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: Deuxième Partie Étude élémentaire sur le théorème de Fermat.
DOI: https://doi.org/10.5169/seals-10162

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 02.10.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

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 Ste-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 :

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

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.

$$x^{n+1} - x^n = x(x-1)\dots(x-n) + Ax\dots(x-n+1) + \dots + Mx(x-1)(x-2) + x(x-1)\,;$$

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

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

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

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

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

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

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

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

Il est donc impossible que la congruence $F(x) \equiv 0$ 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 :

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

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

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

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

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

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 :

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

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

$$a^t \equiv 1 \ , \ c^s \equiv 1 \ , \quad \text{d'où} \quad a^t - c^s = kb \qquad (\text{mod. } b)$$

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

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

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

$$a^{k-1}c^{b-k} \equiv a^{k-1+h}c^{b-k-h} \qquad (\text{mod. } b)$$

ce qui donnera

$$(\beta) \qquad c^h \equiv a^h \qquad (\text{mod. } b)$$

[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* $a^x \equiv 1$ (mod. 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 $t \leqq \varphi(b)$.

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

$$a^f \equiv \alpha \ , \ a^g \equiv \alpha' \qquad \text{(mod. } b)$$

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

$$\beta a' - \beta a \equiv \beta a^f (a^{g-f} - 1) \ , \ \alpha' - \beta\alpha \equiv a^f (a^{g-f} - \beta) \quad \text{(mod. } b)$$

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 $\gamma, \delta, \ldots$ 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 :*

$$a^{\varphi(b)} \equiv 1 \qquad \text{(mod. } b) \tag{11}$$

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 :

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

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 $p \equiv 1$ (mod. 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 $p = 7, 11,$

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 :

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

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

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

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, ... $p - 1$.

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 :

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

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

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

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

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

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

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

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

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

$p, q, \ldots r$, 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 $p = 4 \pm 1$,

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

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

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

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

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

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

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°s 3 et 4.

Formons le tableau

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

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 :

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

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

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

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 :

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

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 $R^{g\theta}$.

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 IIIme 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., IXe année, p. 119; 1907.