Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 9 (1907)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉTUDE ÉLÉMENTAIRE SUR LE THÉORÉME DE FERMAT
Autor: Aubry, A.
Kapitel: Première Partie. L'Arithmétique avant Fermat.
DOI: https://doi.org/10.5169/seals-10162

ÉTUDE ÉLÉMENTAIRE SUR LE THÉORÈME DE FERMAT

Non hic... qui abaco numeros...
scit risisse. Pers. I.

Première Partie.

L'Arithmétique avant Fermat.

Le théorème de Fermat marque une ère décisive dans l'histoire de la théorie des nombres. Jusque là, celle-ci était surtout algébrique et consistait principalement dans l'analyse indéterminée et dans la recherche et les applications des identités, ce qui n'est qu'une partie, — importante il est vrai, — mais accessoire de cette science. Un coup d'œil sur l'histoire de l'arithmétique pure avant Fermat fera mieux sentir l'importance des découvertes de ce grand géomètre [1]. Il fournira une introduction historique au théorème de Fermat dont nous donnerons une étude élémentaire dans un prochain article.

C'est dans l'école de Pythagore que paraissent avoir été émises les premières considérations, — probablement plutôt senties que raisonnées, — sur les nombres *premiers* ou *composés*, les nombres *parfaits*, *amiables*, etc., ainsi que sur les *irrationnelles* et les *formes quadratiques*, dont l'avènement fut préparé par diverses remarques sur les développements des produits $(a \pm b)^2$ et $(a + b)(a - b)$, et par diffé-

[1] Si nous écrivions une histoire de la théorie des nombres, il y aurait lieu de signaler celles des nombres figurés, des nombres polygones, des suites sommables, des combinaisons, des différences, de la formule du binome, des suites récurrentes, des fractions continues, de la théorie des équations, toutes choses que la théorie des nombres met à contribution. Mais notre but est beaucoup plus modeste et ne vise que l'arithmétique proprement dite.

[2] Les trois entiers x, y, z forment ce qu'on appelle un *triangle rectangle en nombres entiers*, ou simplement un *triangle*; x et y en sont les *cathètes*, z, l'*hypoténuse*. Les Egyptiens s'étaient bien aperçus que le triangle 3, 4, 5 est rectangle, mais c'est Pythagore qui paraît avoir démontré et généralisé cette proposition arithmético-géométrique.

rentes solutions de l'équation $x^2 + y^2 = z^2$ [2]. On voit donc posés, dès cette époque, les deux grands problèmes de la théorie des nombres : la composition arithmétique des nombres et leur représentation par une *forme*. Les premiers théorèmes étaient d'abord de simples remarques évidentes trouvées fortuitement ; de nouvelles propositions moins évidentes durent être justifiées pour en montrer la généralité ; et c'est ainsi que peu à peu se créa le mode de présentation des théories, mode qui acquit toute son ampleur chez Euclide, et est encore suivi aujourd'hui dans les livres élémentaires.

Toutefois cette arithmétique se ressentait de son origine géométrique : privée des secours de l'algèbre symbolique, elle empruntait celui de la géométrie ; aussi les énoncés abstraits étaient-ils traduits graphiquement, et les démonstrations, tout intuitives, facilitées par des raisonnements sur des figures, ce qui empêchait la généralisation des théorèmes. D'autre part, l'absence d'une bonne méthode de numération rendait très difficiles les opérations numériques et par suite l'étude des propriétés des nombres. On doit donc d'autant plus admirer la théorie complète et rigoureuse de l'arithmétique élémentaire qu'Euclide a insérée dans ses *Eléments* et dont nous allons rappeler seulement les énoncés.

VII. 1. *Etant donnés deux nombres, retranchons le plus petit du plus grand ; agissons de même sur le reste et le plus petit ; et ainsi de suite : si nous arrivons au reste* 1, *les deux nombres proposés sont premiers entre eux.*

2, 3. *Trouver la plus grande commune mesure de deux grandeurs, de trois grandeurs.*

5, 7. *Tout diviseur de* a *et de* b *divise* a + b *et* a — b.

16. $ab = ba$.

23, 24, 25. *Si* a *et* b *sont premiers entre eux, il en est de même de* ac *et de* bc, *et réciproquement. De plus tout diviseur de* a *est premier avec* b.

26. *Le produit de deux nombres premiers avec un troisième l'est avec ce dernier.*

27. *Si* a *et* b *sont premiers entre eux, tout multiple de* a *l'est avec* b.

28. *Si* a *et* b *sont respectivement premiers avec* α *et* β, aα *l'est avec* bβ.

29, 30. *Si* a *et* b *sont premiers entre eux, il en est de même de* a^n *et de* b^n, *ainsi que de* a + b *et de* a. *La réciproque est vraie.*

31. *Tout nombre premier est premier avec un nombre qui n'en est pas multiple.*

32. *Si un nombre premier divise* ab, *il divise* a *ou* b.

35, 36, 38. *Trouver le p. p. c. m. de plusieurs nombres.*

37. *Le p. p. c. m. de deux nombres divise tout multiple de l'un quelconque de ces nombres.*

41. *Trouver le plus petit nombre ayant des diviseurs donnés.*

IX. 12. *Tout nombre premier qui divise* a^n *divise* a.

13. *Si* p *est premier, aucun nombre plus petit ne divise* p^n.

14. *Le produit de plusieurs nombres premiers n'est divisible par aucun autre nombre premier.*

15. *Si les trois nombres* a, b, c *sont premiers dans leur ensemble, et que* $b^2 = ac$, *chacun d'eux est premier avec la somme des deux autres.*

20. *Les nombres premiers sont en plus grand nombre qu'un nombre quelconque* (en nombre illimité)[1].

21 à 34. Théorie des nombres pairs et des nombres impairs.

36. *Si* $2^n - 1$ *est un nombre premier, son produit par* 2^{n-1} *est un nombre parfait.*

X. Ce livre est consacré à la théorie des irrationnelles de la forme $\sqrt{a} + \sqrt{b}$, théorie qui a perdu tout intérêt depuis l'adoption de la représentation algébrique des identités. Elle se ramène aux divers cas de la relation

$$\sqrt{\frac{a + \sqrt{a^2 - b^2}}{2}} + \sqrt{\frac{a - \sqrt{a^2 - b^2}}{2}} = \sqrt{a} + \sqrt{b}\,.$$

On y trouve aussi ce qui suit :

29, lemme 1. *La solution générale du triangle est :*

$$x = ka^2 - kb^2,\ y = 2kab,\ z = ka^2 + kb^2\,.$$

[1] La démonstration de ce théorème, qui repose comme on sait sur la considération de l'expression 2 . 3 . 5 . 7 . 11 . 13 . 17 ... $p + 1$, témoigne qu'Euclide savait que celle-ci peut ne pas représenter un nombre premier.

117. *La diagonale du carré est incommensurable avec le côté.* Supposons qu'on puisse représenter le rapport de ces deux grandeurs par celui des deux nombres a et b, qu'on peut supposer premiers entre eux : on aura $a^2 = 2b^2$, ce qui demande que a soit un nombre pair 2α, et par suite que b soit impair. On aurait ainsi $4\alpha^2 = 2b^2$ ou $2\alpha^2 = b^2$ et b serait pair. Le nombre b serait ainsi pair et impair, ce qui démontre l'absurdité de la supposition.

Après Euclide, on peut citer : la sommation de Σn et de Σn^2, par Archimède ; les études de ce dernier et d'Apollonius sur la numération ; le *crible* d'Eratosthène ; et ces théorèmes, probablement pythagoriciens, recueillis par divers auteurs :

$\Sigma n^3 = (\Sigma n)^2$. (Epaphroditus.)

$8t_n + 1$ *est un carré.* (Plutarque.) [1]

Si on partage les nombres impairs en groupes de 1, 2, 3, ... *termes, la somme de chaque groupe est un carré.* (Nicomaque.)

La somme de deux triangulaires successifs est un carré. (id.)

Tout carré est de l'une des formes 3 *ou* 3 + 1 [2] *et de l'une des formes* 4 *ou* 4 + 1. (Théon de Smyrne.)

Les fractions $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \ldots \frac{\alpha}{a}, \frac{2a+\alpha}{a+\alpha}, \ldots$ *tendent en oscillant vers la valeur de* $\sqrt{2}$. (id. [3])

Si on additionne les chiffres de la somme de trois entiers consécutifs dont le plus grand est un multiple de 3, *puis les chiffres de cette somme, et ainsi de suite, on arrivera au nombre* 6. (Jamblique.)

Quoique Diophante ait traité exclusivement par l'algèbre [4] les questions qui nous sont restées de lui, il a au plus haut point servi la cause du progrès de l'arithmétique : d'abord en suggérant diverses théories sur l'existence ou le nombre des solutions de ses problèmes, dont la plupart sont de véri-

---

[1] t_n représente le n^e triangulaire, $\frac{n(n+1)}{2}$.

[2] Multiple de 3 ou multiple de 3 augmenté de 1.

[3] Ajoutons que c'est chez Théon qu'on voit la première idée des carrés magiques.

[4] Son artifice le plus employé consiste à ramener le problème à rendre carré le nombre $a^2 + ax + b$: il égale cette expression à $(x + n)^2$, ce qui lui donne $x = \frac{n^2 - b}{a - 2n}$, n étant un nombre entier arbitraire. C'est la première idée de la *méthode des coefficients indéterminés.*

tables théorèmes sur diverses équations quadratiques indéterminées [1], souvent très difficiles et même encore aujourd'hui inaccessibles à toute démonstration ; — ensuite par sa considération des formes des diviseurs numériques. Il sait en effet qu'*un nombre* $2n + 1$ *ne peut être une somme de deux carrés si* n *est impair ;* en outre il paraît admettre qu'*on peut décomposer un entier quelconque en une somme de quatre carrés* (IV, 31) et savoir que *les diviseurs d'une somme de deux carrés premiers entre eux sont de la forme linéaire* $4 + 1$ *et de la forme quadratique* $x^2 + y^2$, car il dit (V, 12) qu'*un nombre impair ne peut être une somme de deux carrés qu'autant que, divisé par son plus grand facteur carré, le quotient n'est pas de la forme* $4 - 1$, et (VI, 15) que *l'équation* $15x^2 - 36 = y^2$ *ne peut avoir lieu parce que* 15 *n'est pas la somme de deux carrés.* — Il tente de résoudre ce problème : *de combien de manières un nombre donné peut-il être polygone,* c'est-à-dire de la forme $\frac{(x+1)(xy+2)}{2}$? Il connaît l'identité de Fibonacci, car il observe (III, 22) que 65 peut se décomposer en deux carrés de deux manières différentes, parce que ce nombre est le produit de deux sommes de deux carrés. Il donne d'ailleurs plusieurs identités algébriques intéressantes, mais dont l'arithmétique ne saurait tirer parti.

Les Indiens ont beaucoup cultivé l'analyse indéterminée des deux premiers degrés ; leurs méthodes étaient du reste plus générales que celles de Diophante, qui se contentait d'une seule solution ; et en outre ils recherchaient des solutions entières, tandis qu'il suffisait au célèbre Alexandrin que la sienne fût rationnelle. Au point de vue qui nous occupe, il convient de citer : la résolution des équations $ax - by = c$ et $x^2 - ay^2 = 1$ au moyen des fractions continues, résolution qu'ils semblent avoir toujours crue possible ; cette remarque que l'équation $ax^2 - y^2 = 1$ n'est possible que si a est la somme de deux carrés, et la méthode pour passer de la solution de l'équation $x^2 - ay^2 = 1$ à celles de $x^2 - ay^2 = b$. Ces découvertes se trouvent, la première

[1] Telles que la suivante : *Trouver trois nombres tels qu'en augmentant ou diminuant leur somme de chacun d'eux, on obtienne six carrés.*

chez Aryabhata, les autres chez Brahmegupta, qui en sont peut-être les auteurs. C'est chez les Indiens qu'ont probablement pris naissance la preuve par 9 et celles par 7 et par 11 : la considération des résidus de puissances leur était du reste familière.

L'arithmétique est redevable de quelques progrès aux Arabes : ainsi Thebit ben Korra a donné cette formule de nombres amiables :

$$(3 \cdot 2^n - 1)(3 \cdot 2^{n-1} - 1)\,2^n \text{ et } (9 \cdot 2^{n-1} - 1)\,2^n ;$$

et un autre auteur dont le nom est inconnu, cette remarque que *toute hypoténuse est de l'une des formes* $12 + 1$, $12 + 5$, et l'identité

$$(a^2 + b^2)^2 \pm 4ab\,(a^2 - b^2) = (a^2 - b^2 \pm 2ab)^2$$

comme solution des équations simultanées

$$x^2 + y = z^2 , \quad x^2 - y = w^2 ,$$

ou de l'équation unique $2x^2 = z^2 + w^2$. Diophante a été connu d'eux vers l'an mil : c'est ainsi que Al-Kadjandi a annoncé l'impossibilité de décomposer un cube en deux autres cubes [1].

Les premiers algébristes italiens s'instruisirent chez les Arabes, qui certainement ont quelque part dans les nouveautés que Léonard de Pise (Fibonacci) a fait connaître en Europe. Toujours est-il que c'est dans le *Liber abaci* de ce dernier qu'on voit pour la première fois cette règle, de diviser un nombre par tous les nombres premiers inférieurs à sa racine carrée, pour s'assurer s'il est premier ; et la célèbre série récurrente 1, 2, 3, 5, 8, 13, 21, 35, ..., dont il définit les termes par le dénombrement mensuel de couples de lapins, en supposant que chaque couple en produit un autre à l'âge de deux mois et disparaît ensuite ; — et dans son *Liber Quadratorum*, que *la différence des carrés de deux nombres impairs consécutifs est un multiple de* 8 ; l'identité célèbre de laquelle il résulte que *le produit de deux sommes de deux*

[1] Diophante avait montré qu'un carré peut toujours se décomposer en deux carrés entiers ou fractionnaires, et paraît avoir tenté d'étendre ce théorème aux cubes.

carrés est, de deux manières différentes, la somme de deux carrés ; que la raison de trois carrés en progression arithmétique, laquelle est de la forme $4ab(a^2 - b^2)$, est un multiple de 24 et qu'elle ne saurait être un carré ; enfin qu'on ne saurait avoir à la fois

$$x^2 + y^2 = z^2 \quad \text{et} \quad x^2 - y^2 = w^2 ,$$

ni avoir

$$x^4 - y^4 = z^4 .$$

Ces trois dernières affirmations ont été données sans preuves satisfaisantes : Fermat les a retrouvées et démontrées.

On voit, dans Planude, l'équivalent de la formule $\Delta^4 n^4 = 24$; — dans Campanus (*Prœcl. liber elem. Eucl.* Venise, 1482), la première idée de la méthode retrouvée par Fermat et appelée par lui la *descente infinie*[1] ; — dans Paciolo (*Summa de Aritmetica,* Venise 1494), la publication de diverses études de Fibonacci et des Arabes ; — dans Charles de Bouvelles (*Opuscula,* Paris, 1511), ces deux théorèmes : *les nombres parfaits sont de la forme* $9 + 1$ et *tout nombre premier est de l'une des formes* 6 ± 1[(2)] ; — dans Stifel (*Arithmetica integra,* Nürnberg, 1544), plusieurs théorèmes, dont les suivants : *les deux nombres* 220 *et* 284 *sont amiables ; la formule* $2 \cdot 4^n - 1$ *ne donne que des nombres premiers*[3] ; n *étant premier avec* 3, on a :

$$\frac{2^{2n3^k} - 1}{2^{2^n} - 1} \equiv 0^4 ; \qquad \text{(mod. 7)}$$

tout entier est de la forme $a + 3b + 9c + 27d + 81e + \ldots$, les coefficients $a, b, c, \ldots$ pouvant prendre les valeurs -1,

---

[1] Campanus démontre géométriquement ainsi qu'*aucun nombre ne peut être divisé en moyenne et extrême raison :* en posant

$$(\alpha) \qquad \frac{a+b}{a} = \frac{a}{b} \quad \text{et} \quad a > b , \quad a - b = c , \quad b - c = d , \quad c - d = e , \ \ldots$$

on aura successivement

$$\frac{a}{b} = \frac{b}{c} \quad \text{et} \quad b > c , \quad \frac{b}{c} = \frac{c}{d} \quad \text{et} \quad c > d , \ \ldots$$

on pourra ainsi trouver une suite indéfinie d'entiers décroissants et répondant à la question Or une suite d'entiers positifs ne peut décroître indéfiniment. L'égalité (α) est donc impossible en nombres entiers.

Ce passage tout à fait inconnu a été remarqué pour la première fois par Genocchi.

[2] *Int. Math.* 1894, p. 122. Voir Ed. Luces, *Th. des n.* (Paris, 1891), p. 424.

[3] Théorème inexact. On sait qu'*aucune expression algébrique finie ne peut représenter que des nombres premiers.* (Euler.)

[4] « Septenarius, quemlibet numerum componit et numerat, qui colligitur ex tribus, sex, nouem, aut duodecim terminis, proportionalitatis duplœ, quadruplœ, aut sedecuplœ. »

0, 1 ; enfin une méthode de recherche d'un nombre pensé qu'on peut rendre par cette remarquable relation

$$\mathrm{R}\,\frac{(a+1)\,\mathrm{R}\,\frac{x}{a}+a^2\mathrm{R}\,\frac{x}{a+1}}{a(a+1)}=x$$

x étant inférieur à $a(a+1)$, et le symbole $\mathrm{R}\,\frac{x}{n}$ désignant le reste de la division de x par n [1].

Bachet, dans la première édition de ses *Prob. plaisants et dél.* (Lyon, 1612), annonçait la solution de l'équation $ax - by = c$, a, b et c étant premiers entre eux ; il la donne dans la seconde édition, publiée en 1624, et démontre l'existence, la périodicité et le calcul des solutions, en faisant voir que *si* b *est premier avec* a, *les valeurs de* $\mathrm{R}\,\frac{\mathrm{a\,x}}{\mathrm{b}}$ *sont toutes différentes, de* $\mathrm{x}=1$ *à* $\mathrm{x}=\mathrm{b}-1$, *et se reproduisent ensuite périodiquement* [2], et que *la relation* $\mathrm{ax}-\mathrm{by}=\mathrm{c}$ *entraîne cette autre* $\left(\mathrm{R}\,\frac{\mathrm{a}}{\mathrm{b}}\right)\mathrm{x}-\mathrm{by}=\mathrm{c}$.

---

[1] Cette fonction ne nous paraît pas avoir été étudiée systématiquement jusqu'ici ; elle semble cependant devoir conduire à des exercices intéressants. Ainsi

$$\mathrm{R}\,\frac{a}{n}+\mathrm{R}\,\frac{b}{n}\equiv\mathrm{R}\,\frac{a+b}{n}\qquad(\text{mod. } n)$$

$$\mathrm{R}\,\frac{a}{n}\,\mathrm{R}\,\frac{b}{n}\equiv\mathrm{R}\,\frac{ab}{n}\qquad(\text{mod. } n)$$

$$\mathrm{R}\,\frac{b\mathrm{R}\,\frac{a}{n}}{n}=\mathrm{R}\,\frac{ab}{n}$$

$$a>b>\mathrm{R}\,\frac{a}{b}>\mathrm{R}\,\frac{a}{\mathrm{R}\,\frac{a}{b}}>\mathrm{R}\,\frac{a}{\mathrm{R}\,\frac{a}{\mathrm{R}\,\frac{a}{b}}}>\mathrm{R}\,\frac{a}{\mathrm{R}\,\frac{a}{\mathrm{R}\,\frac{a}{\mathrm{R}\,\frac{a}{b}}}}>\cdots\qquad(\text{Binet.})$$

$$a>b>\mathrm{R}\,\frac{a}{b}>\mathrm{R}\,\frac{b}{\mathrm{R}\,\frac{a}{b}}>\mathrm{R}\,\frac{\mathrm{R}\,\frac{a}{b}}{\mathrm{R}\,\frac{b}{\mathrm{R}\,\frac{a}{b}}}>\mathrm{R}\,\frac{\mathrm{R}\,\frac{b}{\mathrm{R}\,\frac{a}{b}}}{\mathrm{R}\,\frac{\mathrm{R}\,\frac{a}{b}}{\mathrm{R}\,\frac{b}{\mathrm{R}\,\frac{a}{b}}}}>\cdots\qquad(\text{Euclide.})$$

La théorie des fonctions $\mathrm{R}\,\frac{ax}{b}$, $\mathrm{R}\,\frac{x^2}{b}$ et $\mathrm{R}\,\frac{a^x}{b}$ sont bien connues ; celle de $\mathrm{R}\,\frac{a}{x}$ n'a pas encore été étudiée.

[2] Dans notre dernier article, nous avons omis de dire que le *lemme fondamental* est de Bachet (*Ens. Math.* 1907, p. 286).

Bachet a encore rendu un service éminent à la science des nombres, par sa publication du Diophante (Paris, 1621), qu'il a traduit en latin et commenté. Parmi ses remarques, nous mentionnerons ce théorème qui porte son nom : *tout entier est la somme de quatre carrés au plus*[1], et qui a eu des conséquences importantes.

Mais c'est surtout à Frénicle que revient l'honneur d'avoir ouvert les nouvelles voies où devait s'illustrer Fermat. On connaît quelques-unes de ses découvertes par les *Lettres* de Descartes, les *Varia Opera* de Fermat et ses traités arithmétiques publiés seulement en 1729. Citons les théorèmes et problèmes suivants :

Il y a toujours l'une des cathètes d'un triangle qui est multiple de 3, *et une qui est multiple de* 4. *L'un des trois côtés est multiple de* 5. *La somme et la différence des cathètes est de l'une des formes* 8 ± 1.

Trouver le plus petit nombre qui soit n *fois hypoténuse. Trouver* n *triangles ayant même surface.*

Il paraît avoir remarqué avant Fermat la méthode de la descente infinie, l'impossibilité de la surface d'un triangle d'être représentée par un carré, la propriété des nombres premiers de forme $4 + 1$ d'être la somme de deux carrés, et divers problèmes d'analyse indéterminée. Sa méthode de démonstration était un tâtonnement ou *exclusion* méthodique, qu'il indique par des exemples et qu'il employait très habilement. Une très grande pratique étant nécessaire pour l'emploi de cette méthode, il paraît peu utile de la mentionner autrement.

Descartes, dans la solution de plusieurs problèmes qui lui furent proposés, a montré ce qu'il eût pu produire s'il avait cultivé l'arithmétique. Outre la solution de plusieurs questions diophantines, il fait voir (*Lettres,* Paris, 1667) que *les nombres* $4 - 1$ *ne peuvent être des carrés ni des sommes de deux carrés ;* que *les nombres* $8 - 1$ *ne peuvent être des carrés ni des sommes de deux ou de trois carrés ;* que *si* $3a - 1$, $6a - 1$ *et* $18a^2 - 1$ *sont des nombres premiers, le nombre* $2a(18a^2 - 1)$ *et la somme de ses diviseurs sont amiables*[1] ; que

[1] Théorème laissé sans démonstration jusqu'à Lagrange.

si $\sigma a = (3 + 4k)\,a$ [2] *et que* a *soit multiple de* 3 *et non de* 9, *on a*

$$\frac{a}{3} = \frac{1}{2 + 3k}\,\sigma\,\frac{a}{3}\,;$$

que *si* a *est multiple de* 3 *et non de* 45, *et que* $a = \frac{1}{2}\,\sigma a$, *on a*

$$45a = \frac{1}{3}\,\sigma(45a)\,;$$

que *si* a *est multiple de* 3 *mais non de* 819, *et que* $a = \frac{1}{2}\,\sigma a$, *on a*

$$273a = \frac{1}{3}\,\sigma(273a)\,;$$

que *si* a *n'est divisible ni par* 31, *ni par* 43, *ni par* 127, *ni par* 1024, *on a*

$$\frac{Aa}{\sigma(Aa)} = \frac{Ba}{\sigma(Ba)}\,, \qquad A = 2^{13}\ 43\,.\,127\,, \qquad B = 31\,,$$

théorèmes qui servent de types et permettent de multiplier indéfiniment les solutions des *nombres aliquotaires* [3]. On voit dans les mêmes *Lettres* qu'en 1638, de S^te^ Croix, autre arithméticien insigne. connaissait le théorème des nombres polygones, extension de celui de Bachet; que Descartes savait que *les seuls nombres parfaits pairs sont ceux d'Euclide* et que, *s'il y en a d'impairs, ils sont de la forme* $pp'^2p''^2 \ldots$, p, p′, p″, ... désignant certains nombres premiers [4]. Ajoutons que, dans le t. XII du *B. Bon.* (Rome, 1879), on voit que Descartes avait trouvé ces propositions par le moyen de la relation $f(ab) = f(a)\,f(b)$. (Ch. Henry, *Rech. sur les man. de Fermat.*) Tous ces travaux de Descartes sont de 1638.

Dans les *Cogitata physico-mathematica* (Paris, 1644), de Mersenne, on trouve les énoncés des résultats qu'on vient de voir relatifs aux nombres aliquotaires, et en outre les propositions que voici, dues probablement à Fermat :

---

[1] Descartes applique ces formules aux cas de $a = 2$, ce qui lui donne le couple de Stifel, de $a = 8$ et de $a = 64$.

[2] σn représente la somme des diviseurs de n, $f n$ la somme de n et de ses diviseurs, c'est-à-dire $\sigma n + n$.

[3] Ed. Lucas (l. cit.) donne une restitution très plausible des démonstrations de ces théorèmes. Voir aussi les *Comm. Arith.* d'Euler.

[4] Voir Lionnet (*Nouv. An.*, 1879), Sylvester (*Comptes Rendus*, 1888), Stuyvært (*Mathesis*, 1896).

Les seules valeurs de n *donnant pour* $2^n - 1$ *des nombres premiers, jusqu'à* $n = 257$, *sont* 1, 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 [1].

Le plus petit nombre ayant cent diviseurs est 126765060022 8229401496703205376, *et la* 66e *puissance de ce nombre multipliée par la quatrième de cet autre* 847288609443 *donnerait le plus petit nombre ayant un million de diviseurs.*

Dans son fameux *Traité du triangle arithmétique*, divulgué en 1654, mais publié seulement en 1665, Pascal a donné une théorie complète des nombres figurés, des combinaisons et du développement de $(a + b)^n$, toutes choses connues des Indiens et des Arabes, mais non démontrées et d'ailleurs incomplètement traitées jusque là [2]. Pascal démontre les formules relatives à ces trois théories, fait voir les relations qu'elles ont entre elles, les applique aux questions de probabilité, à l'expression générale de Σx^u qu'on ne connaissait que pour les onze premières valeurs entières de n et en tire la démonstration de la formule

$$\int_0^a x^n \, dx = \frac{a^{n+1}}{n+1} ,$$

ainsi qu'un grand nombre de théorèmes remarquables, dont ceux-ci :

$C_{a+b,\,a} = C_{a+b,\,b}$.

$C_{a,\,b}$ *est divisible par* b !

Le nombre total des combinaisons de n *objets est* $2^n - 1$ [3].

Mais c'est surtout dans sa méthode de démonstration que Pascal a bien mérité de la science, méthode applicable à une foule de questions où il s'agit d'une suite indéterminée de nombres : elle consiste à montrer qu'une certaine propriété supposée vérifiée pour l'entier n, l'est encore pour $n + 1$, de

---

[1] Les neuf premiers de ces nombres étaient déjà connus. Le nombre 67 paraît mis pour 61. L'assertion de Mersenne a été vérifiée, sauf pour les nombres premiers 71, 89, 101, 103, 107, 109, 127, 137, 139, 149, 157, 163, 167, 173, 181, 193, 199, 227, 229, 241 et 257.

[2] En Europe, le calcul des coefficients du développement de $(a + b)^n$ à l'aide de ceux de $(a + b)^{n-1}$ a été d'abord indiqué par Stifel (l. cit.) ; et le calcul des coefficients à l'aide de ceux qui les précèdent dans la même puissance, l'a été par Briggs (*Trigonometria britannica*, Goude, 1633). Voir *Mathesis*, 1907, p. 63.

[3] Cette proposition a été publiée d'abord par Schooten. Voir plus loin.

sorte que si, par l'examen direct, on prouve qu'elle l'est pour $n = 1$, elle l'est pour $n = 2$, puis pour $n = 3$, etc. Il démontre ainsi les deux formules principales des nombres figurés

$$C_{a,b} = C_{a,b-1} + C_{a-1,b-1}$$

$$C_{a,1} + C_{a,2} + C_{a,3} + \ldots\ldots + C_{a,b} = C_{a+1,b}.$$

Wallis, dans sa célèbre *Arithmetica infinitorum* (Oxford, 1655), a introduit dans la science, des idées nouvelles et hardies, qui furent critiquées; elles devaient cependant aboutir à la découverte de vérités importantes. Nous voulons parler de la relation

$$\int_0^1 (1 - x^2)^n = \frac{2 \cdot 4 \cdot 6 \ldots (2n)}{1 \cdot 3 \cdot 5 \ldots (2n-1)},$$

de l'*interpolation* des termes de la suite $1, \frac{2}{3}, \frac{2 \cdot 4}{3 \cdot 5}, \frac{2 \cdot 4 \cdot 6}{3 \cdot 5 \cdot 7}, \ldots$ qu'il suppose être différentes valeurs d'une fonction continue et qu'il représente par une courbe.

Schooten (*Exercitationum mathematicarum*, Leyde, 1657), a fait voir que le nombre total des combinaisons de n objets est $2^n - 1$, et a donné la liste des plus petits nombres ayant respectivement 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ... 100 diviseurs, lesquels sont 2, 4, 6, 16, 12, 64, 24, 36, 48, 1024, 60, ...

Le premier écrit où il est question des travaux arithmétiques de Fermat, est le *Commercium epistolicum*, de Wallis (Oxford, 1658). On y trouve les énoncés de différentes questions importantes dont celles-ci :

Trouver un cube qui, ajouté à ses diviseurs donne un carré, et un carré qui ajouté à ses diviseurs produise un cube ;

l'équation dite de Pell, $x^2 - ay^2 = 1$, dont Brouncker donne la solution pour $a = 13$[1];

les équations

$$x^2 + 2 = y^3, \quad x^2 + 4 = y^3, \quad a^3 + b^3 = x^3 + y^2 ;$$

---

[1] $E\omega$ désignant la valeur de la partie entière du nombre non entier ω, la solution de Brouncker revient à poser $x = (E\sqrt{13})\, y + a$, d'où $4y^2 = 6ay + a^2 - 1$ et de là une expression $4y_1 = 3a + \sqrt{13a^2 - 4}$ de la valeur de y; on pose de même $y = (Ey_1)\, y_1 + b$; et ainsi de suite. — La justification de cette solution n'a été donnée que par Lagrange.

l'impossibilité de partager un cube en deux autres cubes, et celle de trouver un triangle dont l'aire soit un carré ;

l'expression $2^{2^n} + 1$ *représente un nombre premier*[1] ;

tout nombre premier de la forme $4 + 1$ *est une somme de deux carrés ; tout nombre premier de la forme* $3 + 1$ *divise* $x^2 + 3y^2$; *tout nombre premier*[2] *de la forme* $8 - 1$ *est une somme de trois carrés.*

Mais c'est surtout dans la réédition, par le fils de Fermat, du *Diophantus* de Bachet (Toulouse, 1670), que l'on voit les monuments du génie de Fermat. Nous en citerons ce qui suit :

l'impossibilité de l'équation $x^a + y^a = z^a$, pour $a > 2$, non encore démontrée en général.

Si p *désigne un nombre premier de la forme* $4 + 1$, *les équations*

$$x^2 + y^2 = p^{2n-1} \quad \text{et} \quad x^2 + y^2 = p^{2n}$$

ont chacune n *solutions ;*

le produit $(a^2 + b^2)^{2n-k}(c^2 + d^2)^k$ *est, de* n *manières, la somme de deux carrés :* de là, le moyen de *déterminer le nombre de fois qu'un nombre peut être hypoténuse, ou un nombre qui soit* n *fois hypoténuse ;*

résoudre

$$x^3 + y^3 = a^3 + b^3 ;$$

théorème des nombres polygones : *tout entier est la somme de* n n^{gones} ;

trouver une infinité de triangles ayant même aire ;

l'aire d'un triangle ne peut s'exprimer par un nombre carré ; ce qui revient à dire qu'on ne saurait avoir $xy(x^2 + y^2) = z^2$. C'est la seule proposition sur la démonstration de laquelle Fermat ait laissé quelques indications. Il la démontre par la descente infinie dont nous avons déjà parlé[3]. Sa démonstration a été rétablie par Euler.

---

[1] Euler a reconnu que cette proposition est fausse. Fermat, qui la destinait à faciliter la recherche des nombres parfaits, y revient quatre autres fois, dans les écrits qui nous restent de lui. Il paraît l'avoir cherchée très longtemps.

[2] Legendre a reconnu que cette proposition a lieu pour un nombre impair quelconque de cette forme.

[3] S'agit-il de faire voir qu'une certaine propriété ne convient pas à un nombre désigné ? On cherchera un nombre plus petit qui jouisse de cette propriété, s'il en est de même du premier. De là un troisième nombre plus petit et dans les mêmes conditions. En continuant ainsi, on obtiendrait une suite infinie d'entiers décroissants, ce qui est absurde. L'hypothèse du point de départ est donc fausse. Voir par exemple *Mathesis,* 1905, p. 8.

La publication également posthume d'une partie de la correspondance de Fermat (*Opera varia*, Toulouse, 1679), permet d'apprécier encore mieux les découvertes de l'illustre géomètre, et quel regret on doit avoir de ce qu'il n'a pu faire connaître ses méthodes arithmétiques, que les savantes méthodes actuelles n'ont pu remplacer. On peut mentionner ce qui suit :

Tout nombre composé de trois carrés ne peut l'être de deux, même en fractions (*lettre à Mersenne*, 1636).

La méthode de *Maximis*[1] sert pour la recherche des nombres aliquotaires. Les nombres 672 et 120 sont doubles de la somme de leurs diviseurs[2], 220 et 284 sont amiables de même que 17296 et 18416[3]. Sommation des bicarrés et des nombres figurés. (*Diverses lettres à Roberval*, 1636.)

Il parle des progressions géométriques commençant à l'unité, dont il a envoyé de belles propositions à Frénicle; il rappelle qu'il a démontré qu'*aucun nombre de la forme* $4 - 1$ *n'est composé de deux carrés, ni entiers ni fractionnaires;* enfin il avance que *tout diviseur premier d'une somme de deux carrés premiers entre eux ne peut être de la forme* $4 - 1$, ce qui sert pour reconnaître si un nombre donné est premier (*lettre à Roberval*).

Nous sommes arrivé à l'importante *Lettre à Monsieur de* ***, dont il est nécessaire de donner une analyse détaillée. Fermat parle de certaines progressions dont les propriétés servent à trouver les diviseurs des nombres de la forme $a^n \pm 1$, et énonce ainsi le célèbre théorème qui a gardé son nom : «... il m'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 — 1, de quelque progression que ce soit, et l'exposant de ladite 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

---

[1] Le calcul différentiel.

[2] Voir sur ce sujet *Lettres de Descartes*, t. III, p. 392.

[3] Ces quatre nombres ont été trouvés par Descartes. Voir plus haut. Euler a longuement traité de ces nombres (Voir ses *Commentationes Arithmeticæ*, t. I, p. 402; t. II, pp. 627 et 637).

multiples de l'exposant de la première satisfont de même à la question. »

Ainsi on a :

$$3^1 \equiv 3\ ,\quad 3^2 \equiv 9\ ,\quad 3^3 \equiv 1 \qquad \text{(mod. 13)}$$

donc l'exposant 3 divise 13 — 1, et de plus $3^{3k} \equiv 1$ (mod. 13).

Si le *gaussien* [1], t de a est impair, on ne saurait avoir $a^x + 1 \equiv 0$. Ainsi $2^{11} \equiv 1$ (mod. 23) ; donc 23 ne divise aucun nombre de la forme $2^x + 1$. Si, au contraire, t est un nombre pair 2τ, on a . $a^\tau + 1 \equiv 0$.

La difficulté de l'application de cette théorie est dans la recherche du nombre premier p tel qu'on ne puisse écrire $a^x + 1 \equiv 0$, c'est-à-dire tel qu'il divise $a^t - 1$, t étant impair. Elle sert dans la recherche des nombres parfaits et à donner la raison de ce que, par exemple, $2^{37} \equiv 1$ (mod. 223).

Fermat donne encore ces deux théorèmes : *si* p *est un nombre premier de forme* 4 — 1, *et qu'on puisse trouver deux nombres* a *et* b *tels que* $a^{2k+1} \equiv b$, *on aura* $a^t \equiv 1$ *avec* t *impair* [2]. — *Aucun diviseur de* $a^2 - 2$ *n'est de la forme* $x^2 + 2$. (*Lettre à Monsieur de* ***, 1640.)

Si p *est premier, les diviseurs de* $2^p - 2$ *sont de la forme* 2ph *et deux de* $2^p - 1$, *de la forme* 2ph + 1. (*Lettre à Mersenne.*)

Il indique différents nombres aliquotaires (*lettre à Carcavi*), et énonce les propositions suivantes : *On arrive au théorème des nombres polygones en démontrant que tout nombre premier* 4 + 1 *est une somme de deux carrés.* — *Tout nombre premier* 3 + 1 *est de la forme* $x^2 + 3y^2$; et *tout nombre premier* 8 + 1 *ou* 8 + 3, *de la forme* $x^2 + 2y^2$. (*Lettre à Pascal*, 1654.)

Malgré de longues et minutieuses recherches, les écrits contenant les méthodes de Fermat n'ont pas pu être retrouvés, sauf trois lettres intéressantes, non datées, la seconde

---

[1] On appelle ainsi, d'après Ed. Lucas (l. cit.), l'exposant t de la plus petite puissance de a qui donne $a^t \equiv 1$, au lieu de la longue et vague dénomination de Gauss : *exposant appartenant à* a.

[2] Ce qui revient à dire que *a étant* résidu *de* p = 4 — 1, *on ne saurait avoir* $a^x + 1 \equiv 0$. Cela fait voir que Fermat sait que si a est résidu de p, en posant $p = 2m + 1$, on a : $a^m \equiv 1$, et que si pour k impair on a : $a^k \equiv 1$, on ne peut avoir pour $h < k$, $a^h \equiv -1$.

envoyée à Frénicle et la troisième à Huygens, et publiées dans le *B. Bon.* (l. cit.). Nous en donnons ici ce qu'il y a de plus important.

Tout impair non carré est autant de fois la forme $x^2 - y^2$ *qu'il est le produit de deux facteurs.* Soit à trouver les facteurs de $n = 2027651281$; par l'extraction de la racine carrée, on trouve $n = 45029^2 + 40440$. Le carré suivant surpasse n de $2 \cdot 45029 + 1 - 40440 = 49919$, nombre non carré, ce que ses deux derniers chiffres indiquent suffisamment. Le carré qui suit surpasse n de $49619 + 2 \cdot 45029 + 3 = 139680$, nombre non carré. Continuant ainsi, on trouve à la dixième opération, $45041^2 = n + 1020^2$; de là la décomposition $n = 46061 \cdot 44021$.

p *désignant un nombre premier, le nombre* $\frac{2^p + 1}{3}$ *est de la forme* $2ph + 1$. *Si* ab *n'est pas de la forme* 2^n, *le nombre* $2^{ab\ldots} + 1$ *se décompose aisément en ses facteurs* [1].

Enfin, dans la lettre à Huygens, Fermat apprend qu'il se servait de sa méthode de la descente pour démontrer: qu'*aucun facteur de la formule* $a^2 + 3b^2$ *ne peut être de la forme* $3 - 1$; *que la surface d'un triangle ne peut être un carré ni entier ni fractionnaire;* que *tout nombre premier* $4 + 1$ *est une somme de deux carrés;* le théorème de Bachet ; la solution de l'équation de Pell ; l'impossibilité de l'équation $x^3 + y^3 = z^3$; que *l'équation* $x^2 + 2 = y^3$ *a l'unique solution* $x = 5$; que *l'équation* $x^2 + 4 = y^3$ *n'a pas d'autres solutions que celles-ci* $x = 2$, $x = 11$. Il annonce que *l'équation* $(2x^2 - 1)^2 = 2y^2 - 1$ *n'a qu'une solution qui est* $x = 2$; et qu'il a des règles pour résoudre l'équation $ax^2 + b = y^2$, ou démontrer son impossibilité, et de même pour les équations simultanées $ax + b = y^2$, $ax + c = z^2$.

Maintes fois des doutes ont été émis, non sur la bonne foi de Fermat, mais sur la valeur de ses démonstrations ; il faut reconnaître que le seul de ses théorèmes qui ait été reconnu faux était énoncé par lui comme non démontré. D'ailleurs, le cas échéant, il reconnaît lui-même l'imperfection de cer-

[1] Par exemple, a, b, ... étant impairs, il est divisible par $2^a + 1$, par $2^b + 1$, par $2^{ab} + 1$, ... et chacun de ces facteurs est divisible par 3.

taines de ses méthodes, particulièrement dans la recherche des diviseurs numériques[1]. D'un autre côté, il a assez vivement critiqué Wallis de s'être servi de la simple induction dans les démonstrations de son *Arith. inf.* pour qu'on ne puisse croire qu'il avait agi de même. La science, en s'étendant et se perfectionnant, a perdu de sa simplicité, et il n'y a guère lieu de s'étonner que les procédés élémentaires de Frénicle, de S^te^-Croix et de Fermat nous échappent; et, même retrouvés, ils ne pourraient peut-être plus nous servir, l'habitude étant perdue des longs calculs numériques que ne craignaient pas d'entreprendre ces savants non encore habitués aux calculs de l'algèbre, plus mécaniques et moins suggestifs.

Nous terminons notre historique qui sera continué par l'*Œuvre arithmétique* d'Euler, de Lagrange, de Legendre et de Gauss par cette remarque que Fermat ne paraît avoir étudié que dans Euclide, Diophante, Viète et Bachet: ses découvertes paraissent avoir été faites entre 1630 et 1638 et avoir eu pour origine la considération des nombres parfaits ainsi que diverses questions proposées par Frénicle.

Deuxième Partie

Étude élémentaire sur le théorème de Fermat.

1. — *Lemmes*[2] I. *L'expression* $a^k - b^k$ *est algébriquement divisible par* $a - b$. De plus *si* k *est pair, elle l'est par* $a + b$; *si* k *est impair* $a^k + b^k$ *est divisible par* $a + b$.

En outre, *si* k *est multiple de* n, *et dans ce cas là seulement,* $a^k - b^k$ *est divisible par* $a^n - b^n$. Plus généralement, *si* θ *est le* p. g. c. d. *de* k *et de* n, $a^\theta - b^\theta$ *sera le* p. g. c. d. *de* $a^k - b^k$ *et de* $a^n - b^n$. Et ainsi des autres expressions.

---

[1] Cependant, dans une lettre à Mersenne de 1643, il donne la décomposition en facteurs d'un nombre de douze chiffres, qui lui avait été proposé.

[2] Nous donnons ces différents lemmes pour rendre cet article tout à fait indépendant des précédents (*Ens. Math.*, 1907, pp. 24 et 286).