ÉTUDE ÉLÉMENTAIRE SUR LE THÉORÉME DE FERMAT

Autor(en): **Aubry, A.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **9 (1907)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

Persistenter Link: 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).

Il suit de là qu'on a :

$$(1) \qquad (a + bh)^k \equiv a^k\,,\ (bh - 1)^{2k} \equiv 1\,,\ (bh - 1)^{2k+1} \equiv -1 \pmod{b}$$

II. Dans cette identité d'Euler[1]

$$(2) \qquad (1 + a)(1 + b) \ldots (1 + l) = 1 + a + b(1 + a) + \ldots + l(1 + a) \ldots (1 + k)\,,$$

changeons a, b, c, ... en $\frac{n}{1}$, $\frac{n}{2}$, $\frac{n}{3}$, ... il viendra la formule des nombres figurés

$$(3) \qquad 1 + C_{n,1} + C_{n+1,2} + C_{n+1,3} + \ldots + C_{n+\nu-1} = C_{n+\nu,\nu}\,;$$

d'où l'identité de Nicole,

$$(4) \qquad 1.2.3 \ldots n + 2.3 \ldots (n + 1) + 3.4 \ldots (n + 2) + \ldots + \nu \ldots (\nu + n - 1) = \frac{\nu \ldots (\nu + n)}{n + 1}\,.$$

III. *Le nombre*

$$C_{a,b} = \frac{a(a - 1)(a - 2) \ldots (a - b + 1)}{b\,!}$$

est entier (Pascal). De plus, si p est premier, on a

$$(5) \qquad C_{p,n} \equiv 0 \qquad \text{(Euler)}$$

IV. On a :

$$(6) \qquad (a + b)^n = a^n + C_{n,1}\,a^{n-1}b + \ldots + C_{n,n-1}\,ab^{n-1} + C_{n,n}\,b^n \qquad \text{(Briggs)}$$

d'où, à cause de (5), si p est premier,

$$(7) \qquad (a + b)^p \equiv a^p + b^p \qquad \text{(Euler)}$$

V. Posons

$$x^n = x(x - 1) \ldots (x - n + 1) + Ax \ldots (x - n + 2) + \ldots + Mx(x - 1) + x\,,$$

A, B, ... L, M désignant des coefficients qu'il n'est pas indispensable de déterminer, on aura :

[1] Pour d'autres applications de cette identité, voir *Progreso Matematico*, 1900, p. 401 et *Mathesis*, 1907, p. 147.

$$x^{n+1} - x^n = x(x-1)\dots(x-n) + \mathrm{A}x\dots(x-n+1) + \dots +$$
$$\mathrm{M}x(x-1)(x-2) + x(x-1) ;$$

d'où, sommant de $x = 1$ à $x = p-1$, et posant

$$s_k = 1^k + 2^k + 3^k + \dots + (p-1)^k ,$$

$$s_{n+1} - s_n = \frac{p\dots(p-n-1)}{n+2} + \mathrm{A}\frac{p\dots(p-n)}{n+1} + \dots +$$
$$\mathrm{M}\frac{p\,.\,(p-3)}{4} + \frac{p\dots(p-2)}{3}$$

Par suite si

$$n < p-1 ,$$

on a :

$$s_{n+1} - s_n \equiv 0 \ [1] .$$

Or

$$s_1 = \frac{p(p-1)}{2} \equiv 0 ,$$

donc

$$s_2 \equiv 0 , \ s_3 \equiv 0 , \dots$$

(8) $$s_n \equiv 0 . \qquad (n < p-1)$$

(9) $$s_{p-1} \equiv -(p-1)\,!$$

VI. Supposons que la congruence du n^{e} degré $\mathrm{F}(x) \equiv 0$ ait $n+1$ racines, et soient a, b, ... c les $p-n-2$ non-racines ; la congruence du $(p-2)^{\mathrm{e}}$ degré

$$(x-a)(x-b)\dots(x-c)\,\mathrm{F}(x) \equiv 0$$

aurait évidemment $p-1$ racines. Or soit $\mathrm{A}x^{p-2} + \mathrm{B}x^{p-3} + \dots + \mathrm{L}x + \mathrm{M} \equiv 0$ cette dernière congruence ; en y faisant successivement $x = 1, 2, 3, \dots p-1$ et faisant intervenir le lemme V, on aurait en sommant,

$$\mathrm{M}(p-1) \equiv 0 \quad \text{ou} \quad -\mathrm{M} \equiv 0$$

ce qui ne peut avoir lieu que si $\mathrm{M} \equiv 0$, chose impossible, puisque le produit M de toutes les racines ne peut être multiple de p.

Il est donc impossible que la congruence $\mathrm{F}(x) \equiv 0$ ait plus de n racines.

---

[1] Quand le module n'est pas explicitement indiqué, il s'agit du nombre premier p.

Cor. Si la congruence $F(x) \equiv 0$ a n racines et que son premier membre puisse se décomposer en deux facteurs entiers $f(x)$, $\varphi(x)$, de degrés k et $n - k$, les deux congruences ont respectivement k et $n - k$ racines. (Lagrange).

VII. Posons

$$0 < k \pm 1 < 5 , \quad kA^2 \pm B^2 = nn' , \quad n > n' ,$$
$$k(A - n'a)^2 \pm (B - n'b)^2 = n'n'',$$

et prenons a et b tels qu'on ait

$$A - n'a < \frac{n'}{2} \gtrless B - n'b ;$$

il viendra

$$n'n'' < \frac{k \pm 1}{4} n'^2 \leq n'^2 \quad \text{d'où} \quad n'' < n' .$$

Or, en tenant compte de cette identité d'Euler

$$(10) \quad (kA^2 \pm B^2)(kA'^2 \pm B'^2) = (kAA' \mp BB')^2 \pm k(AB' - A'B)^2,$$

on a :

$$(nn')(n'n'') = (kA^2 \pm B^2 - kAA'n' \mp BB'n')^2 \pm k(BA' - AB')^2 n'^2 ,$$

d'où, en remplaçant $kA^2 \pm B^2$ par nn',

$$nn'' = (n - kAA' \mp BB')^2 \pm k(BA' - AB')^2 .$$

On a ainsi un second multiple de n inférieur au proposé, et de la forme $\alpha^2 \pm k\beta^2$.

Opérant de même sur cette expression, on en tirera un troisième multiple nn''' de la même forme et ainsi de suite, jusqu'à ce qu'on arrive au nombre n lui-même, puisque les nombres $n, n', n'', \ldots$ sont de plus en plus petits. Le nombre n est donc de l'une des formes $kx^2 \pm y^2$ ou $x^2 \pm ky^2$.

Ainsi *les diviseurs de* $A^2 + 3B^2$, *de* $A^2 + 2B^2$ *et de* $A^2 + B^2$ *sont respectivement des formes* $x^2 + 3y^2$, $x^2 + 2y^2$ et $x^2 + y^2$. *Ceux de* $A^2 - 3B^2$ *peuvent se mettre sous l'une des deux formes* $x^2 - 3y^2$, $3x^2 - y^2$. Et, à cause des identités

$$x^2 - 2y^2 = 2(x - y)^2 - (x - 2y)^2$$
$$x^2 - 5y^2 = 5(x - 2y)^2 - (2x - 5y)^2 ,$$

on peut encore dire que *les diviseurs de* $A^2 - 2B^2$ *et de* $A^2 - 5B^2$ *peuvent se mettre respectivement sous les formes* $x^2 - 2y^2$ *et* $x^2 - 5y^2$.

Le principe de cette démonstration est dû à Lagrange, qui a prouvé ainsi que *tout diviseur d'une somme de quatre carrés est lui-même une somme de quatre carrés.* Euler avait ouvert la voie, en essayant de démontrer de cette manière les cas de $A^2 + B^2$, de $A^2 + 2B^2$ et de $A^2 + 3B^2$.

2. — Les nombres a, b étant premiers entre eux, on peut se demander quelles sont les propriétés des restes obtenus en divisant par b les multiples ou bien les puissances de a. L'étude du premier cas a fait l'objet de notre précédent article. Le second cas va nous occuper; mais auparavant, il convient de montrer, par quelques exemples, comment on peut souvent abréger le calcul direct des restes.

1° Soit à trouver $R\frac{7^{160}}{641}$. La division des nombres 7, 7^2, 7^4, 7^8, 7^{16}, 7^{32}, 7^{64}, 7^{128} donne les restes 7, 49, 343, 478, 288, 255, 284, — 110, — 79; donc

$$7^{160} \equiv -284.79 \equiv -1 \qquad \text{(mod. 641) (Euler)}$$

2° Trouver le reste de la division de 3^{1000} par 13. On a $3^3 \equiv 1$ (mod. 13), et comme $1000 \equiv 1$ (mod. 3), il s'ensuit $3^{1000} \equiv 3$ (mod. 13). (Gauss).

3° Soit à trouver les restes des puissances de $a = 189$ divisées par $b = 191$.

On trouve directement les restes 1, 189, 4, 183, 16, 159, 64, 63, ... On a ainsi :

$$a^7 \equiv a^6 - a^0 \text{ , d'où } a^8 \equiv a^7 - a^1 \text{ , } a^9 \equiv a^8 - a^2 \text{ , ...} \qquad \text{(mod. 191)}$$

De même, pour $b = 19$ et $a = 3, 4, 5, 6$, on pourra utiliser les relations

$$2a^2 + 1 \equiv 0 \text{ , } a^2 - a - 1 \equiv 0 \text{ , } a^2 - a - 1 \equiv 0 \text{ , } a^2 + 2 \equiv 0 \qquad \text{(mod. 19) (Desmarets)}$$

4° Enfin nous ferons remarquer que, pour les restes des puissances de $a = \frac{b \pm 1}{2}$, on a :

$$2a \pm 1 \equiv 0 \text{ , } 2a^2 \pm a \equiv 0 \text{ , } 2a^3 \pm a^2 \equiv 0 \text{ , ...} \qquad \text{(mod. } b\text{)}$$

3. — *Si* a *est premier avec* b, *il y a toujours dans la progression* a, a^2, a^3, ... a^{b-1}, *au moins un terme* a^t *qui, divisé par* b *donne le reste* 1. *Les restes suivants se reproduisent périodiquement.* (Euler 1759). Aucun reste n'étant nul, parmi les b premiers restes, il y en a au moins deux qui sont égaux. Posons en conséquence :

$$a^x \equiv c \ , \ a^y \equiv c \ , \quad \text{il viendra} \quad a^y(a^{x-y} - 1) \equiv 0 \pmod{b}$$

ce qui démontre la première partie de la proposition. La deuxième se vérifie en observant que de $a^t \equiv 1$, $a^n \equiv \alpha$ (mod. b), on tire $a^{t+n} \equiv \alpha$ (mod. b).

Cor. I. Si t est le *gaussien*[1] de a, tous les restes qui précèdent sont différents. Autrement le raisonnement de tout à l'heure ferait voir qu'il y a une puissance plus petite qui donne le reste 1, et t ne serait pas le gaussien de a.

II. De ce qu'on peut toujours écrire $a^t \equiv 1$ (mod. b), on conclut que tout entier a premier avec b a toujours un *associé* $\alpha = a^{t-1}$, c'est-à-dire un nombre tel que $a\alpha \equiv 1$ (mod. b).

III. a et c étant premiers avec b, on peut toujours écrire

$$a^t \equiv 1 \ , \ c^s \equiv 1 \ , \quad \text{d'où} \quad a^t - c^s = kb \pmod{b}$$

multipliant par c et posant $ca^{t-1} \equiv x$, $kc \equiv y$ (mod. b), cette équation devient

$$(\alpha) \qquad ax - by = c \ ,$$

Ainsi, a *et* c *étant premiers avec* b, *on peut toujours trouver un nombre* x $<$ b, *tel que la relation* α *ait lieu.*

Autrement. Les b nombres

$$a^{b-1}, \ a^{b-2}c \ , \ a^{b-3}c^2, \ \ldots \ a^2c^{b-3}, \ ac^{b-2}, \ c^{b-1}$$

sont incongrus à b : il y en a donc au moins deux qui sont congrus entre eux. Posons en conséquence :

$$a^{k-1}c^{b-k} \equiv a^{k-1+h}c^{b-k-h} \pmod{b}$$

ce qui donnera

$$(\beta) \qquad c^h \equiv a^h \pmod{b}$$

[1] Exposant de la plus petite puissance de a qui donne $a^x \equiv 1$ (mod. b).

Il existe donc un nombre h inférieur à b permettant de satisfaire à (β). Le reste de la démonstration s'achève comme tout à l'heure.

IV. *Si* $a^x \equiv 1 \pmod{b}$, x *est forcément un multiple du gaussien* t.

V. Les t restes sont évidemment premiers avec le diviseur b, de sorte que si, avec Gauss, on désigne par $\varphi(b)$ le nombre des entiers plus petits que b et premiers avec lui, on a $t \leq \varphi(b)$.

Si $t < \varphi(b)$, soient 1, α, α'', ... les t restes, et β, γ, δ, ... les autres nombres inférieurs à b et premiers avec lui. En divisant par b les nombres β, $\beta\alpha$, $\beta\alpha'$, $\beta\alpha''$, ... on aura t restes différant entre eux et différents des premiers, puisque, en posant, par exemple,

$$a^f \equiv \alpha \ , \ a^g \equiv \alpha' \pmod{b}$$

aucune des expressions suivantes, où $f < g < t$,

$$\beta a' - \beta a \equiv \beta a^f (a^{g-f} - 1) \ , \ \alpha' - \beta\alpha \equiv a^f (a^{g-f} - \beta) \pmod{b}$$

ne peut se réduire à un multiple de b ; car a^{g-f} n'est ni $\equiv 1$ (mod b), ni $\equiv \beta$ (mod. b), puisque $g - f < t$ et que le reste correspondant ne peut être que α, ou α', ou α'', ...

Opérons de même sur les restes γ, δ, ... nous finirons par épuiser complètement la suite des nombres $< b$ et premiers avec lui. Cette suite est donc partagée en groupes de t termes et par suite $\varphi(b)$ est un multiple de t. Par conséquent t est égal à $\varphi(b)$ on à un diviseur de $\varphi(b)$. (Euler 1758).

4. — *Théorème d'Euler. Si les nombres* a *et* b *sont premiers entre eux, on a :*

$$a^{\varphi(b)} \equiv 1 \pmod{b} \tag{11}$$

En effet $\varphi(b)$ est un multiple de t, d'après le corollaire qui précède.

5. — *Théorème de Fermat.* Si b est un nombre premier p, on a $\varphi(p) = p - 1$, d'où

$$a^{p-1} \equiv 1 \ . \tag{12}$$

Autrement. De (7) on tire :

$$(x + 1)^p - x^p \equiv 0 \ ,$$

d'où, en changeant successivement x en $a - 1$, $a - 2$, ... 3, 2, 1 et additionnant, la relation

$$a(a^{p-1} - 1) \equiv 0 , \tag{13}$$

identique à (12). (Euler 1748).

Cor. I. Quel que soit l'entier x, on a :

$$x^p - x \equiv 0 . \tag{14}$$ (Euler)

La grande importance du théorème de Fermat résulte de ce fait caractéristique que la congruence (14) quoique non identique, est satisfaite pour x quelconque. Il fait partie du petit nombre de ces vérités simples et fécondes, — telles qu'en géométrie, le théorème de Pythagore et celui des triangles semblables, — lesquelles, condensant en une seule idée un grand nombre de principes en apparence distincts, — parce que la faiblesse de notre intelligence nous empêche de voir qu'ils n'en font souvent qu'un seul vu sous des aspects différents, — nous permettent de ménager nos efforts dans la conquête de nouvelles vérités et d'envisager de nouveaux buts. Aussi les diverses généralisations élémentaires qui ont été données de ce théorème sont-elles restées à peu près sans emploi et ne présentent-elles guère d'autre intérêt que celui d'exercices isolés.

II. Puisque $p - 1$ est un nombre impair, on a, en posant $p = 2m + 1$:

$$(a^m + 1)(a^m - 1) \equiv 0 \tag{15}$$

Les deux facteurs du premier membre ne peuvent avoir d'autre facteur commun que 2 ; on a donc :

$$a^m + 1 \equiv 0 \text{ ou } a^m - 1 \equiv 0 \tag{16}$$

III. *Théorème de Wilson.* De (9) et de (12), on tire

$$(p - 1)! + 1 \equiv 0 \tag{17}$$

IV. 1° Supposons $p = 4q + 1$ et soit $x = a$ une des non-racines de $(x + 1)^{2q} - x^{2q} \equiv 0$. Puisque $(a + 1)^{4q} - a^{4q} \equiv 0$, il s'ensuit que $(a + 1)^{2q} + a^{2q} \equiv 0$. Ainsi $p = 4 + 1$ *divise toujours une somme de deux carrés.* D'ailleurs aucun nombre

premier $p = 4 - 1$ ne peut diviser $x^2 + y^2$; en effet on a : $x^{p-1} - y^{p-1} \equiv 0$; donc en posant $p = 2m + 1$, on voit que $(x^2)^m + (y^2)^m$ ne peut être $\equiv 0$. Or cette expression est divisible par $x^2 + y^2$ puisque m est impair ; donc a fortiori p ne peut diviser $x^2 + y^2$ (Euler).

2° Selon que u et v sont de même parité ou de parité différente, $u^2 + uv + v^2$ peut se mettre sous l'une ou l'autre des deux formes

$$\left(\frac{u - v}{2}\right)^2 + 3\left(\frac{u + v}{2}\right)^2 \quad \text{ou} \quad \left(\frac{2u + v}{2}\right)^2 + 3\left(\frac{u}{2}\right)^2.$$

Donc si $x = a$ est une non-racine de $(x + 1)^{2n} - x^{2n} \equiv 0$, le nombre $p = 6k + 1$ étant premier, on aura :

$$[(a + 1)^{2k} - a^{2k}]\,[(a + 1)^{4k} + (a + 1)^{2k} a^{2k} + a^{4k}] = (a + 1)^{6k} - a^{6k} \equiv 0 ;$$

donc $p = 6 + 1$ divise $y^2 + 3z^2$ (Euler).

V. Chacune des congruences $x^m + 1 \equiv 0$, $x^m - 1 \equiv 0$ a m racines (lemme VI).

La congruence $x^{p-1} - 1 \equiv 0$ a les $p - 1$ racines $1, 2, 3, \ldots p - 1$, ou si l'on veut, les nombres $\pm 1, \pm 2, \pm 3, \ldots \pm m$. De là, les relations

$$(18) \qquad (x - 1)(x - 2)\ldots(x - p + 1) - x^{p-1} + 1 \equiv 0$$

$$(19) \qquad (x^2 - 1)(x^2 - 4)\ldots(x^2 - m^2) - x^{p-1} + 1 \equiv 0 .$$

Ces deux congruences, bien que du degré $p - 2$, ont $p - 1$ racines : elles sont donc identiques, et, en les développant, les coefficients seront tous $\equiv 0$ (Lagrange).

VI. Plus généralement, si f est un diviseur de $p - 1$, la congruence $x^f - 1 \equiv 0$ a f racines (Euler). Ainsi selon que $p = 4 \mp 1$, la congruence $x^4 - 1 \equiv 0$ a deux ou quatre racines.

VII. 1° Soit $p = 4q + 1$, on aura pour certaines valeurs de x,

$$x^{2q} + 1 \equiv 0 .$$

donc $p = 4 + 1$ *divise une somme de deux carrés et est par suite une somme de deux carrés.* (Fermat). On utilise le lemme VII.

2° Soit $p = 8q + 1$, il viendra

$$0 \equiv x^{4q} + 1 = (x^{2q} \mp 1)^2 \pm 2q\,(x)^2$$

par conséquent $p = 8 + 1$ *divise certains nombres des deux formes* $y^2 \pm 2z^2$ *et par suite il est de ces deux formes.* (Lemme VII).

3° Soit $p = 8q + 3$; la valeur $x = 2$ rend incongru à p le second facteur du produit $(x^{4q+1} + 1)(x^{4q+1} - 1)$, puisqu'il est alors de la forme $2y^2 - 1$, laquelle ne convient pas à la forme $8q + 3$, que y soit pair ou qu'il soit impair. On a donc :

$$0 \equiv 2^{4q+1} + 1 = 2y^2 + 1,$$

ce qui fait voir que *les nombres premier* $8 + 3$ *sont diviseurs de nombres de la forme* $2y^2 + z^2$ *et par suite sont de la même forme.*

4° Soit $p = 8q + 7$; on a :

$$0 \equiv (2^{4q+3} + 1)(2^{4q+3} - 1).$$

p ne peut diviser $2^{4q+3} + 1$, ni par suite $2^{4q+4} + 2$, car il serait de la forme $2y^2 + 2$, qui ne peut se réduire à la forme $8q + 7$. On a, par conséquent :

$$0 \equiv 2^{4q+4} - 2 \equiv y^2 - 2.$$

Donc *les nombres premiers* $8 + 7$ *sont diviseurs de* $y^2 - 2z^2$ *et sont de la même forme.*

5° La comparaison de ces quatre théorèmes fait voir que leurs réciproques sont vraies.

6° Si $p = 3 + 1$, la congruence $x^3 - 1 \equiv 0$ a trois racines, puisque son premier membre divise $x^{p-1} - 1$. Soit a une de ces racines ; on aura :

$$(a - 1)(a^2 + a + 1) \equiv 0 \quad \text{d'où} \quad a^2 + a + 1 \equiv 0 \quad \text{et} \quad (2a + 1)^2 + 3 \equiv 0.$$

Donc *tout nombre premier* $3 + 1$ *divise* $x^2 + 3y^2$, *et par suite est de la même forme.*

7° Soit $p = 5 + 1$; il viendra, en appelant a une des racines de $x^5 - 1 \equiv 0$,

$$(a - 1)(a^4 + a^3 + a^2 + a + 1) \equiv 0, \quad \text{d'où} \quad (2a^2 + a + 2)^2 - 5a^2 \equiv 0.$$

Donc *tout nombre premier* $5 + 1$ *divise* $x^2 - 5y^2$, *et par suite est de la même forme.*

8° Enfin soit $p = 7 + 1$ et soit a une racine de $x^7 - 1 \equiv 0$; il viendra :

$$(2a^3 + a^2 - a - 2)^2 + 7(a^2 + a)^2 \equiv 0.$$

Donc *tout nombre premier* $7 + 1$ *divise* $x^2 + 7y^2$.

Ces démonstrations sont dues à Euler (1°, 2°, 7° et 8°) et à Lagrange (3°, 4° et 6°). Gauss a fait voir que A et A′ désignant certains polynomes entiers en a, selon que $p = 4 \pm 1$, on a :

$$4\frac{a^p - 1}{a - 1} = A^2 \pm pA'^2 ;$$

mais la *loi de réciprocité,* qui sera donnée plus tard, dispense d'entrer dans plus de détails à ce sujet.

6. — Si t est le gaussien de a, p est de la forme $th + 1$ (Euler). En effet t divise $p - 1$, donc $p \equiv 1 \pmod{t}$.

Cor. I. Si t est premier, tout facteur premier impair de $a^t - 1$, qui ne l'est pas de $a - 1$ est de la forme $2th + 1$. De plus, il est de la forme quadratique $x^2 - ay^2$, car de $a^t - 1 \equiv 0$, on tire

$$\left(a^{\frac{t+1}{2}}\right)^2 - a \equiv 0 .$$

II. Si t est premier, tout facteur premier de $2^t - 1$ est de de la forme $2th + 1$ (Fermat), et de l'une des formes 8 ± 1, car il divise $2^{t+1} - 2$, qui est de la forme $x^2 - 2$. (Euler).

Ainsi les facteurs premiers de $2^{31} - 1$ étant à la fois $62 + 1$ et 8 ± 1, on trouvera aisément qu'ils appartiennent à l'une des formes $248 + 1$, $248 + 63$. Essayant la division par les nombre premiers de ces deux formes, Euler s'est assuré que $2^{31} - 1$ est premier, comme l'avait affirmé Fermat.

III. Tout diviseur impair p de $a^t + 1$ est de la forme $2th + 1$. En effet p divise $a^{2t} - 1$; or il ne divise aucun nombre $a^n - 1$, où n serait diviseur de $2t$, car il diviserait aussi $a^t - 1$, ce qui ne peut être, puisqu'il divise $a^t + 1$, et que les deux nombres $a^t - 1$ et $a^t + 1$ n'ont d'autre diviseur commun que 2.

Application. Fermat avait pensé que la formule $2^{2^n} + 1$ ne

renferme que des nombres premiers. Euler a prouvé ainsi l'inexactitude de cette proposition. Les diviseurs de $2^{32}+1$ sont de la forme $\mathbf{64}+1$; or les nombres premiers de cette forme $< \sqrt{2^{32}+1}$ sont 193, 257, 449, 641... Essayant la division de $2^{32}+1$ par ces nombres, on trouve qu'elle réussit avec 641 [1].

Depuis, on a trouvé de même que pour $n = 5, 6, 9, 11, 12, 18, 23, 36, 38$, le nombre $2^{2^n}+1$ est composé. Il y en a probablement une infinité dans ce cas.

Cette méthode d'Euler a été l'objet d'importantes extensions. Voici la plus simple, due à Ed. Lucas: *les diviseurs de* $2^{32}+1$ *sont de la forme* $\mathbf{128}+1$ (7, *Appl.*). On a donc à considérer seulement les nombres premiers de cette forme, dont le premier est 641. L'examen des diviseurs à exclure est ainsi considérablement réduit.

7. — *Résidus et non-résidus.* Le reste de la division de a^m par p est, comme on sait, 1 ou — 1. Le nombre a est appelé *résidu* de p dans le premier cas et *non-résidu* dans le second [2]: la raison de ces dénominations est que, suivant qu'on a $a^m \equiv \pm 1$, on peut ou on ne peut écrire $x^2 \equiv a$. En effet :

1° Supposons qu'on pût écrire $x^2 \equiv a$ avec $a^m \equiv -1$, on aurait

$$x^{p-1} = a^m \equiv -1 ,$$

ce qui est faux, car $x^{p-1} \equiv 1$; a n'est donc pas un résidu.

2° Soit $a^m \equiv 1$, on a la congruence

$$x^{p-1} - a^m \equiv 0$$

qui a $p-1$ racines. Or le premier membre est divisible par $x^2 - a$, donc la congruence $x^2 - a \equiv 0$ a deux racines, et a est résidu.

Cor. I. *Le produit de plusieurs nombres est un résidu ou un non-résidu selon que le nombre des non-résidus qui entrent comme facteurs dans ce produit est pair ou impair.*

---

[1] On peut être surpris que Fermat, qui avait fait tous les frais de cette démonstration, en ait laissé l'honneur à Euler. D'après Plana, il ne paraît pas avoir non plus remarqué les deux formes des diviseurs de $2^t - 1$. (*Mém. sur la th. des n,* Turin, 1859.)

[2] Nous rappelons que partout m est mis pour $\frac{p-1}{2}$.

II. *La congruence*

$$(\alpha) \qquad x^2 - ay^2 \equiv b$$

est toujours possible (Lagrange). Il faut démontrer qu'au moins un résidu de p est de la forme $ay^2 + b$, ou que la congruence

$$(\beta) \qquad (ay^2 + b)^m \equiv 1$$

pou toujours avoir lieu. Or la congruence conjuguée $(ay^2 + b)^m \equiv -1$ est du degré $p - 1$ et ne saurait avoir $p - 1$ racines. Elle a donc au moins une non-racine, qui satisfait à (β) et par suite à (α).

III. Si $p = 4 + 1$, a et $-a$ seront ensemble résidus ou non-résidus. Si $p = 4 - 1$, l'un est résidu et l'autre non-résidu. On a en effet, selon l'un ou l'autre cas,

$$a^m(-a)^m = \pm (a^2)^m .$$

IV. 1° Si $p = 8 \pm 1$, on aura :

$$2y^2 \equiv x^2 \quad \text{d'où} \quad 2^m y^{p-1} \equiv x^{p-1} ,$$

ou bien

$$(18) \qquad 2^m \equiv 1 . \qquad (p = 8 \pm 1)$$

2° Si $p = 8 + 3$, on aura :

$$2y^2 \equiv -x^2 , \quad \text{d'où} \quad 2^m y^{p-1} \equiv -x^{p-1} \equiv -1 .$$

Donc

$$(19) \qquad 2^m \equiv -1 . \qquad (p = 8 + 3)$$

3° Si $p = 8 + 5$, p ne peut être de la forme $x^2 - 2y^2$; on ne peut donc écrire $2^m \equiv 1$ et par suite on a :

$$(20) \qquad 2^m \equiv -1 . \qquad (p = 8 + 5)$$

4° En résumé on a :

$$(21) \qquad 2^m \equiv (-1)^{\frac{p^2-1}{8}} .$$

Applications. 1° *Selon que* p *est de l'une des formes* 8 ± 1 *ou de l'une de celles-ci* 8 ± 3, p *divise* $2^m - 1$ *ou* $2^m + 1$. (Euler.)

2° Soit $p = 8hk + 1$ un diviseur premier de $2^{4h} + 1$ (6, III). k est pair; autrement, en élevant à la puissance de degré impair k la congruence $2^{4h} \equiv 1$, on aurait $2^m \equiv -1$ ce qui ne peut être puisque 2 est résidu de p. Ainsi tout diviseur de $2^{4h} + 1$ est de la forme $16h + 1$. (Ed. Lucas.)

8. — *Racines primitives.* On appelle *racine primitive* de p un nombre dont les $p - 1$ premières puissances divisées par p donnent pour restes la totalité des nombres 1, 2, 3, ... $p - 1$.

Le nombre premier p *a* $\varphi(p - 1)$ *racines primitives* (Euler). Démonstration de Gauss. 1° Décomposons $p - 1$ en ses facteurs premiers, et soit $p - 1 = 2^\omega a^\alpha b^\beta c^\gamma \ldots$ soit g une des non-racines de $x^{\frac{p-1}{a}} \equiv 1$, et posons

$$g^{\frac{p-1}{a^\alpha}} \equiv A, \quad \text{d'où} \quad A^{a^\alpha} \equiv g^{p-1} \equiv 1.$$

L'exposant de toute puissance inférieure de A congrue à l'unité doit diviser a^α et elle ne peut être que de la forme $A^{a^{\alpha-k}}$. Or ce nombre ne peut être congru à 1, puisque son multiple

$$A^{a^{\alpha-1}} \equiv g^{\frac{p-1}{a}}$$

ne l'est pas : on peut donc toujours trouver un nombre A tel que a^α soit congru à l'exposant de la plus petite puissance congrue à 1 (gaussien de A).

2° Soient B, C, ... les nombres formés de la même manière avec b^β, c^γ, ... et posons $(ABC\ldots)^t \equiv 1$. L'un des facteurs premiers de $p - 1$, a par exemple, divise donc $\frac{p-1}{t}$, et par suite

$$(\alpha) \qquad (AB\ldots)^{\frac{p-1}{a}} \equiv 1.$$

Or les nombres b^β, c^γ, ... divisent $\frac{p-1}{a}$, donc on a :

$$B^{\frac{p-1}{a}} \equiv 1, \quad C^{\frac{p-1}{a}} \equiv 1, \ldots$$

et par suite, à cause de (α)

$$A^{\frac{p-1}{a}} \equiv 1 .$$

a^α diviserait donc $\frac{p-1}{a}$, ce qui est faux, car $\frac{p-1}{a^{\alpha+1}}$ n'est pas entier. Le nombre $p-1$ est donc le gaussien de (AB...).

3° [1] Soit R la racine primitive (AB...) dont l'existence vient d'être prouvée. Si θ est le *p. g. c. d.* de $p-1$ et de h, on a :

$$(R^h)^{\frac{p-1}{\theta}} = (R^{\frac{h}{\theta}})^{p-1} \equiv 1 .$$

Si $\theta > 1$, le gaussien de (R^h) est $< p-1$, et (R^h) n'est pas une racine primitive. Si $\theta = 1$, h est premier avec $p-1$ et, en appelant t le gaussien de (R^h), on a :

$$R^{ht} = (R^h)^t \equiv 1 ;$$

donc ht est diviseur de $p-1$ et ne peut être que $p-1$.

Ainsi (R^h) sera racine primitive ou non selon que h sera ou ne sera pas premier avec $p-1$.

Cor. I. a, b, c, ... désignant les nombres inférieurs à $p-1$ et premiers avec lui, les termes de la suite R, R^a, R^b, ... sont congrus à toutes les racines primitives.

II. Conservant les mêmes notations, on verra que parmi les racines primitives, R, R^a, R^b, ... il y en a deux dont la somme des exposants est égale à $p-1$. Les racines primitives sont donc associées et par suite leur produit est $\equiv 1$. (Gauss.)

III. Les racines non-primitives ne sont autres que les résidus des puissances dont les exposants ne sont pas premiers avec $p-1$. Ainsi : 1°, 2 et 3 étant les facteurs premiers de $13-1$, les racines non-primitives de 13 sont les résidus quadratiques et les résidus cubiques de ce nombre.

2° Si p est de la forme $2^h + 1$, (ce qui a lieu pour $h = 2, 4, 8, 16$), les racines primitives se confondent avec les non-résidus quadratiques.

3° Si h étant premier, $p = 2h + 1$ (les valeurs $p = 7, 11,$

---

[1] Cette troisième partie de la démonstration avait été donnée antérieurement par Euler.

23, 47, 59, 83, 107, 167, 179, 227, 263, ... sont dans ce cas), les racines primitives sont également les non-résidus, sauf le non-résidu $p - 1 = 2h$.

IV. Les racines de $x^{\frac{p-1}{a}} \equiv 1$, $x^{\frac{p-1}{b}} \equiv 1$, ... sont toutes non-primitives ; donc la congruence

$$\frac{(x^{p-1} - 1)\,\mathrm{X}}{\left(x^{\frac{p-1}{a}} - 1\right)\left(x^{\frac{p-1}{b}} - 1\right)\ldots} \equiv 0 .$$

donne toutes les racines primitives, X désignant la congruence ayant pour racines les racines communes aux facteurs du dénominateur.

Quand $p - 1$ est de la forme $2^{\omega}a^{\alpha}$, on a :

$$\mathrm{X} = x^{\frac{p-1}{2a}} - 1 \quad \text{d'où} \quad \frac{x^{\frac{p-1}{2}} + 1}{x^{\frac{p-1}{2a}} + 1} \equiv 0 ,$$

pour la congruence des racines primitives. Le premier membre divisant $x^{p-1} - 1$, la congruence a toutes ses racines, lesquelles sont ainsi au nombre de

$$\frac{p-1}{2} - \frac{p-1}{2a} .$$

Par exemple, pour $p = 13$ on trouve la congruence $x^4 - x^2 + 1 \equiv 0$, dont les quatre racines, 2, 6, 7, 11. sont les racines primitives de 13. (Cauchy.)

Exercices.

I. Posons

$$1^q + 2^q + 3^q + \ldots + n^q = s_{n.q} , \quad 1^q - 2^q + 3^q - \ldots \pm n^q = \sigma_{n,q} :$$

on aura :

$$\left.\begin{aligned} &\sigma_{2n,q} \equiv 0 , \text{ dans tous les cas ;} \\ &\sigma_{n-1,q} \equiv 0 , \ n \text{ impair et } q \text{ pair ;} \\ &s_{n-1,q} \equiv 0 , \ n \text{ et } q \text{ impairs, } n > q ; \\ &s_{n,q} - 2\,s_{\frac{n-1}{2},\,q} \equiv 0 , \ n \text{ et } q \text{ pairs ;} \end{aligned}\right\} \quad (\text{mod. } n).$$

2. Tout nombre premier, autre que 2 et 5, divise une infinité de nombres formés de chiffres 9 (Crelle) ou de chiffres 1 (Plateau).

3. On a :

$$C_{p-1,\,n-1} \equiv 0 \text{ (mod. } n) \qquad \text{(D. André.)}$$

$$C_{p-1,\,n} \equiv \pm 1 \qquad \text{(Catalan.)}$$

$$(pq)\,! \text{ multiple de } (q\,!)^p\, p\,! \qquad \text{(Weill.)}$$

4. 1° Si le gaussien t de a est un nombre pair 2τ, a^τ donne le reste $b - 1$, ainsi que $a^{t+\tau}$, $a^{2t+\tau}$, ... Autrement a^t ne pourrait être $\equiv 1$ (mod. b).

2° Si t est impair, $b - 1$ ne fait pas partie des t restes. (Euler.)

3° Si t est pair, on a $a^{t+k} \equiv -a^{\tau-k}$ (mod. b).

4° Si $a^p \equiv 1$ (mod. b) et que p soit un nombre premier, p divise t. (Euler.)

5° Si b est un nombre premier de la forme $4 + 1$, t ne peut être impair puisque -1 fait partie des t restes.

5. 1° a^n et a^{t-n} étant évidemment associés, les restes qui en proviennent en divisant par b, sont associés deux à deux, sauf le reste $b - 1$ quand il a lieu.

2° Si α est l'associé de a relativement à b, les deux périodes de restes de a^x et de α^x sont formées de mêmes nombres dans des ordres inverses. En effet, soit $a^n - \alpha^{t-n} \equiv c$ (mod. b), il viendra $a^t - (a\alpha)^{t-n} \equiv ca^{t-n}$; donc $c = 0$.

3° La somme des t restes est congru à b (Gauss). On le voit en faisant la somme

$$a^c + a^1 + a^2 + \ldots + a^{t-1}\,.$$

4° Le produit des t restes est $\equiv \pm 1$ (mod. b) selon que t est pair ou impair. Ce produit est en effet congru au produit $a^1 a^2 \ldots a^{t-1}$ (Gauss).

6. Si $a^f \equiv r$ et $a^{f+g} \equiv rs$ (mod. b), on a : $a^g \equiv s$ (mod. b. (Euler).

7. A + M étant incongru à p, la congruence $Ax^{p-1} + \ldots + M \equiv 0$ ne saurait avoir toutes les racines 1, 2, ... $p - 1$, car

en y faisant successivement $x = 1, 2, 3, \ldots p - 1$ et additionnant, on aurait $A + M \equiv 0$, à cause de (8) et (9).

8. La période de la fraction décimale provenant de la division de a par p a un nombre de chiffres qui est un diviseur de $p - 1$ (Gauss).

9. On a :

$$(a + b + c + \ldots + l)^p \equiv a^p + b^p + c^p + \ldots + l^p . \quad \text{(Gauss.)}$$

Cette relation se démontre, d'après Serret, en changeant successivement dans (7) b en $b + c$, etc.

10. La solution de la congruence $gx \equiv k$ est $x \equiv kg^{p-2}$.

En général soit $gx - hy = k$. Décomposons h en ses facteurs premiers et soit $h = a^\alpha b^\beta \ldots$; $(1 - g^{a-1})^\alpha$ est divisible par a^α, $(1 - g^{b-1})^\beta$ l'est par b^β, ... ; donc on a :

$$gG = 1 - (1 - g^{a-1})^\alpha (1 - g^{b-1})^\beta \ldots = 1 - hH$$

d'où

$$x = Gk , \quad y = Hk .$$

Cette solution est due à Gauss. On a aussi, avec Libri,

$$x = \frac{(g^{a-1} - 1)^{A\alpha} (g^{b-1} - 1)^{B\beta} \ldots + 1}{g} k$$

A, B, ... désignant des entiers quelconques.

11. Si a et $b = a - k$ sont premiers avec p, on a :

$$\frac{a^{p-1} - b^{p-1}}{k} \equiv 0 .$$

12. Si $a^k \equiv b^k$ on ne peut avoir $a^{k-1} \equiv b^{k-1}$ car il s'ensuivrait $a^{k-1} b \equiv b^k \equiv a^k$ et $a \equiv b$. On ne peut donc écrire $a^{p-2} \equiv b^{p-2}$, et les restes de la division de x^{p-2} par p donnent la série $1, 2, 3, \ldots p - 1$.

On peut donc toujours écrire $x^{p-2} \equiv a$, et cette congruence a une racine unique.

De là la relation $ax \equiv x^{p-1} \equiv 1$. Ainsi le nombre a a toujours un associé, qui est unique.

13. 1° Si $a^\alpha \equiv 1$, on a :

$$\alpha^m \equiv a^m , \quad \text{car} \quad 0 \equiv \alpha^{2m} - 1 \equiv \alpha^m (\alpha^m - a^m) .$$

Plus généralement, si a est une racine de $Ax^k + \ldots + M \equiv 0$, son associé α en est une de $Mx^k + \ldots + A \equiv 0$, ce qu'on démontre en posant $x\xi \equiv 1$ et multipliant la première congruence par ξ^k.

2° Si $a^\alpha \equiv 1$, on a :

$$a^{p-k} \equiv \alpha^{k-1} .$$

3° Les restes des divisions de a^{p-k} et de a^{k-1} par p sont associés.

14. Si k est premier avec $p - 1$, on peut toujours résoudre la congruence $x^k \equiv r$ (Sophie Germain). En effet si on avait, par exemple, $a^k \equiv b^k$, en posant $ky - (p-1)z = 1$, cette congruence deviendrait

$$a^{ky} \equiv b^{ky} \quad \text{d'où} \quad a^{(p-1)z+1} \equiv b^{(p-1)z+1} \quad \text{ou} \quad a \equiv b ,$$

ce qui est absurde.

On voit d'ailleurs que la valeur de x n'est autre que le reste ξ de la division de r^y par p, puisqu'on a :

$$\xi^k \equiv (r^y)^k \equiv r^{(p-1)z+1} \equiv r \equiv x^k , \quad \text{d'où} \quad x \equiv \xi .$$

15. Démontrer les relations suivantes :

$$2^{p-2} \equiv m + 1 ; \quad (p-2)^{p-2} \equiv m ; \quad \left(\frac{p \pm 1}{2}\right)^{p-2} \equiv \pm 2 ;$$

$$2^m = \left(\frac{p+1}{2}\right)^m ;$$

$$\left(\frac{p \mp 1}{4}\right)^m \equiv 1 , \text{ (pour } p = 4 \pm 1) ; \quad \frac{a^{p(p-1)} - 1}{p} \equiv 0 ;$$

$$a^{(b-2)^p - b} \equiv 1 ;$$

$$s_{p-1,\,p-1} \equiv -1 ; \quad s_{p-1,\,p} \equiv 0 ; \quad 2s_{m,\,p-1} \equiv -1 ; \quad s_{m,\,p} \equiv 0 ;$$

$$\sigma_{p-1,\,p-1} \equiv 0 ; \quad s_{2a,\,p} + a(2a+1)^p \equiv 0 ; \quad \sigma_{4a,\,p} + (2a)^p \equiv 0 ;$$

$$\sigma_{2a+1,\,p} - (2a+1)^p \mp 0 ; \quad s_{m,\,2a} \equiv 0 \text{ (pour } 2a < p-2) ;$$

$$a^{p-1} \equiv (p-1)^a \equiv 0 \ (\mp, \text{ selon que } a \text{ est pair ou impair}) ;$$

$$\left(\frac{n}{p}\right)^{p-1} + \left(\frac{n}{q}\right)^{q-1} + \ldots + \left(\frac{n}{r}\right)^{r-1} \equiv 1 \text{ (mod. } pq\ldots r),$$

$p, q, \ldots r$, nombres premiers.

16. Soient p, q, r, ... s, des nombres premiers qui ne divisent pas a et tels que $p-1$ soit multiple de $q-1$, de $r-1$, ... de $s-1$; $a^p - a$ est divisible par le produit $pqr \ldots sa$ (Euler). En effet $a^{p-1}-1$ peut s'écrire

$$(a^{Q})^{q-1}-1 \text{ . ou } (a^{R})^{r-1}-1, \ldots$$

En outre le produit suivant est entier

$$(a^{p-1}-1)\left(\frac{1}{q}+\frac{1}{r}+\ldots\right).$$

17. Soit $p-1=qr$. Si $Aa^q \equiv Bb^q$, A, a, B et b étant premiers avec p, on aura : $A^r \equiv B^r$. (Euler.) En effet $A^r a^{p-1} - B^r b^{p-1}$ est divisible par $Aa^q - Bb^q$ et par suite par p, de même que $A^r a^{p-1} - A^r b^{p-1}$. On a ainsi $b^{p-1}(A^r - B^r) \equiv 0$.

On a des cas particuliers intéressants avec $A = b = 1$, $B = b = 1$, $B = 1$, etc.

18. 1° Si f et g sont deux facteurs de $p-1$ ayant ε comme *p. g. c. d.* on pourra poser $f\mu - g\nu = \varepsilon$, d'où, si on désigne par a une racine commune de $x^f - 1 \equiv 0$ et de $x^g - 1 \equiv 0$, il viendra $1 \equiv a^{f\nu} \equiv a^{g\mu+\varepsilon} \equiv a^{\varepsilon}$. Donc les racines de $a^{\varepsilon} - 1 \equiv 0$ sont les racines communes aux deux congruences données.

Ainsi si f et g sont premiers entre eux, les deux congruences n'ont d'autre racine commune que 1.

Si $g = p-1$, la congruence $x^f - 1 \equiv 0$ n'a pas d'autres racines que celles de $x^{\varepsilon} - 1 \equiv 0$. On peut ainsi se contenter d'étudier la congruence $x^{\varepsilon} - 1 \equiv 0$, où ε est un diviseur premier de $p-1$.

Autre exemple. k et l désignant deux facteurs premiers de $p-1$, les racines communes à $x^{\frac{p-1}{k}} - 1 \equiv 0$ et à $x^{\frac{p-1}{l}} - 1 \equiv 0$ sont celles de $x^{\frac{p-1}{kl}} - 1 \equiv 0$.

2° Soient k, l, ... les facteurs premiers de f. Si a est une non-racine des congruences $x^{\frac{f}{k}} - 1 \equiv 0$, $x^{\frac{f}{l}} - 1 \equiv 0$, ... les solutions de $x^f - 1 \equiv 0$ sont 1, a, a^2, ... a^{f-1}. Supposons en effet qu'on ait $a^c \equiv a^d$, d'où $a^{d-c} \equiv 1$; en appelant θ le *p. g. c. d.* de $d-c$ et de f, on peut écrire :

$$fy - (d - c)z = \theta \quad \text{d'où} \quad 1 \equiv (a^f)^y \equiv a^{(d-c)z+\theta} \equiv a^\theta ;$$

on aurait ainsi l'une ou l'autre des relations $a^{\frac{f}{k}} - 1 \equiv 0$, $a^{\frac{f}{l}} - 1 \equiv 0$, contrairement à l'hypothèse.

3° Si $a^k \equiv r$, on aura $r^{\frac{p-1}{k}} \equiv 1$, donc, en divisant les puissances r, r^2, r^3, ... par p, on trouvera le reste 1 avant r^{p-1}. Les résidus de p sont dans ce cas, puisque 2 est un facteur premier de $p - 1$.

4° Supposons $\alpha^h \equiv 1$ et soit θ le *p. g. c. d.* de h et de $p - 1$. On aura :

$$h\mu - (p-1)\nu \equiv 0 \quad \text{d'où} \quad a^\theta \equiv \alpha^{h\mu} \equiv 1 \quad \text{et} \quad x^{p-1} - \alpha^\theta \equiv 0 .$$

Le premier membre de cette dernière congruence est divisible par $x^{\frac{p-1}{\theta}} - \alpha$, donc la congruence $x^{\frac{p-1}{\theta}} - \alpha \equiv 0$ a $\frac{p-1}{\theta}$ racines.

Soit $h = 2$, on a $\theta = 2$ et la valeur $\alpha = -1$ répond ou ne répond pas à la question selon que $p = 4 \pm 1$; donc, dans les mêmes cas, la congruence $x^2 + 1 \equiv 0$ a ou n'a pas de racines.

5° Soit t le gaussien de a. La division de a, a^2, ... a^t par p donne pour restes les t racines de $x^t - 1 \equiv 0$ et par suite les périodes des restes sont formées des mêmes nombres.

Ainsi la période de m restes comprend tous les résidus.

Pour $p = 19$, les puissances des nombres 5, 6, 9, 16, 17 donnent des périodes composées des nombres 1, 4, 5, 6, 7, 9, 11, 16, 17.

6° Euler, à qui sont dues, en principe, toutes ces propositions, remarque aussi que :

Si $\alpha^h \equiv \beta^h$ et si a n'est pas multiple de p, on a :

$$\alpha x^{\frac{p-1}{h}} - \beta a^{\frac{p-1}{h}} \equiv 0 ;$$

si $ab^h \equiv c^h$, on peut écrire :

$$ax^h \equiv d^h \quad \text{et} \quad ad^h \equiv y^h .$$

19. Si la congruence $F(x) \equiv 0$, de degré $n < p - 1$, a n racines, $F(x)$ est un diviseur de $x^{p-1} - 1$. Si elle en a k, $(k < n)$, $F(x)$ et $x^{p-1} - 1$ ont un diviseur commun du degré k. (Gauss.)

20. 1° Si $p - 1$ est le produit de q par un nombre impair et que a soit incongru avec p, on ne saurait avoir $x^q + a^q \equiv 0$. (Euler.) Posons en effet $x^{p-1} - a^{p-1} \equiv 0$, on ne peut avoir $x^{p-1} - a^{p-1} \equiv 0$, ni a fortiori, $x^q + a^q \equiv 0$.

2° Si $p - 1$ est le produit de q par un nombre pair, p divise $x^{2q} + 1$.

Ainsi $p = 13$ divise $x + 1$, $x^2 + 1$, $x^3 + 1$, $x^6 + 1$, ce qui revient à dire que 12 est résidu *linéaire*, *quadratique*, *cubique* et *sextique* de 13.

$p = 4 + 1$ divise $x^2 + 1$; $p = 8 + 1$ divise $x^4 + 1$; $p = 16 + 1$ divise $x^8 + 1$; ... $p - 1$ est donc résidu quadratique de $p = 4 - 1$. résidu *biquadratique* de $p = 8 + 1$, résidu *octique* de $p = 16 + 1$. ...

21. Si $p = 4 - 1$, on peut toujours trouver x et y tels que $x^2 + y^2 + 1 \equiv 0$. (Euler.) Démonstration de Lagrange. Posons

$$X = \frac{x^{p-1} + (y^2 + 1)^m}{x^2 + (y^2 + 1)} = x^{p-3} - x^{p-5}(y^2 + 1) + \ldots$$

$$Y = (y^2 + 1)^m - 1 =$$

$$= [(y^2 + 1) - 1]\,[(y^2 + 1)^{m-1} + (y^2 + 1)^{m-2} + \ldots + 1]\,.$$

L'expression $\frac{Y}{y^2}$ étant du degré $p - 3$ en y, $\frac{Y}{y^2} \equiv 0$, et par suite $Y \equiv 0$, ont au moins deux non-racines. De même, y étant ainsi déterminé, X peut devenir incongru à p pour deux valeurs au moins de x. On peut ainsi déterminer x et y de manière que XY soit incongru à p. Or on a identiquement :

$$(x^2 + y^2 + 1)\,XY = (x^{p-1} - 1)\,Y + [(y^2 + 1)^{p-1} - 1]\,.$$

Le second membre est $\equiv 0$, puisque $x < p$ et que, quel que soit y, p ne divise pas $y^2 + 1$. Donc p divise le premier membre et par suite $x^2 + y^2 + 1$, si x et y ont les valeurs déterminées plus haut.

22. Tout nombre premier $p = 4 + 1$ divise une somme de deux carrés; tout nombre premier $p = 4 - 1$ divise une somme de trois carrés. (Euler.) Seconde démonstration de Matrot. On a:

$$(\alpha) \qquad x^m - 1 \equiv 0 \text{ ou } x^m + 1 \equiv 0$$
$$s_{p-1,\,m} \equiv 0$$

par conséquent moitié des nombres 1, 2, 3, ... $p - 1$ satisfont à l'une des congruences (α) et l'autre moitié à l'autre. Soit $p = 4 + 1$ et soit a une racine de la seconde (α): le premier membre est une somme de deux carrés, car alors $m = \frac{p-1}{2}$ est pair.

Soit $p = 4 - 1$. Considérons deux nombres consécutif b, $b + 1$, satisfaisant l'un à la première (α), l'autre à la seconde, chose toujours possible, puisque 1 fait partie des m nombres qui vérifient la première. Cela posé, on a:

$$(\beta) \qquad b^m - 1 \equiv 0 \ , \ (b+1)^m + 1 \equiv 0 . \qquad (\gamma)$$

Multipliant (β) par b et (γ) par $b + 1$, puis ajoutant, il vient :

$$b^{m+1} + (b+1)^{m+1} + 1 \equiv 0 .$$

Les exposants $m + 1$ sont pairs, car dans ce second cas, m est impair.

23. Tout diviseur d'une somme de quatre carrés est lui-même une somme de quatre carrés (Lagrange). Démonstration analogue à celle du lemme VII.

On tire de là le théorème de Bachet, en se servant des propositions de l'exercice précédent.

24. Les diviseurs premiers de $a^t + b^t$ sont de la forme $2th + 1$. (Euler).

25. Les diviseurs de $2^p - 1$ sont de l'une des formes

$$8ph + 1,\ 8ph + 2(2 \pm 1)\,p + 1 \qquad (p = 4 \pm 1)$$

(Plana.)

26. Si $p = 4 + 1$ divise $a^2 \pm kb^2$, il divise un autre nombre de la forme $x^2 \mp ky^2$. Si $p = 4 - 1$ divise $a^2 \pm kb^2$, il n'en divise aucun de la forme $x^2 \mp ky^2$, et, quel que soit l, il divise $x^2 + ly^2$ ou $x^2 - ly^2$.

Si p divise des nombres appartenant aux formes $x^2 - ky^2$, $x^2 - ly^2$, il en divise également un appartenant à la forme $x^2 - kly^2$.

Si p ne divise ni $x^2 - ky^2$ ni $x^2 - ly^2$, il divise $x^2 - kly^2$.

27. Voici un exemple de l'emploi des imaginaires dans la théorie des nombres.

1° On a :

$$(1 + i)^{4h} = (2i)^{2h} = -2^{2h},$$

d'où pour $p = 4 \pm 1$,

$$(1 + i)^p = (-1)^{\frac{p \pm 1}{4}} (1 \pm i) 2^{\frac{p-1}{2}}.$$

Développant le premier membre et comparant les parties réelles, il vient

$$(-1)^{\frac{p \pm 1}{4}} 2^m \equiv 1 \quad \text{ou} \quad 2^m \equiv (-1)^{\frac{p \mp 1}{4}}.$$

2 est donc résidu ou non selon que $\frac{p \mp 1}{4}$ est pair ou impair, c'est-à-dire selon qu'on a $p = 8 \pm 1$ ou $p = 8 \pm 5$ (Lebesgue).

2° Pour $p = 3 \pm 1$, on a :

$$(1 + \sqrt{-3})^p = (-1)^{\frac{p \mp 1}{3}} 2^{p-1} (1 \pm i),$$

d'où

$$(-3)^m \equiv \pm (-1)^{\frac{p \mp 1}{3}} 2^{p-1} \equiv \pm (-1)^{\frac{p-1}{3}} \equiv \pm 1.$$

Donc -3 est résidu de $p = 3 + 1$ et non résidu de $p = 3 - 1$. Comme $(\pm 3)^m = (-1)^m 3^m$, 3 est résidu de 12 ± 1 et non résidu de 12 ± 5, (Libri.)

28. Soient ρ un non résidu de p et k un diviseur de $p + 1$; la congruence

$$\frac{(x + \sqrt{\rho})^k - (x - \sqrt{\rho})^k}{\sqrt{\rho}} \equiv 0.$$

a $k - 1$ racines. (Lagrange.) En effet le premier membre est un diviseur de celui de la congruence

$$\frac{(x + \sqrt{\rho})^{p+1} - (x - \sqrt{\rho})^{p+1}}{\sqrt{\rho}} \equiv 0,$$

laquelle est du degré p et a p racines, puisque son premier membre développé devient

$$2(p+1)(x+x\rho^m) \equiv 2(p+1)(x^p - x).$$

29. Vérifier que $2^p - 1$ est divisible par

$$23,\ 47,\ 233,\ 223,\ 431,\ 439,\ 167,\ 263,$$

pour $p = 11,\ 23,\ 29,\ 37,\ 43,\ 73,\ 83,\ 131.$

Les deux premiers et le quatrième cas sont de Fermat, les autres d'Euler.

On se sert, pour cette vérification, de la méthode d'Euler, n° 2, 1°.

29. Démonstration du théorème de Fermat, par la supposition de b premier, dans les n^{os} 3 et 4.

Formons le tableau

$$\begin{array}{lllll}
1, & a, & a^2, & a^3, \ldots & a^t \equiv 1, \\
2, & 2a, & 2a^2, & 2a^3, \ldots & 2a^t \equiv 2, \\
3, & 3a, & 3a^2, & 3a^3, \ldots & 3a^t \equiv 3, \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
(p-1), & (p-1)a, & (p-1)a^2, & (p-1)a^3, \ldots & (p-1)a^t \equiv p-1.
\end{array}$$

Si $ka^f \equiv la^g$, on a : $ka^{f+\theta} \equiv la^{g+\theta}$. Donc si un terme de la l^e rangée est congru à un de ceux de la k^e, ces deux rangées sont identiques, à l'ordre près des termes. La k^e rangée contenant t termes différents, il y a donc t rangées identiques à la k^e, et les termes des autres rangées sont entièrement différents des premiers. Supposons que la première de ces autres rangées soit la h^e : il y aura de même t rangées identiques à celle-ci et leurs termes différeront de ceux des autres. La première des $p - 1 - 2t$ rangées non éliminées fournira également $t - 1$ autres rangées identiques. Et ainsi de suite : on voit que les $p - 1$ rangées seront disposées en groupes de t termes identiques chacun. (Desmarets.)

30. Déduire le théorème d'Euler de celui de Fermat. On a :

$$a^{p-1} \equiv 1 \pmod{p},\ a^{(p-1)p} \equiv 1 \pmod{p^2},\ \ldots\ a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$$

soit $b = p^f q^g \ldots$, p, q désignant des nombres premiers. On peut écrire :

$$a^{(p-1)p^{f-1}} - 1 \equiv 0 \pmod{p^f}\ ,\ a^{(q-1)q^{g-1}} - 1 \equiv 0 \pmod{q^g}\ ,\ \ldots$$

Posons $\psi(b) = (p-1)\,p^{f-1}\,(q-1)\,q^{g-1}\ldots$ Les premiers membres des congruences qui précèdent sont tous diviseurs de $a^{\psi(b)} - 1$: donc, en multipliant,

$$a^{\psi(b)} - 1 \equiv 0 \pmod{b}\,.$$

Or on sait que la fonction $\psi(b)$ représente celle qui a été désignée par $\varphi(b)$. Cette démonstration est d'Euler.

31. Le nombre des solutions $\geqq 0$ et $< p$ de la congruence $ax^2 - by^2 \equiv c$ est $p \mp 1$ selon que (ab) est résidu ou non résidu. (Libri.)

32. Le nombre des termes de la période décimale de $\frac{1}{p}$ n'est autre chose que le gaussien de 10, de sorte que si la période a $p-1$ chiffres, 10 est racine primitive de p (Gauss.) Ceci a lieu pour $p = 7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313\ldots$

33. Si a est une racine non primitive, aucun reste provenant de la division des puissances de a n'est racine primitive. Car de $a^t \equiv 1$ et $a^b \equiv r$, on tire $r^t \equiv 1$.

34. On n'a pas de méthode générale pour découvrir les racines primitives d'un nombre premier donné. L'exemple suivant, de Gauss, montrera suffisamment le procédé préconisé par cet illustre géomètre. Soit $p = 73$; l'essai du nombre 2 donne $2^9 \equiv 1$, donc 2 n'est pas racine primitive. Essayons le nombre 3, qui ne fait pas partie de la période qu'on vient d'obtenir : on trouve $3^{12} \equiv 1$; 3 n'est pas non plus racine primitive, mais on tire de ces résultats cette relation

$$\left(\frac{3^{\frac{12}{9}}}{2^{\frac{9}{9}}}\right)^{36} = 54^{36} \equiv 1 \pmod{73}$$

qui suggère l'essai de 54, dont la période ne comprend pas le nombre 5. Ce dernier, essayé, fait voir que c'est une racine primitive.

Les remarques suivantes facilitent la recherche dans certains cas.

1° p étant de la forme $4 - 1$, si m est le gaussien de R, — R est racine primitive. (Jacobi.)

2° p étant $4 + 1$, m le gaussien de a et $R^2 \equiv a$, R et $-$ R sont racines primitives. (Id.)

3° p étant $8 + 5$, m le gaussien de a et $R^2 \equiv -a$, R est racine primitive. (Id.)

4° Si $p = 3q + 1$, que q soit le gaussien de a et que $R^3 \equiv a$, R est racine primitive. (Id.)

5° R est généralement racine primitive quand $p = 8q + 5$, si $R^2 \equiv -1$; quand $p = 16q + 9$, si $a^2 \equiv -1$ et $R^2 \equiv a$; quand $p = 12q + 1$. Si $R^{4q+2} \equiv R^{2q+1} - 1$; quand $p = 6q + 1$, q désignant un nombre non multiple de 3, si $a^q = \pm 1$, $b^3 \equiv -1$ et $R \equiv \pm ab$. (Desmarets.)

35. Si R est racine primitive, $-$ R l'est ou ne l'est pas selon que $p = 4 \pm 1$ (Cauchy).

Dans le premier cas, si h est pair, $(-R)^h = R^h$; si h est impair, $(-R)^{h+m} \equiv -R^{h+m} \equiv R^h$, puisque $-$ R est non-résidu.

Dans le second cas, R étant non-résidu, $-$ R est résidu et par suite racine non primitive.

36. On a :

$$R^a + R^{2a} + R^{3a} + \ldots + R^{(p-1)a} \equiv s_{p-1,\,a}.$$

Le premier membre est $\equiv -1$ si a est multiple de $p - 1$ et dans le cas contraire, il est $\equiv 0$, puisqu'il peut s'écrire

$$\frac{R^{(p-1)a} - 1}{R^a - 1} R^a.$$

De même on a $R^1 R^2 R^3 \ldots R^{p-1} \equiv (p-1)!$ Or le premier membre est égal à $R^{pm} \equiv -1$.

On a ainsi d'autres démonstrations des théorèmes de Libri et de Wilson. La seconde est d'Euler.

37. Soit θ le *p. g. c. d.* de $p - 1$ et de h; la division des puissances $1^h, 2^h, 3^h \ldots$ par p donne $\frac{p-1}{\theta}$ restes différents (Euler). Si R est une racine primitive, les $\frac{p-1}{\theta}$ restes de 1, $R^\theta, R^{2\theta}, R^{3\theta}, \ldots R^{(p-1)\theta}$ sont tous différents et se reproduisent périodiquement. Soit $R^g \equiv r$, r peut prendre toutes les valeurs de 1 à $p - 1$, et comme on peut écrire $hx - (p-1)\,y = \theta$, on a :

$$(r^x)^h \equiv r^{(p-1)y+\theta} \equiv r\theta \equiv \mathrm{R}^{g\theta}.$$

x est évidemment premier avec $p-1$, donc le reste de r^x prend toutes les valeurs 1, 2, 3, ... $p-1$, et on peut mettre r au lieu de r^x. On peut donc dire que r^h a les mêmes valeurs que $\mathrm{R}^{g\theta}$.

En particulier, si h est premier avec $p-1$, il y a $p-1$ restes différents. Si $h=2$, il y en a $\frac{p-1}{2} = m$, qui sont les résidus quadratiques. En général, le nombre des résidus de puissances $h^{èmes}$ est $\frac{p-1}{h}$.

A. Aubry (Beaugency, Loiret).

SUR LES PROJECTIONS DES DROITES PERPENDICULAIRES

(A propos d'un récent article de M. *Lehr*[1]).

Dans divers ouvrages sur la géométrie descriptive on ne fait presque aucune mention des projections de deux droites perpendiculaires. Même dans les récentes *Leçons sur la Géométrie descriptive* de M. Loria, qui contiennent un grand nombre de particularités très intéressantes, on ne trouve que quelques indications sur cette question. Je me propose de développer ici une démonstration simplifiée de la condition donnée par M. Lehr pour les projections de deux droites perpendiculaires (théorème III^me^ de l'article cité).

Les projections orthogonales $g'g''$, $h'h''$ de deux droites g et h étant données, menons par le point commun des projections horizontales et par l'intersection des projections verticales deux droites m et n perpendiculairement à la direction de la ligne de terre. Nous obtiendrons ainsi deux triangles que l'on peut considérer comme deux projections d'un tétraèdre $ABCD$. Les arêtes AB et CD sont toujours per-

[1] L'Enseign. math., IX^e^ année, p. 119; 1907.