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

Artikel: THÉORIE ÉLÉMENTAIRE DES RÉSIDUS QUADRATIQUES
Autor: Aubry, A.
DOI: https://doi.org/10.5169/seals-10133

THÉORIE ÉLÉMENTAIRE DES RÉSIDUS QUADRATIQUES

Avant-propos. — Par suite de la création de nombreux journaux scientifiques dans le courant du XIX^{e} siècle, de doctes et ingénieux pionniers se sont attachés de plus en plus et dans un grand nombre de directions, à poursuivre surtout le défrichement de l'immense champ mathématique, dont la production a pris ainsi une intensité inquiétante pour l'avenir de la science : il est certain que dans cent ans, bien des étendues cultivées aujourd'hui, seront délaissées, à cause de leur isolement ou de leur aridité. Mais on peut affirmer que les deux parties qui en forment l'entrée, ou, si l'on veut, l'initiation — la géométrie et l'arithmétique — seront toujours l'objet d'une culture de plus en plus suivie et iront se généralisant de plus en plus, jusqu'à l'absorption de la plus grande partie du reste.

De la première de ces deux sciences, on possède des traités élémentaires, aujourd'hui, bien près de toute la perfection désirable. Quant à la seconde, en dépit de nombreux écrits qui en traitent, elle est loin d'être aussi connue que le mériteraient son extrême importance, l'élégance de ses propositions, l'attrait que lui ont reconnu tous ceux qui s'y sont livrés, enfin la beauté des problèmes non encore résolus et d'une foule d'autres qu'il serait facile de se poser et peut-être de résoudre, si les efforts d'un plus grand nombre d'intelligences étaient dirigés dans cette voie. La faute n'en serait-elle pas aux traités, même élémentaires, où elle est exposée, lesquels visent trop haut et abordent dès le début des questions trop générales? Et ne conviendrait-il pas, si on veut arriver à la vulgariser, d'en illustrer au moins les théories initiales par des applications et des exercices choisis, qui soutiendraient l'intérêt du lecteur sans le rebuter et lui mon-

treraient rapidement et mieux que toute explication, l'esprit de la théorie des nombres, son but et sa méthode ?

Cela nous a fait penser qu'une série d'études sur les éléments de l'arithmétique pourrait servir la cause que nous défendons, savoir la vulgarisation de cette belle théorie, en contribuant à la production d'un traité véritablement élémentaire. Nous donnons ici la première de ces études.

1. — On appelle *résidus quadratiques* du nombre premier p, les restes de la division par p, des carrés entiers non multiples de p. Ainsi les nombres 1, 3, 4, 9, 10, 12 sont les résidus de 13, et 2, 5, 6, 7, 8, 11 en sont les *non-résidus*.

Dans la première partie de ce mémoire, il ne sera question que de résidus quadratiques ; nous pouvons donc nous borner, pour abréger, à dire simplement *résidus*.

Posons $p = 2m + 1$; *il y a* m *résidus de* p *et on les détermine en divisant par* p *les* m *premiers carrés entiers* (Euler). En effet si pour $0 < a < b < m$, on avait les deux *congruences* [1] $a^2 \equiv r$, $b^2 \equiv r$, il s'ensuivrait $(a+b)(a-b) \equiv 0$, ce qui est impossible, puisque $a + b$ et $a - b$ sont inférieurs à p et par suite premiers avec lui.

Divisant par p les carrés supérieurs à m^2 puis ceux supérieurs à p^2, on retrouve symétriquement puis périodiquement les mêmes restes, quisqu'on a $(p - a)^2 \equiv a^2$ et $(kp + a)^2 \equiv a^2$. Il n'y a donc que m résidus.

On désignera les résidus par les lettres r, r', r'', ... et les non-résidus par celles-ci, ρ, ρ', ρ'', ...

2. — *Les produits d'un résidu quelconque par les* m *résidus sont congrus à ces mêmes résidus, dans un certain ordre* (Euler). On voit d'abord que le produit de deux résidus est congru à un résidu, car de $r \equiv a^2$, $r' \equiv b^2$, on conclut $rr' \equiv (ab)^2$. D'ailleurs les deux relations $r'r'' \equiv r$, $r'r''' \equiv r$ entraîneraient la suivante $r'r'' \equiv r'r'''$, d'où, contrairement à l'hypothèse $r'' \equiv r'''$. On obtient donc ainsi tous les m résidus.

---

[1] La *congruence* $a \equiv b$, qui s'énonce *a congru à b*, indique que a diffère de b d'un multiple de p, ou que p divise la différence $a-b$.

Ainsi $(p + a)^n \equiv a^n$, ce qui résulté de ce que $(p + a)^n - a^n$ est divisible par $(p + a) - a$.

Cor. I. Ainsi les m produits rr, rr', rr'', ... sont congrus aux m résidus, et on peut écrire

$$rr.rr'.rr''... \equiv r.r'.r''...,$$

d'où

$$r^m \equiv 1. \tag{1}$$

Cor. II. Le produit d'un résidu par les m *non-résidus sont congrus à tous les non-résidus, et ceux d'un non-résidu par les* m *non-résidus sont congrus aux* m *résidus* (Gauss). Le produit $r\rho$ est incongru aux m produits rr, rr', ... : il est donc congru à un non-résidu. De même le nombre $\rho\rho'$ ne peut être congru à aucun des produits ρr, $\rho r'$, $\rho r''$, ... tous congrus à des non-résidus.

D'ailleurs les produits $r\rho$, $r\rho'$, $r\rho''$, ... sont incongrus entre eux, de même que les produits $\rho\rho$, $\rho\rho'$, $\rho\rho''$, ... Les premiers sont donc congrus aux m non-résidus et les seconds aux m résidus.

3. — De $\rho\rho' \equiv r$, on tire $\rho^m \rho'^m \equiv r^m \equiv 1$: on a donc $\rho^m \equiv 1$ ou $\equiv -1$.

Cor. I. On a donc toujours $a^m \equiv \pm 1$, d'où, en quarrant, cette congruence, qui constitue le *Théorème de Fermat,*

$$a^{p-1} \equiv 1. \tag{2}$$

Cor. II. Puisqu'on ne peut avoir $\rho \equiv x^2$, on ne saurait avoir non plus $\rho^m \equiv x^{p-1} \equiv 1$: on a donc

$$\rho^m \equiv -1. \tag{3}$$

Ainsi *le nombre* a *est résidu ou non-résidu selon que* a^m *est* $\equiv 1$ *ou* $\equiv -1$. Cette importante proposition s'appelle le *critérium d'Euler.*

Cor. III. Puisque 1 est toujours résidu, on peut toujours trouver deux nombres x et ξ tels qu'on ait $rx \equiv 1$ et $\rho\xi \equiv 1$, et cela d'une seule manière.

Le nombre x (ou ξ) est dit *l'associé* de r (ou de ρ). Ainsi *tout nombre* a *inférieur à* p, *a son associé, c'est-à-dire un nombre* y *tel que* ay $\equiv 1$.

Posons $ab \equiv c$; en multipliant par la congruence $1 \equiv ay$, on aura $cy \equiv b$: *on peut donc trouver un nombre* y *inférieur à* p *et tel que* cy ≡ b.

Ces deux importants théorèmes sont dus à Euler. Parmi les nombreuses applications qui peuvent en être faites, nous indiquerons la suivante, qui nous sera utile plus loin.

Si la valeur a *de* x, *inférieure à* p, *satisfait à la congruence* $Ax^2 + Bx + C \equiv 0$, *il y a une autre valeur de* x, *également plus petite que* p, *qui y satisfait, et il n'y en a pas d'autre.* Les deux congruences $Ax^2 + Bx + C \equiv 0$, $Aa^2 + Ba + C \equiv 0$ donnent par soustraction

$$A(x^2 - a^2) + B(x - a) \equiv 0 ,$$

d'où, comme $x - a$ est un nombre premier avec p,

$$A(x + a) + B \equiv 0 .$$

Or on a vu plus haut que cette congruence est toujours possible.

On appelle *racine* de la congruence du n^e degré $Ax^n + Bx^2 + \ldots + Lx + M \equiv 0$, tout nombre plus petit que p et qui, mis à la place de x, satisfait à cette congruence. On peut donc dire que *la congruence du premier degré* $Ax + B \equiv 0$ *a toujours une solution unique et que celle du second degré a deux racines ou n'en a pas.*

On étendrait aisément ce théorème au cas général et on arriverait ainsi à une proposition importante, due à Euler et à Lagrange.

Cor. IV. Le produit de plusieurs entiers plus petits que p *est congru à un résidu ou à un non-résidu selon que le nombre des non-résidus qu'ils comprennent est pair ou impair.* (Euler).

Cor. V. Si le produit ab *est résidu,* a *et* b *sont tous deux résidus ou tous deux non-résidus.*

Cor. VI. Posons $r^m \equiv 1$, $\rho^m \equiv -1$: on aura $(p - r)^m \equiv \pm 1$ et $(p - \rho)^m \equiv \mp 1$ selon que m est pair ou impair. Donc si $p = 4 + 1$[1], *les nombres* a *et* p-a *sont ensemble résidus ou*

[1] Par ce symbole, 4 + 1, nous entendons un *multiple* de 4 augmenté de 1.

non-résidus. Si $p = 4 - 1$, *les deux nombres* a *et* p-a *sont l'un résidu et l'autre non-résidu.*

4. — La question de décider si un nombre donné a est résidu ou non-résidu de p peut se traiter, indépendamment de toute théorie, dans certains cas très simples. Ainsi : 1° on a $(\alpha^2)^m = \alpha^{p-1} \equiv 1$; donc tout carré est congru à un résidu, ce qui suit de la définition des résidus.

2° On a $(p-1)^m \equiv (-1)^m$. Ainsi selon que $p = 4 \pm 1$, on a :

$$(p-1)^m \equiv \pm 1 . \tag{4}$$

3° Soit $a = 2$. Si $p = 4 + 1$, m est pair et le produit des m premiers multiples de 2 peut s'écrire

$$2^m m! = [2.4.6\ldots m]\left[\left(p - \frac{p-3}{2}\right)\left(p - \frac{p-7}{2}\right)\ldots(p-3)(p-1)\right]$$

$$\equiv 2.4.6\ldots m\left(-\frac{p-3}{2}\right)\left(-\frac{p-7}{2}\right)\ldots(-3)(-1) = m!\,(-1)^{\frac{m}{2}}$$

Si $p = 4 - 1$, m est impair et on a .

$$2^m m! = \left[2.4.6\ldots\frac{p-3}{2}\right]\left[\left(p - \frac{p-1}{2}\right)\left(p - \frac{p-5}{2}\right)\ldots(p-3)(p-1)\right]$$

$$\equiv 2.4.6\ldots\frac{p-3}{2}\left(-\frac{p-1}{2}\right)\left(-\frac{p-5}{2}\right)\ldots(-3)(-1)$$

$$= m!\,(-1)^{\frac{p+1}{4}} .$$

Par conséquent

$$2^m \equiv (-1)^{\frac{p\mp 1}{4}} . \qquad (\text{pour } p = 4 \pm 1). \tag{5}$$

Or $\frac{p^2-1}{8}$ diffère d'un nombre pair de $\frac{p-1}{4}$, dans le premier cas, et de $\frac{p+1}{4}$, dans le second cas, puisque les deux différences sont $\frac{p-1}{4}\ \frac{p-1}{2}$ et $\frac{p-3}{4}\ \frac{p+1}{2}$. La formule (5) peut donc s'écrire, quel que soit le cas,

$$2^m \equiv (-1)^{\frac{p^2-1}{8}} . \tag{6}$$

2 est donc résidu ou non selon que le nombre $\frac{p^2-1}{8}$ est pair ou impair.

4° Soit $a = 3$; p peut prendre seulement l'une des formes $6 + 1$ ou $6 - 1$. Dans le premier cas, on a

$$3^m m! = [3.6.9 \ldots m]\left[\left(p - \frac{p-5}{2}\right) \ldots (p-7)\,(p-4)\,(p-1)\right]\cdot$$

$$\left[(p+2)\,(p+5) \ldots \left(p + \frac{p-3}{2}\right)\right]$$

$$\equiv m!\,(-1)^{\frac{m}{3}} ;$$

d'où

$$3^m \equiv (-1)^{\frac{p-1}{6}} . \qquad (p = 6 + 1) \tag{7}$$

De même dans le second cas,

$$3^m m! = [3.6 \ldots (m-2)]\,[(p-m)\,(p+3-m) \ldots (p-2)]$$

$$[(p+1)\,(p+4) \ldots (p+m-1)]$$

$$\equiv m!\,(-1)^{\frac{p+1}{6}} ,$$

d'où

$$3^m \equiv (-1)^{\frac{p+1}{6}} . \qquad (p = 6 - 1) \tag{8}$$

5° Soit $a = p - 2$: on a visiblement :

$$(p-2)^m \equiv (-2)^m \equiv 2^m\,(-1)^m \equiv (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}} = (-1)^{\frac{(p-1)\,(p+5)}{8}} ;$$

ou bien

$$(p-2)^m \equiv (-1)^{\frac{(p-1)\,(p-3)}{8}} . \tag{9}$$

De la même manière, on trouvera :

$$(p-3)^m \equiv (-1)^{\frac{p-1}{6}}\,(-1)^{\frac{p-1}{2}} = (-1)^{\frac{2p-2}{3}} . \qquad (p = 6 + 1). \tag{10}$$

$$(p-3)^m \equiv (-1)^{\frac{2p-1}{3}} . \qquad (p = 6 - 1). \tag{11}$$

Cor. I. On a $(p-1)^m \equiv 1$, si $p = 4 + 1$. Donc dans ce cas on peut trouver un nombre f tel que $f^2 \equiv p - 1$, ou $f^2 + 1 \equiv 0$. De là successivement,

$$(f \pm 1)^2 \equiv \pm 2f,\ (f \pm 1)^4 \equiv -4,\ (f \pm 1)^{4n} \equiv (-4)^n .$$

Ainsi *un nombre premier* $p = 4 + 1$ *divise au moins deux nombres assignables de chacune des formes* $x^2 + 1$, $y^4 + 4$, $z^8 - 16$, $w^{16} + 64$, ... Par exemple, soit $p = 13$, on aura $f = 5$: donc 13 divise $6^{16} + 64$ et $4^{16} + 64$. La possibilité d'écrire $y^4 + 4 \equiv 0$ pour $p = 4 + 1$, a été signalée d'abord par Sophie Germain.

De plus on a : $(fx \pm y)^2 + (fy \mp x)^2 \equiv 0$; donc $p = 4 + 1$ *divise une infinité de sommes de deux carrés premiers entre eux* (Fermat).

Cor. II. D'après (6), 2 est résidu de $p = 8 \pm 1$ et non-résidu de $p = 8 \pm 3$. D'après (9), $p - 2$ est résidu si $p = 8 + 1$ ou $8 + 3$ et non-résidu si $p = 8 - 1$ ou $8 + 5$.

m est pair ou impair en même temps que $\frac{p-1}{6}$, et, dans les mêmes cas, $p = 12 + 1$ ou $12 + 7$. Donc, d'après (7),

pour $p = 12 + 1$, $(\pm 3)^m \equiv 1$: 3 et -3 sont[1] résidus ;

pour $p = 12 + 7$, $(\pm 3)^m = \pm 3^m \equiv \pm(-1) = \mp 1$: 3 est non-résidu et -3 résidu.

On verra de même que, à cause de (8), $3^m \equiv \pm 1$ selon que $p = 12 - 1$ ou $12 + 5$. Par suite, dans les deux cas, on a $(-3)^m \equiv -1$.

Ainsi, selon que $p = 6 \pm 1$, il a -3 pour résidu ou non-résidu, c'est-à-dire qu'il divise ou ne divise pas $x^2 + 3$[2].

Cor. III. Soit $f^2 + a \equiv 0$. Si x est le reste de la division de fy par p, il viendra $x^2 + ay^2 \equiv 0$. Donc *si* p *divise un nombre* $f^2 + a$ *il en divise aussi une infinité de la forme* $x^2 + ay^2$. On résoudra ainsi la congruence $x^2 + ay^2 \equiv 0$ en posant $y = 1, 2, 3, \ldots$ et $x \equiv fy$.

D'ailleurs pour $a = 1, 2, 3, \ldots$ on voit que $p = 4 + 1$ *divise une infinité de sommes de deux carrés ;* $p = 8 \pm 1$ *une infinité de nombres de la forme* $x^2 - 2y^2$; $p = 6 + 1$ *une infinité de nombres de la forme* $x^2 + 3y^2$; *etc.* (Fermat).

Cor. IV. Si $p = 4 - 1$, $(p-1)^m \equiv -1$; donc on ne saurait dans ce cas poser $f^2 \equiv p - 1$ ou $f^2 + 1 \equiv 0$, ni $x^2 + y^2 \equiv 0$,

[1] Pour abréger on écrit souvent $-a$, au lieu de $p - a$.

[2] On veut dire par là que p divise un certain carré augmenté de 3, ou bien qu'il n'y a aucun carré qui augmenté de 3, fasse un nombre divisible par p.

x et y étant premiers entre eux. Par conséquent, $p = 4 - 1$ ne divise aucune somme de deux carrés premiers entre eux, ce qui permet d'affirmer que *les diviseurs premiers d'une telle somme sont tous de la forme* $4 + 1$ [1]. (Fermat).

De même aucun nombre premier $6 - 1$ ne divisant $x^2 + 3$, ni par suite $x^2 + 3y^2$, il s'ensuit que *tous les diviseurs premiers de* $x^2 + 3y^2$ *sont de la forme* $6 + 1$.

Cor. V. Tout nombre premier $p = 4 - 1$ *divise une somme de trois carrés dont l'un est l'unité* (Euler). La série $1,2,3,\ldots$ $p - 1$ commençant par un résidu et finissant par un non-résidu, il y a au moins un résidu r suivi d'un non-résidu $\rho = r + 1$. Par suite, $p - r - 1$ est un résidu et on peut écrire :

$$x^2 \equiv r\ ,\ y^2 \equiv -r - 1\ ,\quad \text{d'où}\quad x^2 + y^2 + 1 \equiv 0\ .$$

Cor. VI. Soit à résoudre $jx^2 + ky^2 \equiv 0$. Cherchons le nombre c tel que $jc \equiv k$: il viendra $x^2 + cy^2 \equiv 0$. Posant $x \equiv yz$, le problème est ramené à résoudre $z^2 + c \equiv 0$; il est possible par conséquent si $-c$ est résidu.

Cor. VII. Soit $p = 8 + 1$; -1 est résidu, de même que 2 et -2 : on peut donc écrire :

$$f^2 + 1 \equiv 0\ ,\qquad \text{d'où}\qquad (f \pm 1)^2 \equiv \pm 2f\ .$$

Ainsi $2f$ et $-2f$ sont résidus ; et comme 2 et -2 le sont eux-mêmes, le nombre f l'est également. On peut donc poser :

$$k^2 \equiv f,\quad \text{d'où}\quad k^4 \equiv -1\ ,\ g^2 \equiv 2\ ,\ h^2 \equiv -2\ ,\ g^4 \equiv 4\ ,\ j^4 \equiv -4\ ,$$

en posant

$$g \equiv k^3 - k\ [2]\ ,\quad h \equiv k^3 + k\ ,\quad j \equiv f \pm 1\ .$$

La possibilité de trouver un nombre k tel que $k^4 + 1 \equiv 0$, pour $p = 8 + 1$ [3], a été démontrée d'abord par Gauss.

---

[1] Euler démontre ainsi cette proposition : $p = 4 - 1$ ne saurait diviser $x^2 + y^2$ sans diviser $x^{p-1} + y^{p-1}$ qui est multiple de $x^2 + y^2$ puisque m est impair. Or cette divisibilité est impossible puisque, à cause du théorème de Fermat, p divise $x^{p-1} - y^{p-1}$.

[2] Soit $k^3 + \alpha \equiv 0$; α est l'associé de k. De là $k^2 \equiv k^4\alpha^2 \equiv -\alpha^2$ et $(\alpha \pm k)^2 \equiv \pm 2k\alpha \equiv \pm 2$.

[3] Si $p = 8 + 5$, on a également $f^2 + 1 \equiv 0$, $(f \pm 1)^2 \equiv \pm 2f$, puisque p est $4 + 1$; $(2f)$ est donc résidu, mais 2 étant alors non-résidu, f l'est également et on ne peut plus écrire $k^2 \equiv f$, ni par suite $k^4 \equiv -1$.

On remarquera d'ailleurs avec Euler et avec Gauss, que si, pour $p = 4 + 1$, $a^4 \equiv r$, les nombres $(-a)^4$, $(fa)^4$, $(-fa)^4$ sont également $\equiv r$ et sont incongrus entre eux, car, autrement, de $fa \equiv \pm a$, on conclurait $f \equiv \pm 1$, ce qui est impossible, puisque $f^2 \equiv -1$. De plus il n'y a que ces quatre nombres dans ce cas, car les deux congrues $a^2 - x^2 \equiv 0$ et $a^2 + x^2 \equiv 0$ ne peuvent avoir chacune plus de deux racines, et par suite la congruence $a^4 - x^4 \equiv 0$ ne peut en avoir plus de quatre.

Ainsi $p = 8 + 1$ divise quatre nombres de chacune des formes $g^4 - 4$, $j^4 + 4$ et $k^4 + 1$. On pourra appliquer tout cela au cas de $p = 17$, qui donne $f = 4$ ou 13, $g = 6$ ou 11, $l = 7$ ou 10, $j = 5$ ou 3, ou 12 ou 14, $k = 8$.

Cor. VIII. Soient $p = 8 + 1$, $k^4 \equiv -1$; on résoudra $x^4 + y^4 \equiv 0$ en posant $x = 1, 2, 3, \ldots$ $y \equiv k, 2k, \ldots$ On peut donc dire, avec Euler, que *tout nombre premier de la forme* $8 + 1$ *divise de plusieurs manières une somme de deux bicarrés.*

On résoudra $x^2 \pm 2y^2 \equiv 0$ en posant $ak \equiv A$ d'où $A^4 + a^4 \equiv 0$ ou bien $(A^2 \pm a^2)^2 \mp 2(Aa)^2 \equiv 0$.

En général si p divise $\alpha a^n + \beta$, en posant $ay \equiv x$, on voit qu'il divise également $\alpha x^n + \beta y^n$. Réciproquement si p divise $\alpha a^n + \beta b^n$, il divise aussi $\alpha x^n + \beta$, ce qu'on vérifie en posant $\alpha \equiv \beta x$.

Cor. IX. D'après II, le nombre premier $p = 6 + 1$ divise un certain nombre $s^2 + 3$. Ecrivons d'après cela

$$(\alpha) \qquad (s-1)^2 + 2(s-1) + 4 \equiv 0 .$$

Soit n l'associé de $(s-1)$; multiplions la relation (α) par n^2 et posons $2n \equiv \alpha \equiv -1 - \beta$; il viendra :

$$\alpha^2 + \alpha + 1 \equiv 0 , \ \beta^2 + \beta + 1 \equiv 0 , \quad \text{d'où} \quad \alpha^3 - 1 \equiv 0 , \ \beta^3 - 1 \equiv 0 ,$$

$$(\beta + 1)^2 \equiv \alpha^2 \equiv \beta , \ (\alpha + 1)^2 \equiv \beta^2 \equiv \alpha , \ \alpha^2 + \beta^2 + \alpha\beta \equiv 0 ,$$

$$s \equiv \beta - \alpha \equiv 2\beta + 1 \equiv -2\alpha - 1 , \ (s \pm 1)^3 \equiv \pm 8$$

$$\alpha\beta \equiv (\alpha + 1)(\beta + 1) \equiv 1 , \ (\alpha + 1)^3 \equiv (\beta + 1)^3 \equiv -1 ,$$

$$(\alpha \pm 1)(\beta \mp 1) \equiv \pm s , \ (\alpha - 1)(\beta - 1) \equiv 3 .$$

Soit a un entier inférieur à p ; posons $a\alpha \equiv x$, $a\beta \equiv y$, d'où

$$a^2 + x^2 + ax \equiv 0 \ , \quad a^2 + y^2 + ay \equiv 0 \ , \quad x^2 + y^2 + xy \equiv 0 \ ;$$

si on écrit $a^3 \equiv r$, il viendra :

$$x^3 \equiv y^3 \equiv r \ , \quad a + x + y \equiv 0 \ , \quad ax + xy + ya \equiv 0 \ , \quad axy \equiv r \ ,$$

$$a^2 \equiv xy \ , \quad x^2 \equiv ay \ , \quad y^2 \equiv ax \ , \quad a^2 + x^2 + y^2 \equiv 0 \ , \quad (\alpha x \pm \beta y)^2 + (\alpha y \mp \beta x)^2 \equiv -1$$

$$(a \pm 1)\,(x \pm 1)\,(y \pm 1) \equiv r \pm 1 \ , \quad (a + x)\,(x + y)\,(y + a) \equiv -r \ .$$

On voit, entre autres choses, que α et β sont des résidus associés ; qu'il en est de même de $\alpha + 1$ et $\beta + 1$; que p divise, de plusieurs manières, une somme de trois carrés ; qu'il divise aussi une somme assignable de quatre carrés, ainsi que les sommes de deux cubes $(s + 1)^3 + (s - 1)^3$ et $(\alpha - 1)^3 + (\beta - 1)^3$.

On pourra appliquer ces formules au cas de $p = 19$, qui donne $s = 4$, $n = 13$, $\alpha = 17$, $\beta = 11$.

5. — *Résidus cubiques.* Par extension de la notion des résidus, on appelle *résidus cubiques, biquadratiques, ...* les restes provenant de la division par p des cubes, des bicarrés, ... ; quelques résultats sont assez simples pour trouver place dans un exposé élémentaire.

1° Il est inutile d'aller au-delà des m premières divisions puisque $(p - a)^3 + a^3 \equiv 0$; deux cubes à égales distances de m sont donc complémentaires à p. En particulier, 1 et — 1 sont toujours résidus cubiques.

2° Si r est résidu cubique, il en est de même de r^2, et réciproquement, car de $x^3 \equiv r$, on tire $(x^2)^3 \equiv r^2$.

3° Si $p = 6 - 1$, les $p - 1$ premiers entiers sont tous résidus cubiques, car si on pouvait écrire $a^3 - b^3 \equiv 0$, il viendrait $a^2 + b^2 + ab \equiv 0$. d'où $(2a + b)^2 + 3b^2 \equiv 0$: or cette expression n'a pas de diviseurs de la forme $6 - 1$. (n° 4, II et III).

4° Si $p = 6 + 1$, il y a trois valeurs, 1, α, β, de x, qui donnent $x^3 \equiv 1$(n° 4, X) et il n'y a que celles-là, puisque la congruence $x^2 + x + 1 \equiv 0$ ne peut avoir que deux racines.

Ces trois racines sont d'ailleurs inégales, car autrement, de $\alpha \equiv \beta$, on tirerait $\beta \equiv \alpha^2 \equiv \beta^2$ et $\beta \equiv 1$.

De même, si $a^3 \equiv r$, il n'y a que les nombres a, $a\alpha$, $a\beta$, dont les cubes soient congrus à r. Les $p - 1$ premiers cubes se partagent donc en groupes de trois donnant le même reste quand on les divise par p. Il y a donc $\frac{p-1}{3}$ résidus cubiques.

5° Si r est résidu cubique, p divise $x^3 + ry^3$ et $z^3 + r^2y^3$.

Euler connaissait à peu près tout ce qui précède.

6° La multiplication du résidu cubique r par tous les résidus cubiques donne ces mêmes résidus dans un certain ordre. De là, les relations

$$rr \,.\, rr' \,.\, rr'' \ldots \equiv r \,.\, r' \,.\, r'' \ldots \qquad \text{et} \qquad r^{\frac{p-1}{3}} \equiv 1 \,.$$

Les résidus cubiques ne sont donc autres que les racines de la congruence $x^{\frac{p-1}{3}} \equiv 1$.

Les deux congruences $x^{\frac{p-1}{3}} \equiv \alpha$ et $x^{\frac{p-1}{3}} \equiv \beta$ ont également chacune $\frac{p-1}{3}$ racines ; elles sont distinctes des précédentes et ce sont par conséquent les $2\frac{p-1}{3}$ non-résidus cubiques.

6. — *Résidus biquadratiques.* 1° En élevant au carré les résidus, on obtiendra les résidus biquadratiques et ceux-ci doivent évidemment être choisis parmi les résidus : on les trouvera donc en se bornant à diviser par p les m premiers bicarrés.

Soit $a^2 \equiv r$; si $p = 4 - 1$, l'un des nombres $\pm a$ est résidu, quel que soit r ; donc dans ce cas, tous les résidus sont en même temps résidus biquadratiques.

2° Si r est résidu biquadratique, r^2 et r^3 le sont également.

3° Si $p = 8 \pm 1$, on peut écrire $a^2 \equiv -2$, d'ou $a^4 \equiv 4$, $a^8 \equiv 16$, $a^{16} \equiv 256$, ... Donc, dans les mêmes cas, 2 est résidu quadratique, 4 résidu biquadratique, 16 résidu octique, ... de p.

4° Si $p = 4 + 1$, p a $\frac{p-1}{4}$ résidus biquadratiques (n° 4, VII).

5° Si $p = 8 + 1$, -1 est résidu biquadratique, ainsi que 4 et -4 (id.).

6° On démontre comme au n° précédent que, pour $p = 4 + 1$, la congruence des résidus biquadratiques est $x^{\frac{p-1}{4}} \equiv 1$, et, de là, que les $p - 1$ premiers entiers se partagent en quatre classes d'un nombre égal de termes, qui sont les racines des quatre congruences

$$x^{\frac{p-1}{4}} \equiv \pm 1 , \qquad x^{\frac{p-1}{4}} \equiv \pm f .$$

Exercices.

1. Etant donné le théorème de Fermat, si on appelle résidus et non-résidus de p les nombres qui lui sont inférieurs et qui donnent respectivement $r^m \equiv 1$ et $\rho^m \equiv -1$, on a les propositions suivantes :

Le produit de deux résidus ou de deux non-résidus est congru à un résidu et celui d'un résidu par un non-résidu l'est à un non-résidu.

Le nombre p a m résidus et m non-résidus[1].

Les résidus sont les restes de la division par p des m premiers carrés.

2. Si $p = 4 + 1$ divise $a^2 \pm kb^2$, il divise aussi $x^2 \mp ky^2$. Quelque soit k, $p = 4 - 1$ divise $x^2 + ky^2$ ou $x^2 - ky^2$. Si p divise $a^2 - kb^2$ et $c^2 - ld^2$, il divise également $x^2 - aly^2$. Si p ne divise ni $x^2 - ky^2$ ni $x^2 - ly^2$, il divise $x^2 - kly^2$. (Lagrange).

3. $B^2 - R$ étant divisible par A et $R - r$ l'étant par p, p divise ou ne divise pas A selon que r est résidu ou non-

[1] Soient n le nombre des résidus et ν celui des non-résidus. Les produits ρr, $\rho r'$, ... donneront n non-résidus différents; par suite $n \leq \nu$. La multiplication de ρ par les ν non-résidus donnerait ν résidus différents. Donc $n \leq \nu$ et $n = \nu = m$.

Cette démonstration est beaucoup plus simple que celle de Matrot (J. E. 1893, p. 74).

résidu. Ce théorème sert, dans certains cas, à décomposer les grands nombres en leurs facteurs. (Gauss [1]).

4. Le produit des résidus est $\equiv \mp 1$ et celui des non-résidus $\equiv \pm 1$, selon que $p = 4 \pm 1$. De là, le *théorème de Wilson*, que représente la congruence

$$(p-1)! + 1 \equiv 0 ,$$

et cette autre congruence, due à Libri,

$$\frac{(p-1)!}{a} + a^{p-2} \equiv 0 .$$

5. Si $p = 4 - 1$, $m! \equiv \pm 1$ selon que p a un nombre impair ou un nombre pair de résidus inférieurs à $\frac{p}{2}$ (Lejeune-Dirichlet).

6. Si $p = 4 + 1$, $(m!)^2 + 1 \equiv 0$ (Lagrange).

7. p diyise toujours $rx^2 - r'y^2$ et $\rho x^2 - \rho' y^2$, mais jamais $rx^2 - \rho y^2$. $p = 4 + 1$ divise $rx^2 + \rho y^2$ et non $rx^2 + r'y^2$ ni $\rho x^2 + \rho' y^2$; le contraire a lieu pour $p = 4 - 1$. (Euler).

8. Si $(b^2 - 4ac)$ est résidu, la congruence $ax^2 + bx + c \equiv 0$ a deux racines (Gauss). Plus généralement, la même chose a lieu si $a(b^2 - 4ac)$ est résidu (Cauchy).

9. Si $p = 4 + 1$, on a $(1 + \rho)(1 + \rho') \ldots \equiv 2$ et si $p = 4 - 1$, $(1 + r)(1 + r') \ldots \equiv 2$ (Stieltjès).

10. Pour $p = 4 + 1$, la suite $1 + \rho$, $1 + \rho'$, ... comprend $\frac{p-1}{4}$ résidus et autant de non-résidus. Si $p = 4 - 1$, la suite $1 + r$, $1 + r'$, ... comprend $\frac{p-3}{4}$ résidus et $\frac{p+1}{4}$ non-résidus (Stieltjès).

---

[1] Ainsi on a $93019 = 305^2 - 6$; comme le montre la table des résidus, 6 n'est pas résidu des nombres 7, 11, 13, 17, 31, 37, 41, 53, 61, 71, 79, 83: aucun de ces nombres ne divise donc 93019.

Or $2.93019 = 432^2 - 586$. Le reste 11 de la division de 586 par 23 est non-résidu de 23 ; donc 23 ne divise pas 93019. Le reste 27 de la division de 586 par 43 est de même non-résidu de 43, donc 43 ne divise pas 93019.

$3.93019 = 529^2 - 784 = 529^2 - 28^2 = 501.257$, d'où $93019 = 167.257$, ce qui termine le calcul. Autrement, on continuerait ainsi . $5.93019 = 682^2 - 29$; or 29 n'est résidu d'aucun des nombres 31, 37, 41, 43, 47, 61, 73, 79, 97, ... On déterminerait ainsi successivement d'autres facteurs premiers impossibles à admettre et on n'aurait plus qu'à essayer les divisions par les quelques facteurs inférieurs à $\sqrt{93019}$ qu'on n'aurait pu éliminer.

On voit l'intérêt qu'il y aurait à posséder une table des résidus des nombres premiers jusqu'à 10.000, ou même plus loin, comme le souhaitait Gauss.

11. Si ni $p-1$ ni m ne sont résidus, il y a au moins un résidu r tel que $-r-1$ soit également résidu. (Matrot).

12. Appelons *variation* la succession d'un résidu (ou non-résidu) et d'un non-résidu (ou résidu). La suite $1,2,3,\ldots p-1$, présente un nombre pair ou impair de variations selon que $p = 4 \pm 1$. (Stieltjès).

13. Si $p = 4 - 1$, la congruence $x^2 \equiv a$ a les deux racines $x \equiv \pm a^{\frac{p+1}{4}}$; si $p = 8 + 5$ et que $a^{\frac{p-1}{4}} \equiv 1$, ses racines sont $x \equiv \pm a^{\frac{p+3}{8}}$ (Legendre).

Si $p = 8 + 5$ et que $a^{\frac{p-1}{4}} \equiv -1$, les deux racines sont $x \equiv \pm a^{\frac{p+3}{8}}\, m\,!$ (Mathews).

14. *Lemme de Gauss.* Soit μ le nombre des restes obtenus en divisant par p les m premiers multiples de a, et ne conservant de ces restes que ceux qui sont plus grands que m ; on a :

$$a^m = (-1)^{\mu}$$

15. On a aussi, avec Eisenstein,

$$a^m = \prod_1^m \frac{\sin \frac{2ka\pi}{p}}{\sin \frac{2k\pi}{p}},$$

et avec Liouville,

$$a^m = (-1)^{mn} \prod_1^n (\alpha^k - \alpha^{-k})^{p-1}.$$

Dans cette dernière formule $a = 2n + 1$ et α désigne une racine imaginaire de l'équation $x^p - 1 = 0$.

16. Le nombre μ est de même parité que le produit

$$\prod \left(\frac{h}{p} - \frac{k}{a}\right)\left(\frac{h}{p} + \frac{k}{a} - \frac{1}{2}\right)$$

h variant de 1 à m et k de 1 à $\frac{a-1}{2}$ (Kronecker).

17. Appelons, avec Lagrange, $E\omega$ la partie entière du nombre non entier ω, et posons

$$f(a,b) = E\frac{a}{b} + E\frac{2a}{b} + E\frac{3a}{b} + \ldots + E\frac{\frac{b-1}{2}a}{b},$$

$$4r_n = p + \left(4n - p - 2pE\frac{2n}{p}\right)(-1)^{E\frac{2n}{p}},$$

on aura :

$$f(1,b) = 0\ ,\ f(a+b,b) = \frac{b^2-1}{8} + f(a,b) \qquad \text{(Tchebichef).}$$

$$r_a \cdot r_{2a} \cdot r_{3a} \ldots r_{ma} \equiv a^m m!\,(-1)^{f(2a,p)} \qquad \text{(id.)}$$

$$a^m \equiv (-1)^{f(2a,p)} \equiv 2^m (-1)^{f(a+p,p)} \qquad \text{(id.)}$$

$$a^m \equiv (-1)^{f(a,p)}\ . \qquad \text{(Gauss).}$$

18. Etendre la notion des résidus aux restes de carrés divisés par un nombre composé P. En particulier, si a est résidu de p, il l'est de p^n. Le nombre p^n a mp^n résidus. (Gauss).

Soit le nombre $P = ax^2 + bxy + cy^2$, où x et y sont premiers entre eux $(b^2 - 4ac)$ est résidu de P. (Gauss).

A. Aubry (Beaugency, Loiret).