonstration de MRT $\Rightarrow$ MDI

On suppose que MRT est vérifiée et que $\{(n\in A)\Rightarrow(\exists n'<n \mid n'\in A)\}$

0 n'ayant pas d'antécédent ne peut appartenir à A. Donc $0\in B = CA$

On a : $\{(\forall n'<n+1 \mid n'\in B)\Rightarrow(n+1\in B)\}$ car, sinon, on aurait $(n+1)\in A$ avec $\forall n'<n+1, n'\in B \quad c'est-à-dire \quad n'\notin A$; ce qui contredit $\{(n\in A)\Rightarrow(\exists n'<n \mid n'\in A)\}$.

Autrement dit, on a $\{(\forall n'\le n \mid n'\in B)\Rightarrow(n+1\in B)\}$

On en conclut que $B = N$ par MRT, et donc que $A=\varnothing$.

Annexe 3
Une démonstration du théorème de Fermat par Euler et Gauss

Voici d'abord les idées essentielles de la démonstration :

Etant donnés un nombre premier *p* et un nombre *a* premier à *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 en (II.2) est de « classer » les différents restes possibles modulo un entier premier *p* en utilisant les puissances de *a* modulo *p*[37].

Comme nous l'avons vu en lisant le texte d'Euler, celui-ci commence par montrer qu'il existe des puissances de *a* dont le reste est 1 dans la division par *p* : en effet, la suite $a, a^2, a^3, ..., a^\lambda, ...$ étant infinie et le nombre de restes possibles dans la division par *p* étant fini égal à $p-1$, il existe des puissances a^λ et a^μ, avec $\lambda \neq \mu$, présentant le même reste dans la division par *p* [MPT]. Donc le nombre premier *p* divise $a^\mu - a^\lambda = a^{\mu-\lambda}(a^\lambda - 1)$ (on peut supposer $\mu > \lambda$). Or, *p* premier ne divise pas $a^{\mu-\lambda}$, donc *p* divise $a^\lambda - 1$ (LE1].

On considère alors le plus petit entier λ strictement positif ayant cette propriété [MPPE]; alors les puissances $1, a, a^2, a^3, ..., a^{\lambda-1}$ ont toutes des restes différents (non nuls) dans la division par *p*, sinon le raisonnement précédent donne un entier λ' plus petit que λ tel que *p* divise $a^{\lambda'} - 1$. Si on obtient ainsi les $p-1$ restes possibles non nuls modulo *p*, alors $\lambda = p - 1$ et le théorème est démontré. Sinon, soit *r* un reste non nul non obtenu ; *r* est premier à *p*. On considère les nombres $r, ra, ra^2, ra^3, ..., ra^{\lambda-1}$; 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'est pas obtenu comme reste dans la division d'une puissance de *a* par *p*. 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 $s, sa, sa^2, sa^3, ..., sa^{\lambda-1}$. On montre de même que tous ces nombres ont des restes différents entre eux et différents des restes obtenus précédemment. Si on a obtenu tous les restes non nuls possibles, alors $p - 1 = 3\lambda$. Sinon, on continue jusqu'à obtenir tous les restes possibles et le même raisonnement prouve : $p - 1 = t\lambda$.

Ce raisonnement, en termes modernes, revient à faire une partition du groupe multiplicatif $(Z/pZ)^*$ formée des classes d'équivalences selon le sous-groupe cyclique engendré par *a*.

La méthode est reprise par Gauss, mais allégée par l'utilisation des congruences, aussi donnons-nous ci-dessous le texte de Gauss (in *Recherches arithmétiques*)[5].

On remarquera aussi dans celle-ci l'utilisation d'exemples numériques.

De plus, aussi bien Euler que Gauss aboutissent à un résultat plus fort que l'énoncé usuel du Théorème de Fermat (si *p* est premier, alors $a^p \equiv a \bmod p$). C'est d'ailleurs ce résultat plus fort qu'énonçait déjà Fermat (cf III.3)

[37] De manière beaucoup plus tardive et avec des concepts modernes, 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

SECTION TROISIÈME.

Des Résidus des Puissances.

45. THEOREME. *Dans toute progression géométrique* . . $1, a^2, a^3$ *etc., outre le premier terme* l , *il y en a encore un autre* a^t *congru à l'unité suivant le module* p *premier avec* a, *l'exposant t étant* < p.

Puisque le module *p* est premier avec *a,* et par conséquent avec une puissance quelconque de *a,* aucun terme de la progression ne sera = 0 (mod. *p*), mais chacun d'eux sera congru à quelqu'un des nombres 1, 2, 3, 4… *p* - 1. Comme le nombre de ces derniers est

p - 1, il est évident que si l'on considère plus de *p* - 1 termes de la progression, ils ne pourront pas avoir tous des résidus *minima* différents. Ainsi parmi les nombres $1, a^2, a^3 ... a^{p-1}$ on en trouvera au moins deux congrus. Soit donc $a^m \equiv a^n$ et *m* > *n,* on aura, en divisant par a^n ,[..] $a^{m-n} \equiv 1$ où $m - n < p$ et > 0.

Exemple. Dans la progression 1, 2, 4, 8, etc. le premier terme qui est congru avec l'unité suivant le module 13, se trouve être $2^{12} = 4096$, mais suivant le module 23, on a dans la même progression, $2^{11} = 2048 \equiv 1$; de même $5^6 = 15625 \equiv 1$ (mod. 7) ; et $5^5 = 3125 \equiv 1$ (mod. 11). Ainsi dans quelques cas la puissance de *a* congrue avec l'unité est plus petite que a^{p-1} et dans d'autres, il faut remonter jusqu'à la puissance *p* - 1 elle-même.

46. Quand la progression est continuée au delà du terme qui est congru à l'unité, on retrouvera les mêmes résidus qu'on avait à partir du commencement. Ainsi, soit $a^t \equiv 1$, on aura $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$ etc. , jusqu'à ce qu'on parvienne au terme a^{2t} dont le résidu *minimum* sera de nouveau ≡ 1, et la *période* des résidus recommencera. On aura ainsi une période de *t* résidus qui se répétera continuellement, et l'on ne pourra trouver un seul résidu qui ne fasse partie de cette période. On aura en général $a^{mt} \equiv 1$ et $a^{mt+n} \equiv a^n$; ce qui peut se présenter ainsi suivant notre notation : si $r \equiv \rho$ (mod. *t),* on aura $a^r \equiv a^\rho$ (mod. *p*).

47. Ce théorème fournit le moyen de trouver facilement les résidus des puissances, quelle que soit la grandeur de l'exposant dont elles sont affectées, en même temps qu'on découvrira la puissance congrue à l'unité. Si, par exemple, on demande le reste de la division de 3^{1000} par 13, comme $3^3 \equiv 1$ (mod.13), on a *t=3,* et comme d'ailleurs 1000 ≡ 1 (mod.3), on trouvera $3^{1000} \equiv 3$ (mod. 13).

48. Si a^t est la plus petite puissance congrue à l'unité, (en exceptant $a^0 = 1$, cas que nous ne considérons pas), les *t* restes qui composent la période seront tous différens, comme on le voit sans difficulté par la démonstration du n° 45. Alors la proposition du n° 46 peut être renversée. Savoir, si $a^m \equiv a^n$ (mod. *p),* on aura *m* ≡ *n* (mod. *t)* : car si *m* et *n* étaient incongrus suivant *t,* leurs résidus *minima* μ et ν seraient différens. Mais $a^\mu \equiv a^m$, $a^\nu \equiv a^n$; donc $a^\mu \equiv a^\nu$, c'est-à-dire, que toutes les puissances au dessous de *a'* ne seraient pas incongrues, ce qui est contre l'hypothèse.

Si donc $a^k \equiv 1$ (mod. *p),* on aura $k \equiv 0$ (mod. *t),* c'est-à-dire que *k* sera divisible par *t.*

Nous avons parlé jusqu'ici de modules quelconques, pourvu qu'ils fussent premiers avec *a.* A présent examinons à part les modules qui sont des nombres premiers absolus, et établissons sur ce fondement des recherches plus générales.

49. THÉORÈME. *Si* p *est un nombre premier qui ne divise pas* a, *et que* a^t *soit la plus petite puissance de* a *congrue à l'unité, l'exposant* t *sera* = p - 1, *ou une partie aliquote de* p-1.

Voyez pour des exemples le n° 45.

Comme nous avons déjà prouvé que *t* est = p - 1 ou < *p* - 1, il reste à faire voir que dans le dernier cas il est toujours une partie aliquote de *p* - 1.

1° Rassemblons les résidus *minima* positifs de tous les termes, $1, a^2, a^3 ... a^{t-1}$ et désignons-les par $\alpha, \alpha', \alpha''$, etc. de sorte qu'on ait $\alpha \equiv 1, \alpha' \equiv a, \alpha'' \equiv a^2$, etc. il est visible qu'ils seront tous différens ; car si deux termes a^m, a^n donnaient les mêmes résidus, on aurait $a^{m-n} \equiv 1$ (en supposant *m* > *n* et *m* - *n* < *t);* ce qui est absurde, puisque *a'* est la plus petite puissance de *a* congrue à l'unité. Au reste tous les nombres $\alpha, \alpha', \alpha''$, etc. sont compris dans la série 1, 2, 3, 4. . *p*- 1, série qu'ils n'épuisent pas lorsque *t* < *p* - 1. Nous désignerons par (*A*) la somme [l'ensemble] de tous ces résidus et (*A*) comprendra un nombre *t* de termes.

2°. Prenons un nombre quelconque,β, parmi ceux de la série 1, 2, 3... *p* - 1 qui manquent dans (*A*). Multiplions β par $\alpha, \alpha', \alpha''$, etc. et nommons. β, β', β'', etc. les résidus *minima* qui en proviendront, et qui seront aussi en nombre *t.* Ces résidus seront différens entr'eux , et différeront des nombres $\alpha, \alpha', \alpha''$, etc. En effet, si la première assertion était fausse, on aurait $\beta\alpha^m \equiv \beta\alpha^n$, d'où l'on tire, en divisant par β, $\alpha^m \equiv \alpha^n$: ce qui est contre ce que nous venons de démontrer ; si la dernière l'était, on aurait $\beta\alpha^m \equiv \alpha^n$; d'où, quand *n* > *m*, $\beta \equiv \alpha^{n-m}$, c'est-à-dire que β serait congru à quelqu'un des nombres $\alpha, \alpha', \alpha''$, etc.: ce qui est contre l'hypothèse; mais si *n*< *m,* on aura, en multipliant par $a^{t-m}, \beta a^t \equiv a^{t+n-m}$, ou comme $a^t \equiv 1, \beta \equiv a^{t-(m-n)}$, d'où résulte la même absurdité. Désignons par (*B*) la somme des nombres β, β', β'', etc. qui sont en nombre *t*; on aura déjà 2*t* nombres parmi ceux-ci 1, 2 ,3 , . . . *p-l.* Donc si (*A*) et (*B*) épuisent cette série, on .aura $t = \frac{p-1}{2}$.

3°. Mais s'il en manque quelques-uns, soit γ un de ceux-là. Multiplions $\alpha, \alpha', \alpha''$, etc par γ, et soient $\gamma, \gamma', \gamma''$, etc. les résidus *minima* de ces produits, dont nous désignerons l'ensemble par (*C*); (*C*) comprendra *t* nombres pris dans la série 1,2,3...*p-1* qui seront tous différens entr'eux et non~compris dans (*A*) et (*B*). Les deux premières assertions se démontrent comme ci- dessus (2°); quant à la troisième, si l'on avait $\gamma\alpha^m \equiv \beta\alpha^n$ on en tirerait $\gamma \equiv \beta\alpha^{n-m}$, ou $\gamma \equiv \beta\alpha^{t-(m-n)}$, suivant que *m* <*n* ou >*n.* Dans l'un ou l'autre cas γ serait congru à quelqu'un des nombres qui composent (*B*); ce qui serait contre l'hypothèse. On aura ainsi 3*t* nombres pris dans la série 1, 2,3.. .*p*-l, et s'il n'en reste plus, $t = \frac{p-1}{3}$, conformément au théorème.

4°. Mais s'il en reste encore quelques-uns, on arrivera de même à une quatrième somme de nombres (*D*), etc.; et comme la série 1,2,3, etc. *p*- 1 est finie, on voit que l'on parviendra nécessairement à l'épuiser, et *p* - 1 sera un multiple de *t;* donc *t* sera une partie aliquote de *p* - 1.

50. Puisque $\frac{p-1}{t}$ est un nombre entier, il suit qu'en élevant chaque membre de la congruence $a^t \equiv 1$ (mod. *p)* à la puissance $\frac{p-1}{t}$, on aura $a^{p-1} \equiv 1$ (mod. *p*); c'est-à-dire, que $a^{p-1}-1$ *sera toujours divisible par* p *quand* p *est premier et qu'il ne divise pas* a. Ce théorème remarquable, tant par son élégance que par sa grande utilité, s'appelle ordinairement *théoréme de Fermat,* du nom de l'inventeur. *(Fermatii opera Math. Tolosoe 1679,Fol.p.* 165.) 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 théorèmes 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 par conséquent $(a+1)^p - (a+1)$ 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.

Lambert en a donné une semblable, *(Acta eruditorum.* 1769, p. 109.) Mais comme le développement de la puissance d'un binôme semble étranger à la théorie des nombres, Euler (*Comm.nov. Petrop*. T. VIII, p. 70) donna une autre démonstration qui est conforme à celle que nous venons d'exposer. Dans la suite il s'en présentera encore d'autres : ici nous nous contenterons d'en donner encore une déduite du même principe que celle d'Euler. La. proposition suivante, dont le théorème en question n'est qu'un cas particulier, nous sera utile pour d'autres recherches.

Annexe 4

le théorème de Gauss dans les *Recherches Arithmétiques*[5]

SECTION SECONDE.

Des Congruences du premier degré.

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.

La démonstration de ce théorème a déjà été donnée par Euclide, *El.* VII, 32. Nous n'avons pas cependant voulu l'omettre, tant parceque plusieurs auteurs modernes ont présenté des raisonnemens 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.

15. *Si aucun des nombres* a, b, c, d, *etc. n'est divisible par le nombre premier* p, *le produit* abcd, *etc. ne le sera pas non plus.*

Suivant l'article précédent, ab n'est pas divisible par p; donc il en est de même de abc, et ainsi de suite.

16. THÉORÈME. *Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers.*

Il est évident par les élémens, que l'on peut toujours décomposer un nombre quelconque en facteurs premiers; mais on suppose à tort tacitement que cette décomposition ne soit possible que d'une manière. Imaginons qu'un nombre composé.....

$A = a^{\alpha} b^{\beta} c^{\gamma}$ etc., a, b, c, etc. étant des nombres premiers inégaux, soit encore décomposable d'une autre manière en facteurs premiers. Il est d'abord manifeste que dans ce second système de facteurs il ne peut entrer d'autres nombres premiers que a, b, c, etc., puisque quelqu'autre que ce fût ne pourrait diviser A, qui est composé des premiers. De même aucun des nombres premiers a, b, c, etc. ne peut y manquer, car sans cela il ne diviserait pas A (n° 15); la différence ne peut donc porter que sur les exposans. Or soit un nombre premier p, qui ait dans l'un des systèmes l'exposant m, et dans l'autre l'exposant n, m étant $> n$: divisons de part et d'autre par p^n, p restera dans l'un affecté de l'exposant $m-n$, et disparaîtra de l'autre, donc $\frac{A}{p^n}$ pourrait se décomposer de deux manières, dans l'une desquelles p n'entrerait pas, tandis qu'il resterait dans l'autre, ce qui est contre ce que nous avons démontré.

17. Si donc le nombre A est le produit de B, C, D, etc., il s'ensuit que les nombres B, C, D, etc ne peuvent avoir de facteurs premiers différens de ceux de A, et que chacun de ces facteurs doit se trouver autant de fois dans les nombres B, C, D, etc, pris ensemble, que dans A. On déduit de là le caractère pour reconnaître si le nombre B divise ou non un autre nombre A. Il le divisera s'il ne contient aucun facteur premier étranger à A, ni aucune puissance plus grande d'un des facteurs premiers de A. Si une de ces conditions manque, B ne divisera pas A.

A l'aide du calcul des combinaisons, on verra aisément que si... $A = a^{\alpha} b^{\beta} c^{\gamma}$ etc, a, b, c, etc. étant comme ci-dessus des nombres premiers différens, le nombre des diviseurs différens de A, en y comprenant 1 et A, est $(\alpha+1)(\beta+1)(\gamma+1)$ etc.

18. Si donc $A = a^{\alpha} b^{\beta} c^{\gamma}$ etc., $K = k^{\varkappa} l^{\lambda} m^{\mu}$ etc., et si tous les facteurs a, b, c, etc. diffèrent des facteurs k, l, m, etc.; A et K n'auront d'autre diviseur commun que 1, ou bien seront premiers entr'eux.

Le plus grand commun diviseur entre plusieurs nombres donnés A, B, C, etc. se trouve de la manière suivante : On décompose les nombres en facteurs premiers, et l'on prend ceux qui sont communs à tous les nombres A, B, C, etc. (s'il n'y en avait pas de tels, les nombres donnés n'auraient pas de commun diviseur); alors on remarque quels sont les exposans de ces facteurs, dans chacun des nombres A, B, C, etc.; on donne à chaque facteur le plus petit des exposans qu'il a dans A, B, C, etc., et l'on compose un produit des puissances qui en résultent; ce sera le plus grand commun diviseur cherché.

Si l'on cherchait au contraire le plus petit nombre divisible à-la-fois, par les nombres A, B, C, etc., on prendrait tous les nombres premiers qui diviseraient quelqu'un des nombres A, B, C, etc, et on donnerait à chacun d'eux le plus haut exposant qu'il ait dans les nombres A, B, C, etc. Le produit de toutes ces puissances serait le nombre cherché.

$A = 504 = 2^3 . 3^2 . 7$; $B = 2880 = 2^6 . 3^2 . 5$; $C = 864 = 2^5 . 3^3$.

Pour trouver le plus grand diviseur commun, on a les facteurs premiers 2 et 3, qui doivent être affectés des exposans 3 et 2, d'où il vient $2^3 . 3^2 = 72$. Quant au plus petit nombre divisible par A, B, C, il sera $2^6 . 3^3 . 5 . 7 = 6048$.

Nous omettons les démonstrations à cause de leur facilité ; d'ailleurs on sait par les élémens comment on résout ces problêmes, quand les nombres A, B, C, etc. ne sont point donnés tout décomposés en facteurs.

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.

Annexe 5

Une démonstration originale du théorème de Fermat

Le document d'accompagnement des programmes de Terminale S (spécialité), diffusé sur le site du CNDP, donne une démonstration combinatoire du petit théorème de Fermat. Nous reproduisons ci-dessous un extrait de ce document :

Démonstration 3

On donne ici une démonstration *combinatoire*, qui fournit au passage une interprétation du quotient $(a^p - a)/p$.
Considérons un polygone régulier $(A_0, \ldots, A_{p-1})$ ayant p sommets et étudions les façons de le colorier avec a couleurs. Le nombre total de coloriage est a^p. Parmi ces coloriages, il en existe a qui sont unicolores. Il s'agit donc de montrer que le nombre de coloriages multicolores du polygone est multiple de p. Or, étant donné un coloriage, il est possible d'en déterminer $p - 1$ autres par les rotations R_k d'angles $2k\pi/p$ $(1 \leqslant k \leqslant p - 1)$: si $(c_0,\ldots,c_{p-1})$ représente le coloriage initial, alors le coloriage final est représenté par $(c'_0,\ldots,c'_{p-1})$ caractérisé par la condition $c'_j = c_r$ où r est le reste de $j + k$ dans la division euclidienne par p. On montre qu'on obtient, avec le coloriage initial, p coloriages distincts : en effet, si un coloriage $(c_0,\ldots,c_{p-1})$ est invariant par une rotation R_k $(1 \leqslant k \leqslant p - 1)$, alors, par récurrence sur n, on doit avoir $c_0 = c_j$ lorsque j est le reste de la division euclidienne de nk par p. Comme p est premier, quand n parcourt $[0, p - 1]$, on obtient, pour j, toutes les valeurs de $[0, p - 1]$ (géométriquement, on parcourt les sommets du polygone en appliquant successivement une certaine rotation et en reliant les sommet successifs, on obtient un polygone convexe ou étoilé) : cela prouve que les seuls coloriages invariants par R_k sont les coloriages unicolores. Les coloriages multicolores sont au nombre de $a^p - a$ et peuvent être rassemblés par groupes de p. Donc $a^p - a$ est multiple de p. Le quotient $(a^p - a)/p$ peut s'interpréter comme le nombre de coloriages multicolores comptés à rotation près.

Annexe 6

Quelques exemples d'exercices d'arithmétique (Bac S, spécialité)

France métropolitaine, Juin 2003

Le début de l'exercice s'intéresse au cône Γ d'équation cartésienne dans un repère orthonormal $\left(O,\vec{i},\vec{j},\vec{k}\right)$: $y^2+z^2=7x^2$.

3a. Montrer que l'équation $x^2 \equiv 3 \quad [7]$, dont l'inconnue *x* est un entier relatif, n'a pas de solution.

3b. Montrer la propriété suivante :

pour tous entiers relatifs *a* et *b*, si 7 divise a^2+b^2 alors 7 divise *a* et 7 divise *b*.

4a Soient *a*, *b* et *c* des entiers relatifs non nuls. Montrer la propriété suivante :

Si le point de coordonnées (*a*, *b*, *c*) est un point du cône Γ alors *a*, *b* et *c* sont divisibles par 7.

4b. En déduire que le seul point de Γ dont les coordonnées sont des entiers relatifs est le sommet de ce cône.

Remarques : La troisième question induit clairement une disjonction des cas modulo7. La dernière question peut se résoudre par descente infinie (méthode qui paraît bien difficile pour un élève de terminale), ou en utilisant le plus petit entier strictement positif *a* tels qu'il existe une solution (*a, b, c*) .

Centres étrangers I, juin 2005

Partie B

On admet que 250 507 n'est pas un entier premier.

On se propose de chercher des couples d'entiers naturels (*a* ; *b*) vérifiant la relation :

(E) : $a^2 - 250\,507 = b^2$.

1) Soit X un entier naturel.

a) Donner dans un tableau, les restes possibles de X modulo 9 ; puis ceux de X^2 modulo 9.

b) Sachant que $a^2 - 250\,507 = b^2$, déterminer les restes possibles modulo 9 de $a^2 - 250\,507$; en déduire les restes possibles modulo 9 de a^2.

c) Montrer que les restes possibles modulo 9 de *a* sont 1 et 8.

Remarques : Cette question induit clairement une disjonction des cas (remarquons aussi qu'elle est clairement très inspirée, jusque dans le choix de l'exemple numérique, d'activités en classes moultes fois présentées par le groupe M. : A.T.H. sur la machine de Carissan, lors de stages à l'I.R.E.M. Paris 7 ou d'exposés divers, et finalement publiées dans le bulletin vert de l'A.P.M.E.P.).

Inde, avril 2005

Le plan complexe est rapporté à un repère orhonormal direct $(O,\vec{u},\vec{v})$. On considère l'application *f* qui au point M d'affixe *z* fait correspondre le point M' d'affixe *z*' tel que :

$$z' = \frac{3+4i}{5}\bar{z} + \frac{1-2i}{5}$$

1. On note *x* et *x*', *y* et *y*' les parties réelles et imaginaires de *z* et *z*'.

Démontrer que : $\begin{cases} x' = \dfrac{3x+4y+1}{5} \\ y' = \dfrac{4x-3y-2}{5} \end{cases}$.

…..

5. On considère les points M d'affixe $z = x + iy$ tels que $x = 1$ et $y \in Z$. Le point M' $= f$(M) a pour affixe z'. Déterminer les entiers y tels que Re(z') et Im(z') soient entiers (on pourra utiliser les congruences modulo 5).

Remarques : La dernière question a été effectivement traité par un certain nombre d'élèves en effectuant une disjonction des cas modulo 5 ; on a en effet, si $x = 1$,

$$\begin{cases} x' = \dfrac{4+4y}{5} \\ y' = \dfrac{2-3y}{5} \end{cases}.$$

Un tableau des possibilités modulo 5 donne alors :

y	0	1	2	3	4
$4 + 4y$	4	3	2	1	0
$2 – 3y$	2	4	1	3	0

Il est alors immédiat de conclure :

x' et y' sont entiers si et seulement si 5 divise à la fois $4 + 4y$ et $2 – 3y$, c'est-à-dire si et seulement si $y \equiv 4 \pmod 5$. Il est évidemment aussi possible de s'attaquer d'abord à x' en constatant que, si 5 divise $4(1 + y)$, alors 5 divise $y + 1$ grâce au théorème de Gauss. Le raisonnement pour obtenir l'équivalence souhaitée est alors assez simple.

Nice, juin 1978

1. Déterminer l'ensemble des entiers relatifs x tels que : $8x \equiv 7 \pmod 5$.

Remarques : On peut voir cet exercice comme résolution de l'équation $8x – 5k = 7$ (un classique du programme de TS), à inconnues dans Z, ou une application de la méthode de disjonction des cas.

On pourrait citer d'autres exemples, mais ceux-ci suffisent à voir comment interviennent certaines méthodes dans les sujets de baccalauréat.

Nous ne résistons pas au plaisir de vous donner l'énoncé du premier exercice du Concours général de Mathématiques 2006 (merci à Didier Trotoux de l'I.R.E.M. de Caen de nous l'avoir transmis) :

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, $0 \le j \le i$, 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

$$f_q(n) = \overline{a_i a_{i-1} \ldots a_1} + q a_0$$

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

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

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

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 : $f_q(n_m) < n_m$, 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.

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 $\{1, 2, 3, \ldots, p\text{-}1\}$, il existe k et k', avec $k < k'$, tels que $n_k = n_{k'}$ (principe des tiroirs). La suite est alors périodique de période $k'\text{-}k$ à partir du rang k.

La question 4. utilise le théorème de Gauss.

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

Comme $p = 10q - 1$, on a : $10q \equiv 1 \ (\mathrm{mod}.p)$ et donc $10 f_q(n) \equiv 10qn \ (\mathrm{mod}.p)$. 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 $f_q(n) - qn$.

Bibliographie

Sources primaires

[1] E. BOREL et J. DRACH, *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, 1894.

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

[2bis] EUCLIDE, L*es Elements*, Vol.2 Livres V à IX ,trad. B.Vitrac, Paris , PUF, 1994

[3] L. EULER : Théorèmes sur les restes laissés par la division des puissances, Traité 262 du catalogue Enestr., *Nouveaux mémoires de l'Académie de Saint Petersbourg* ,7, (1758/9, 1761,pp.49-82). Traduction libre. Réed. *L.Euleri Commentiones Arithmeticae* , 1, Rudio, Lipsiae et Berolini,1915.

[4] P. de FERMAT, *Œuvres* (tome II et III) éditées par Tannery et Henry, 1896.

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

[6] A.M LEGENDRE, *Théorie des Nombres*, Paris, 1830. Réédition Blanchard 1955

[7] *Correspondance du Père Marin Mersenne* publiée et annotée par Cornelis de Waard tome III (pp. 266-267), Editions du CNRS, 1969.

[8] B. PASCAL, *Œuvres Complètes*, Seuil, Paris, 1963.

[9] J. PRESTET, *Eléments des Mathématiques*, Paris, 1675 (deuxième édition 1689).

Sources secondaires

[10] V. BATTIE, *Spécificités et potentialités de l'Arithmétique élémentaire pour l'apprentissage du raisonnement mathématique.* Thèse IREM Paris 7, 2004.

[11] J.L.CHABERT et al., *Histoire d'algorithmes*, Belin, 1994.

[12] Commission inter I.R.E.M. Histoire et Epistémologie des Mathématiques, *Histoires de problèmes Histoire des Mathématiques*, Ellipses, 1993.

[13]J.P. DELAHAYE, *Merveilleux nombres premiers* , Belin-Pour la Science, 2000.

[14] A. DJEBBAR, *Une histoire de la science arabe*, Collection Points Sciences, Seuil, 2001.

[15] C. GOLDSTEIN, *Un théorème de Fermat et ses lecteurs*, Presses Universitaires de Vincennes, 1995

[16] C. GOLDSTEIN, On a Seventeeth Century Version of the «Fundamental Theorem of Arithmetic », *Historia Mathematica*, 1992 (pp. 177-187).

[16bis] C. GOLDSTEIN, Le métier des nombres aux XVIIème et XIXèmes siècles, in *Eléments d'Histoire des Sciences*, dir. Michel Serres, Larousse-Bordas, 1997.

[17] M. GUILLEMOT, « En route vers l'infini », *Histoires de problèmes, histoire des mathématiques*, Ellipses, Paris, 1993, pp. 7-32

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

[19] D. PERRIN, *Cours d'Algèbre pour l'Agrégation*, Editions ENSJF, 1981

[20] R.RASHED, *Entre arithmétique et algèbre Recherches sur l'histoire des mathématiques arabes*, Les Belles Lettres, 1984.

[21] J.A. RODDIER, *L'arithmétique en Lycée avec Excel*, IREM de Clermont-Ferrand, 2002.

Les portraits sont tirés du site de l'Université de Saint-Andrew (Ecosse) : www.groups.dcs.st-and.ac.uk./~history/