

EXPOSITION ÉLÉMENTAIRE DE LA LOI DE RÉCIPROCIÉ DANS LA THÉORIE DES NOMBRES

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

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **12 (1910)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **16.07.2024**

Persistenter Link: <https://doi.org/10.5169/seals-12787>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

EXPOSITION ÉLÉMENTAIRE DE LA LOI DE RÉCIPROCITÉ DANS LA THÉORIE DES NOMBRES

1. Soit à déterminer le reste de la division de a^m par le nombre premier p , m étant égal à $\frac{p-1}{2}$. Pour les cas de $a = 1, 2, 3, \dots, p-1, p-2, p-3, \dots$ on peut y arriver directement¹; la théorie qui va être exposée permet d'y arriver généralement et de la manière la plus simple.

2. Si r, r', r'', \dots désignent les restes de la division par b des nombres a, a', a'', \dots les deux produits $rr' r'' \dots$ et $aa' a'' \dots$ divisés par b donnent le même reste.

3. On a :

$$(1) \quad (a + c)^k \equiv a^k \pmod{c}$$

car $(a + c)^k - a^k$ est divisible par $(a + c) - a = c$.

De même

$$(2) \quad (c - a)^k \equiv \pm a^k \pmod{c}$$

selon que k est pair ou impair.

4. b désignant un nombre impair premier avec a , et $E\omega$ désignant la partie entière du nombre non entier ω ; posons

$$f(a, b) = E\frac{a}{b} + E\frac{2a}{b} + E\frac{3a}{b} + \dots + E\frac{\beta a}{b}, \quad \left(\beta = \frac{b-1}{2}\right)$$

on aura :

$$(3) \quad f(1, b) = 0$$

$$(4) \quad f(a + b, b) = \left(1 + E\frac{a}{b}\right) + \left(2 + E\frac{2a}{b}\right) + \dots + \left(\beta + E\frac{\beta a}{b}\right) \\ = \frac{b^2 - 1}{8} + f(a, b). \quad (\text{Tchébichef})$$

¹ Voir *Ens. math.*, 1907, p. 28. On a encore un cas de ce genre, quand p est de la forme $a^k \pm 1$, comme 3, 5, 17, 31, 37, 101, 127, 197, 257, ... ce cas est du reste aisé à traiter.

5. Soit $a < b$; les $E \frac{b}{a}$ premiers termes de $f(a, b)$ sont tous nuls; les suivants, jusqu'au $\left(E \frac{2b}{a}\right)^{\text{ème}}$, sont tous égaux à 1; les suivants, jusqu'au $\left(E \frac{3b}{a}\right)^{\text{ème}}$, tous égaux à 2; etc. (Gauss.)

En effet, on a :

$$0 < \frac{kb}{a} - E \frac{kb}{a} < 1 \quad \text{d'où} \quad \frac{a}{b} E \frac{kb}{a} < k < \frac{a}{b} \left(1 + E \frac{kb}{a}\right);$$

donc les nombres 1, 2, 3, ... se trouvent respectivement entre les $\left(E \frac{b}{a}\right)^{\text{ème}}$, $\left(E \frac{2b}{a}\right)^{\text{ème}}$, $\left(E \frac{3b}{a}\right)^{\text{ème}}$, ... termes de la série $\frac{a}{b}$, $\frac{2a}{b}$, $\frac{3a}{b}$, ... et ceux qui les suivent immédiatement.

Les $\left(E \frac{b}{a}\right)$ premiers multiples de $\frac{a}{b}$ sont ainsi < 1 , et leur partie entière est 0. Les $\left(E \frac{2b}{a} - E \frac{b}{a}\right)$ suivants ont des valeurs comprises entre 1 et 2; leur partie entière est donc 1. Les $\left(E \frac{3b}{a} - E \frac{2b}{a}\right)$ suivants ont une valeur comprise entre 2 et 3; leur partie entière est donc 2. Et ainsi de suite.

$$6. \text{ On a, en posant } \alpha = \frac{a-1}{2}, \beta = \frac{b-1}{2},$$

$$(5) \quad f(a, b) + f(b, a) = \alpha\beta. \quad (\text{Gauss})$$

D'après 5, $f(a, b)$ a pour valeur

$$(a) \quad \left\{ \begin{aligned} &0 \left(E \frac{b}{a}\right) + 1 \left(E \frac{2b}{a} - E \frac{b}{a}\right) + 2 \left(E \frac{3b}{a} - E \frac{2b}{a}\right) + 3 \left(E \frac{4b}{a} - E \frac{3b}{a}\right) + \dots \\ &+ \frac{a-3}{2} \left(E \frac{a-1}{2} \frac{b}{a} - E \frac{a-3}{2} \frac{b}{a}\right) + \alpha \left(\beta - E \frac{ab}{a}\right). \end{aligned} \right.$$

Le dernier groupe, au lieu d'aller du $\left(E \frac{ab}{a}\right)^{\text{ème}}$ terme de $f(a, b)$ au $\left(E \frac{a+1}{2} \frac{b}{a}\right)^{\text{ème}}$, s'arrête au $\beta^{\text{ème}}$, d'après l'expression même de $f(a, b)$: or ce dernier terme fait partie du groupe en question, car

$$E \frac{a-1}{2} \frac{b}{a} < \frac{b-1}{2} \leq E \frac{a+1}{2} \frac{b}{a},$$

et, en effet,

$$E \frac{a-1}{2} \frac{b}{a} < \frac{a-1}{2} \frac{b}{a} < \frac{b-1}{2} < \frac{b+1}{2} + E \frac{b-a}{2a} = E \frac{a+1}{2} \frac{b}{a}$$

(α) se réduit donc bien à (5).

7. THÉORÈME. p désignant un nombre premier égal à $2m + 1$, et a , un nombre non divisible par p , on aura :

$$(6) \quad a^m \equiv (-1)^{f(a,p)} \pmod{p} \quad (\text{Gauss})$$

Démonstration de Tchébichef. Posons

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

Selon que $E \frac{2n}{p}$ est pair ou impair, r_n prend l'une ou l'autre des valeurs

$$n - \frac{p}{2} E \frac{2n}{p}, \quad -n + \frac{p}{2} \left(1 + E \frac{2n}{p}\right),$$

toutes deux entières et comprises entre 0 et $\frac{p}{2}$. De plus, on peut écrire

$$r_n \equiv n (-1)^{E \frac{2n}{p}} \pmod{p}$$

On tire de là

$$(7) \quad r_a r_{2a} r_{3a} \dots r_{ma} \equiv a^m m! (-1)^{f(2a,p)} \pmod{p}$$

On ne peut supposer $r_{ka} \equiv r_{la}$, car il s'ensuivrait $a(k \pm l) \equiv 0$, ce qui est impossible, puisque k et l sont $< \frac{p}{2}$ et que a est premier avec p . Par conséquent, les facteurs du premier membre de (7), qui sont d'ailleurs compris entre 0 et $\frac{p}{2}$, ne

¹ Pour abrégér, on sous-entend l'indication (mod p), quand le module est le nombre premier indéterminé p .

² En effet, on a

$$0 < \frac{2n}{p} - E \frac{2n}{p} < 1, \quad \text{d'où} \quad 0 < n - \frac{p}{2} E \frac{2n}{p} < \frac{p}{2},$$

et

$$0 < 1 - \frac{2n}{p} + E \frac{2n}{p} < 1, \quad \text{d'où} \quad 0 < \frac{p}{2} \left(1 + E \frac{2n}{p}\right) - n < \frac{p}{2}.$$

sont autres que les nombres 1, 2, 3, ... m , dans un certain ordre, et (7) peut se simplifier ainsi :

$$(8) \quad 1 \equiv a^m (-1)^{f(2a, p)} \quad \text{ou} \quad a^m \equiv (-1)^{f(2a, p)},$$

ou encore, d'après (1), (8) et (4),

$$(9) \quad a^m \equiv 2^m \left(\frac{a+p}{2} \right)^m \equiv 2^m (-1)^{f(a+p, p)} = 2^m (-1)^{\frac{p^2-1}{8} + f(a, p)}.$$

Pour $a = 1$, on a, à cause de (3)

$$(10) \quad 1 \equiv 2^m (-1)^{\frac{p^2-1}{8}} \quad \text{d'où} \quad 2^m \equiv (-1)^{\frac{p^2-1}{8}},$$

et de là, la relation (6).

A titre d'application, soit à trouver le reste de la division de 5^8 par 17 ; on a

$$E \frac{5}{17} + E \frac{10}{17} + \dots + E \frac{40}{17} = 7, \quad \text{nombre impair ;}$$

on a donc $5^8 \equiv -1 \pmod{17}$.

Cor. I. On a donc toujours cette remarquable relation

$$(11) \quad a^m \equiv \pm 1.$$

Désignons par le *symbole de Legendre*, $\left(\frac{a}{p}\right)$, qui s'énonce *caractère quadratique* de a relativement à p , le reste de la division de a^m par p ; (11) s'écrira ainsi

$$\left(\frac{a}{p}\right) = \pm 1,$$

selon que le nombre $f(a, p)$ est pair ou impair. Dans le premier cas, a est un *résidu* de p , et dans le second, c'en est un *non-résidu*.

II. THÉORÈME DE FERMAT. De (11) on tire, en élevant au

carré, la relation suivante

$$(12) \quad a^{p-1} \equiv 1 \pmod{p}$$

III. La formule (10) montre que $\left(\frac{2}{p}\right)$ a pour valeur 1 quand p est de l'une des formes 8 ± 1 , et -1 , quand il est de l'une des formes 8 ± 3 .

IV. D'après (1), si $a \equiv b$, on a :

$$(13) \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

V. D'après (11), si $\left(\frac{ab}{p}\right) = 1$, on a $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

VI. D'après 2, on a :

$$(14) \quad \left(\frac{abc \dots}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \dots$$

¹ Les deux démonstrations suivantes figurent-elles parmi celles assez nombreuses qu'on a données de ce célèbre théorème. A vrai dire, elles ne sont que des variantes de démonstrations connues ?

1° a et b désignant deux entiers $< p$, formons le cycle de congruences $ab \equiv c, ac \equiv d, ad \equiv e, \dots ak \equiv l, al \equiv b$, qui se trouve en contenir un nombre $n \leq p - 1$. Soit b' un nombre non compris dans la suite $b, c, d, \dots k, l$; on aura ces n' congruences $ab' \equiv c', ac' \equiv d', \dots af' \equiv g', ag' \equiv b'$, et les n' nombres $b', c', \dots g'$ seront différents des n premiers, autrement ils reproduiraient le premier cycle.

Soit b'' un nombre non compris dans les $n + n'$ premiers, on aura ces n'' nouvelles congruences $ab'' \equiv c'', \dots ad'' \equiv e'', ae'' \equiv b''$.

Continuant ainsi, on épuîsera toute la série des $p - 1$ premiers entiers; et multipliant ces congruences, on aura

$$a^{n+n'+\dots} \equiv a^{p-1} \equiv 1.$$

2° Aucun des p produits $a^{p-1}, a^{p-2}b, a^{p-3}b^2, \dots a^2b^{p-3}, ab^{p-2}, b^{p-1}$ n'est $\equiv 0$; il y en a donc au moins deux congrus entre eux. Soit

$$a^{k-1}b^{p-k} \equiv a^{h-1+h}b^{p-k-h}, \quad \text{d'où} \quad a^h \equiv b^h;$$

on voit qu'on peut toujours écrire

$$a^x \equiv b^x, \quad b^y \equiv 1, \quad \text{et de là} \quad az \equiv b \quad (x, y \text{ et } z < p)$$

en posant $a^{x-1}b^{y+1-x} \equiv z$. Il est donc permis de poser

$$az_1 \equiv 1, \quad az_2 \equiv 2, \quad az_3 \equiv 3, \dots az_{p-1} \equiv p - 1,$$

les nombres z_1, z_2, \dots étant tous différents, ce qui donne, en multipliant,

$$a^{p-1}(p-1)! \equiv (p-1)!$$

VII. Puisque $\left(\frac{a}{p}\right) = \pm 1$, on peut écrire :

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{p}\right) = 1 .$$

Donc

$$(15) \quad \left(\frac{a^2 bc \dots}{p}\right) = \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \dots$$

VIII. On a :

$$(16) \quad (p-1)^m \equiv \pm 1, \quad \text{ou} \quad \left(\frac{p-1}{p}\right) = \pm 1,$$

selon que m est pair ou impair (2), c'est-à-dire selon que $p = 4 \pm 1$.

IX. On a :

$$(17) \quad \left(\frac{p-a}{p}\right) = \left(\frac{p-1}{p}\right) \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) (-1)^m .$$

Ainsi

$$(18) \quad \left(\frac{p-2}{p}\right) = \left(\frac{p-1}{p}\right) \left(\frac{2}{p}\right) = (-1)^m (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p-3)}{8}} .$$

8. THÉORÈME. Désignant par p et q deux nombres premiers impairs, et par m et n , les entiers $\frac{p-1}{2}$ et $\frac{q-1}{2}$, on a :

$$(19) \quad \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{mn} \quad (\text{Legendre})$$

C'est la conséquence de (5) et de (6), puisqu'on a :

$$\left(\frac{q}{p}\right) = (-1)^{f(q,p)} \quad \text{et} \quad \left(\frac{p}{q}\right) = (-1)^{f(p,q)} . \quad (\text{Gauss})$$

Ainsi le caractère de p par rapport à q est le même que celui de p par rapport à q , à moins que p et q ne soient tous deux de la forme $4-1$.

La formule (19) peut aussi s'écrire

$$(20) \quad \left(\frac{q}{p}\right) = \pm \left(\frac{p}{q}\right) (-1)^m \quad (p = 4 \pm 1) .$$

Cor. I. On sait (voir *Ens. math.*, 1907, p, 444, 7 et 228, VI) que si $a^m \equiv 1$, p divise $x^2 - ay^2$. Donc si p et q sont de la forme $4 + 1$ et que p divise $x^2 + qy^2$, q divisera $x^2 + py^2$. En effet, on a

$$\left(\frac{-q}{p}\right) = 1, \quad \text{d'où} \quad \left(\frac{-p}{q}\right) = 1. \quad (\text{Legendre})$$

II. Si p est de la forme $4 - 1$ et q , de la forme $4 + 1$; si en outre p ne divise pas $x^2 + qy^2$, q divisera $x^2 + py^2$. En effet, on a :

$$\left(\frac{-p}{q}\right) = -1, \quad \text{d'où} \quad \left(\frac{-q}{p}\right) = 1. \quad (\text{Legendre})$$

III. 1° Soit $q = 3$; on aura, suivant que $p = 4 \pm 1$, ce qui donne $(-1)^m = \pm 1$,

$$\left(\frac{3}{p}\right) = \pm \left(\frac{p}{3}\right).$$

En outre, selon que $p = 3 \pm 1$, il viendra

$$\left(\frac{p}{3}\right) = (-1)^m \left(\frac{3}{p}\right) = (-1)^m \left(\frac{\pm 1}{3}\right) = \pm 1.$$

On a ainsi à examiner les quatre combinaisons 12 ± 1 et 12 ± 5 . On trouve immédiatement

$$p = 12 + 1, \quad \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1, \quad p = 12 - 1, \quad \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1$$

$$p = 12 + 5, \quad \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1, \quad p = 12 - 5, \quad \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1.$$

Ainsi $p = 12 \pm 1$ est diviseur, et $p = 12 \pm 5$ non diviseur de $x^2 - 3y^2$. On peut ajouter que $p = 12 + 1$ et $12 - 5$ sont diviseurs et $p = 12 + 5$ et $12 - 1$, non diviseurs de $x^2 + 3y^2$.

2° Soit $q = 5$; on aura $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \pm 1$, selon que p sera de l'une des formes 20 ± 1 ou 20 ± 9 ; ou de l'une des suivantes 20 ± 3 , 20 ± 7 . De là ce théorème : les nombres premiers 20 ± 1 ou 20 ± 9 sont diviseurs, et les nombres premiers 20 ± 3 ou 20 ± 7 , non diviseurs de $x^2 - 5y^2$; les

nombre premiers $20 + 1, 3, 7, 9$ sont diviseurs et les nombres $20 - 9, -7, -3, -1$, non diviseurs de $x^2 + 5y^2$.

3° Soit encore le nombre composé 15, on aura $\left(\frac{15}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{3}{p}\right)$. Combinant les deux formes 12 ± 1 et 20 ± 1 , on trouve les formes $60 + 1, 7, 11, 17, 43, 49, 53, 59$, pour les diviseurs de $x^2 - 15y^2$.

4° Soit enfin $q = 20$. On a : $\left(\frac{20}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{2^2}{p}\right)$; on est ramené au cas de 5, et en effet les diviseurs de $x^2 \pm 20y^2$ doivent être cherchés dans ceux de $x^2 \pm 5(2y)^2$.

IV. 1° p étant $4 + 1$, tout diviseur impair a de $u^2 + pv^2$ ou de $x^2 + p$ fournit la relation $\left(\frac{a}{p}\right) = \pm 1$, selon que $a = 4 \pm 1$. En effet a est le produit d'une certaine quantité de facteurs premiers α de forme $4 + 1$ par un nombre pair ou impair de facteurs β de forme $4 - 1$. On a donc

$$\left(\frac{-p}{\alpha}\right) = 1 \quad \text{et} \quad \left(\frac{-p}{\beta}\right) = 1, \quad \text{d'où} \quad \left(\frac{p}{\alpha}\right) = 1 \quad \text{et} \quad \left(\frac{p}{\beta}\right) = -1$$

et de là

$$\left(\frac{\alpha}{p}\right) = 1 \quad \text{et} \quad \left(\frac{\beta}{p}\right) = -1, \quad \text{d'où} \quad \left(\frac{a}{p}\right) = \pm 1. \quad (\text{Legendre})$$

Ainsi r étant un résidu et ρ un non résidu de p , on prendra comme diviseurs de $x^2 + p$, les nombres $4 + 1$ qui sont en même temps $\equiv r$, et les nombres $4 - 1$ qui sont en même temps $\equiv \rho$,

Soit $p = 13$; les résidus étant 1, 3, 4, 9, 10, 12, et les non résidus, 2, 5, 6, 7, 8, 11; on prendra d'une part 1, 9, 17, 25, 29, 49, et d'autre part 7, 11, 15, 17, 19, 31, 47, ainsi que les mêmes nombres augmentés de 4. 13, puisque si n est de la forme 4 ± 1 , il en sera de même de $4 + n$. Par conséquent, les diviseurs de $u^2 + 13v^2$ sont de l'une des formes suivantes

$$52 + 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49.$$

2° p étant un nombre premier $4 - 1$, tout diviseur impair

de $u^2 + pv^2$ donne $\left(\frac{a}{p}\right) = 1$. Démonstration et usages analogues (Legendre).

V. Tout nombre premier q compris dans les formes linéaires des diviseurs de $x^2 + py^2$ est nécessairement diviseur de cette forme, p étant $4 + 1$. En effet on a :

$$\left(\frac{q}{p}\right) = \pm 1, \quad \text{selon que } q = 4 \pm 1$$

d'où

$$\left(\frac{p}{q}\right) = \pm 1. \quad (\text{Legendre})$$

Si $p = 4 - 1$, on a une conclusion analogue, mais il y a deux cas à examiner¹.

VI. L'exemple suivant, de Legendre, fera comprendre la marche à suivre pour déterminer le caractère d'un nombre quelconque, si grand soit-il.

On a successivement :

$$\begin{aligned} \left(\frac{601}{1013}\right) &= \left(\frac{1013}{601}\right) = \left(\frac{103}{601}\right) = \left(\frac{601}{103}\right) = \left(\frac{86}{103}\right) = \left(\frac{2}{103}\right) \left(\frac{43}{103}\right) = \left(\frac{43}{103}\right) \\ &= -\left(\frac{103}{43}\right) = -\left(\frac{17}{43}\right) = -\left(\frac{43}{17}\right) = -\left(\frac{9}{17}\right) = -\left(\frac{1}{17}\right) = -1. \end{aligned}$$

Ainsi 1013 ne divise aucun nombre de la forme $x^2 + 601y^2$.

VII. Le nombre 3 est non résidu de $p = 2^{2n} + 1$. En effet, $p + 1 = 2(2^{2n-1} + 1)$ est multiple de 3, d'où $p = 3 - 1$ et par suite

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1. \quad (\text{Tchébichef})$$

VIII. $p = 2^{4n+1} - 1 = 2(4^n - 1) + 1$ est de la forme $3 + 1$; par suite

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1;$$

donc 3 est non résidu de p (Ed. Lucas).

¹ Voir LEJEUNE-DIRICHLET, *Werke*, I, p. 202 et 226, plusieurs extensions de ces théorèmes.

IX. 3 est non résidu de $p = 2^n + 1$ (Ed. Lucas). En effet on a :

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = 1 .$$

(Voir *C. R.*, t. 87, un théorème analogue du P. Pépin.)

9. Soit $p = a^2 + b^2$ un nombre premier $4\mu + 1 = 2m + 1$, a impair et b pair; a est résidu de p , et chacun des deux nombres $a \pm b$ l'est ou ne l'est pas selon qu'il est 8 ± 1 ou 8 ± 3 .

1° Soit α un facteur premier de a ; p est résidu de α ; on a donc :

$$\left(\frac{p}{\alpha}\right) = 1 , \quad \text{d'où} \quad \left(\frac{\alpha}{p}\right) = 1 \quad \text{et} \quad \left(\frac{\Pi\alpha}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{a}{p}\right) = 1 .$$

2° On a : $2p = (a + b)^2 + (a - b)^2$. Soit g un facteur premier du nombre impair $a \pm b$. On peut écrire :

$$\left(\frac{2p}{g}\right) = 1 , \quad \text{donc} \quad \left(\frac{p}{g}\right) = \left(\frac{2}{g}\right) \quad \text{et} \quad \left(\frac{g}{p}\right) = \left(\frac{p}{g}\right) = \left(\frac{2}{g}\right) = \pm 1$$

selon que g est 8 ± 1 ou 8 ± 3 . De là aisément

$$\left(\frac{a \pm b}{p}\right) = (-1)^{\frac{(a \pm b)^2 - 1}{8}} .$$

Cor. On a : $(a + b)^2 \equiv 2ab$, d'où, en élevant à la puissance μ et posant $f \equiv -1^1$, $b \equiv af$,

$$2^\mu f^\mu \equiv (a + b)^m \equiv (f^2)^{\frac{(a + b)^2 - 1}{8}} = f^{\mu + \frac{ab}{2}}$$

et par suite

$$2^\mu \equiv f^{\frac{ab}{2}} ,$$

comme Gauss l'avait autrement démontré. Ainsi 2 est résidu biquadratique si $b = 8b'$: alors $p = a^2 + 64b'^2$, car dans ce cas, $\frac{ab}{2} = 4ab'$ et $f^4 \equiv 1$ (Lejeune-Dirichlet). Reuschle a donné de même le *caractère octique* de 2; et le lieut.-col.

¹ Ce qui est toujours possible si $p = 4 + 1$. (Voir *Ens. math.*, 1907, p. 29.)

Cunningham, son *caractère sextodécimique* (voir le t. XXVII des *Proceed. of the London math. Soc.*, p. 85).

10. Soit $p = a^2 + 2b^2$, un nombre premier $8 + 1$, b est résidu de p . Soient $2, \beta, \beta', \dots$ les facteurs premiers de b . On a :

$$\left(\frac{p}{\beta}\right) = 1, \quad \text{d'où} \quad \left(\frac{\beta}{p}\right) = 1, \quad \text{et comme} \quad \left(\frac{2}{p}\right) = 1, \quad \left(\frac{b}{p}\right) = 1.$$

Cor. Soient g les facteurs premiers 8 ± 1 du nombre impair a , et h ses facteurs premiers 8 ± 3 . De la relation $2p = 2a^2 + (2b)^2$, on tire

$$\left(\frac{2p}{g}\right) = \left(\frac{2p}{h}\right) = 1;$$

et, comme $\left(\frac{2}{g}\right) = 1, \left(\frac{2}{h}\right) = -1$, il vient

$$\left(\frac{p}{g}\right) = 1, \quad \left(\frac{p}{h}\right) = -1, \quad \left(\frac{g}{p}\right) = 1, \quad \left(\frac{h}{p}\right) = -1.$$

Donc $\left(\frac{a}{p}\right) = \pm 1$, et par suite a est ou n'est pas résidu selon que les facteurs h sont en nombre pair ou impair, c'est-à-dire selon que $a = 8 \pm 1$ ou 8 ± 3 .

Elevons à la puissance paire μ , les deux membres de la congruence $a^2 \equiv 2b^2$ et remarquons que $b^m \equiv 1$, on trouve $2^\mu \equiv a^m$. Ainsi 2 et -2 sont ou ne sont pas résidus biquadratiques selon que $a^m \equiv \pm 1$, c'est-à-dire selon que $a = 8 \pm 1$ ou 8 ± 3 (Gauss).

Lejeune-Dirichlet, l'auteur de cette démonstration, en donne plusieurs variantes et extensions, entre autres ce théorème : q désignant un nombre premier $4 - 1$, et p , un nombre premier $4 + 1$, si $p = a^2 + qb^2$, q est résidu biquadratique ou ne l'est pas selon que a est résidu ou non résidu de q .

11. Gauss, qui a introduit les imaginaires dans la théorie des nombres, leur a appliqué plusieurs des théorèmes connus relatifs aux nombres réels. On donnera seulement ici

l'extension de la loi de réciprocité, avec la démonstration de Lejeune-Dirichlet.

On dit qu'un nombre *complexe* $a + bi$ est premier quand il n'a d'autres diviseurs que lui-même et l'une des quatre *unités* $\pm 1, \pm i$. De là les remarques suivantes dues à Gauss.

1° *Tout nombre premier réel* $p \equiv 4 - 1$ *est premier complexe*, car si l'on avait $p = (a + bi)(c + di)$, on pourrait aussi écrire $p = (a - bi)(c - di)$, d'où on tirerait, en multipliant, $p^2 = (a^2 + b^2)(c^2 + d^2)$, ce qui est impossible, p ne pouvant diviser une somme de deux carrés.

2° *Le nombre réel 2 et les nombres premiers réels* $p \equiv 4 + 1$ *sont composés au point de vue complexe*, car on a : $2 = (1 + i)(1 - i)$, et d'autre part, on peut écrire :

$$p = a^2 + b^2 = (a + bi)(a - bi) .$$

3° *Pour que* $a + bi$ *soit premier, il faut et il suffit que sa norme* $a^2 + b^2$ *le soit, au point de vue réel*. Supposons que $a + bi = (c + di)(e + fi)$; on aura de même $a - bi = (c - di)(e - fi)$, d'où

$$a^2 + b^2 = (c^2 + d^2)(e^2 + f^2) .$$

Réciproquement, si $a^2 + b^2$ est un nombre composé, il en est de même de $a + bi$. Soit $p = g^2 + h^2$ un des diviseurs premiers de $a^2 + b^2$, on aura :

$$a^2 \equiv -b^2 \quad \text{et} \quad g^2 \equiv -h^2 , \quad \text{d'où en multipliant,} \quad (ag + bh)(ag - bh) \equiv 0 .$$

Or

$$p(a^2 + b^2) = (ag \pm bh)^2 + (ah \mp bg)^2 .$$

De ces deux congruences, on conclut que l'un des deux nombres $ag \pm bh$ est de la forme kp ; et par suite, l'un des deux autres $ah \mp bg$, de la forme lp . De là, en éliminant a et b , la relation

$$a + bi = (k + li)(g + hi) .$$

12. 1° *Disons par extension que* $a + bi$ *est résidu ou non résidu de* $p \equiv 4 - 1$ *selon qu'on peut ou qu'on ne peut écrire :* $(x + yi)^2 \equiv a + bi$; $a + bi$ *est résidu ou non en même temps*

que $a^2 + b^2$. Soit $(x + yi)^2 \equiv a + bi$; on aura de même $(x - yi)^2 \equiv a - bi$, et par suite,

$$(x^2 + y^2)^2 \equiv a^2 + b^2 .$$

D'un autre côté, on peut toujours écrire¹: $g^2 + h^2 + 1 \equiv 0$; $g^2 + h^2$ est donc un non résidu puisque -1 est non résidu de $p = 4 - 1$; et il en est de même de $g + hi$, car autrement, d'après le premier cas, $g^2 + h^2$ serait résidu.

Si $a + bi$ est également un non résidu, le produit

$$(a + bi)(g + hi) = (ag - bh) + (ah + bg)i$$

est résidu, ainsi que

$$(ag - bh)^2 + (ah + bg)^2 = (a^2 + b^2)(h^2 + g^2) ;$$

par conséquent, $a^2 + b^2$ est non résidu.

Ainsi $1 + i$ et $1 - i$ sont résidus ou non résidus en même temps que 2, c'est-à-dire selon que $p = 8 - 1$ ou $8 + 3$.

2° On peut toujours écrire $x \equiv (a + bi) \pmod{A + Bi}$, les nombres A et B étant premiers entre eux; car cette relation revient à

$$x - a - bi = (y + zi)(A + Bi) .$$

Or on peut poser $By + Az = -b$; y et z étant ainsi déterminés, on aura, pour la valeur de x , l'entier $a + Ay - Bz$.

3° On démontrera, de la même manière que pour les nombres réels, que *le produit de deux résidus est un résidu, etc.*

4° Soit $p = A^2 + 4B^2$ un nombre premier $4 + 1$; on dira que $a + bi$ est ou n'est pas résidu de $A + 2Bi$ selon qu'on peut ou qu'on ne peut trouver deux nombres y et z tels que $(y + zi)^2 \equiv (a + bi) \pmod{A + 2Bi}$.

Posons d'après 2° $x \equiv y + zi \pmod{A + 2Bi}$. La question revient à découvrir les conditions de possibilité de la relation

$$(\alpha) \quad x^2 - a - bi = (A + 2Bi)(t + ui)$$

¹ Voir *Ens. math.*, 1907, p. 31 et 454.

ou celle des suivantes

$$(\beta) \quad x^2 = a + At - 2Bu, \quad -b = Au + 2Bt,$$

d'où

$$(\gamma) \quad Ax^2 - Aa - 2Bb = pt,$$

ce qui montre que $Aa + 2Bb$ est résidu de p , car A l'est lui-même (9).

Réciproquement si cette condition a lieu, $a + bi$ est résidu de $A + 2Bi$. En effet il y a un résidu $r \equiv x^2$ qui, multiplié par le résidu $Aa + 2Bb$, donne le résidu A ; de là la relation (γ) qu'on peut écrire

$$A(a + At - x^2) + 2B(2Bt + b) \equiv 0 :$$

$2Bt + b$ est donc de la forme $-Au$, ce qui donne (β) et de là (α).

Ainsi, p désignant un nombre premier $A^2 + 4B^2$ de forme $4 + 1$, $a + bi$ est résidu ou non résidu de $A + 2Bi$ selon que $Aa + 2Bb$ l'est ou ne l'est pas de p . Autrement dit, on a :

$$(\delta) \quad \left(\frac{a + bi}{A + 2Bi} \right) = \left(\frac{Aa + 2Bb}{p} \right). \quad (\text{Lejeune-Dirichlet})$$

Ainsi on a :

$$\left(\frac{1 + i}{A + 2Bi} \right) = \left(\frac{A + 2B}{p} \right);$$

donc, à cause de 9, on peut dire que $1 + i$ est résidu ou non résidu de $A + 2Bi$ selon que $A + 2B$ est 8 ± 1 ou 8 ± 3 .

5° Soit q un nombre premier $4 - 1$ et $p = A^2 + 4B^2$ un nombre premier $4 + 1$; on a, d'après 1° et 4°,

$$\begin{aligned} \left(\frac{A + 2Bi}{q} \right) &= \left(\frac{p}{q} \right) = \left(\frac{q}{p} \right), \\ \left(\frac{q}{A + 2Bi} \right) &= \left(\frac{qA}{p} \right) = \left(\frac{q}{p} \right) \left(\frac{A}{p} \right) = \left(\frac{q}{p} \right) \end{aligned}$$

d'où

$$\left(\frac{A + 2Bi}{q} \right) = \left(\frac{q}{A + 2Bi} \right).$$

6° Soient $p = A^2 + 4B^2$, $p' = A'^2 + 4B'^2$, deux nombres premiers $4 + 1$; on a :

$$\left(\frac{A + 2Bi}{A' + 2B'i}\right) = \left(\frac{AA' + 4BB'}{p'}\right), \quad \left(\frac{A' + 2B'i}{A + 2Bi}\right) = \left(\frac{AA' + 4BB'}{p}\right)$$

$$(AA' + 4BB')^2 + (2AB' - 2BA')^2 = pp'$$

Si g est un des facteurs premiers du nombre impair $AA' + 4BB'$, on a, d'après ce qui précède :

$$\left(\frac{p}{g}\right) = \left(\frac{p'}{g}\right), \quad \text{d'où} \quad \left(\frac{g}{p}\right) = \left(\frac{g}{p'}\right) \quad \text{et} \quad \left(\frac{AA' + 4BB'}{p}\right) = \left(\frac{AA' + 4BB'}{p'}\right),$$

d'où cette généralisation, due à Gauss,

$$\left(\frac{A + 2Bi}{A' + 2B'i}\right) = \left(\frac{A' + 2B'i}{A + 2Bi}\right).$$

13. Il ne paraît pas nécessaire de reproduire ici les renseignements historiques donnés précédemment (*E. M.*, 1909, pp. 347, 432, 434, 440, 446) sur la loi de réciprocité. Il suffira, pour la présente note, — qui n'a d'autre ambition que celle de fournir l'idée et la matière d'un chapitre à un traité élémentaire des nombres, — de la compléter par l'exposé de trois des plus simples démonstrations qu'on a données de ce si remarquable théorème : elles s'appuient toutes les trois sur ce lemme de Gauss, démontré, *E. M.*, 1907, p. 37 :

p désignant un nombre premier, et a un entier inférieur à p , appelons $\varphi(a, p)$ le nombre des restes supérieurs à $\frac{p}{2}$ obtenus en divisant par p les m premiers multiples de a ; on a :

$$a^m \equiv (-1)^{\varphi(a, p)} \quad \text{ou bien} \quad \left(\frac{a}{p}\right) = (-1)^{\varphi(a, p)}.$$

1° *Démonstration d'Eisenstein.* Soient a et b deux entiers impairs premiers entre eux; construisons un parallélogramme sur ces deux nombres, menons la diagonale et traçons le réseau correspondant aux divisions des côtés. Le nombre des intersections de la $k^{\text{ème}}$ ordonnée entre la base et la diagonale est $E \frac{ka}{b}$. Il ne se trouve aucune intersection

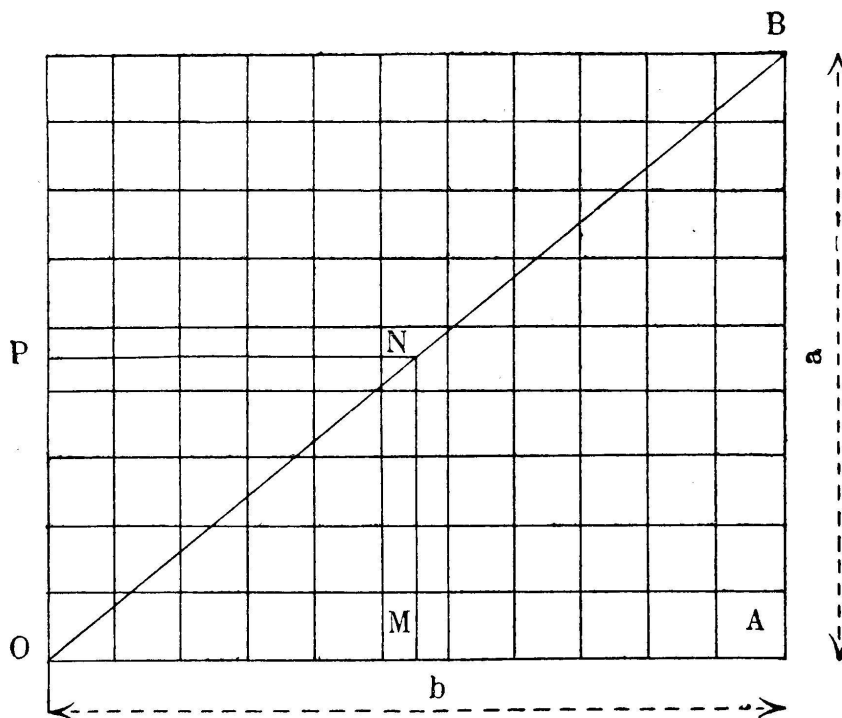
sur la diagonale; on a donc :

$$E \frac{ka}{b} + E \frac{(b-k)a}{b} = a - 1, \text{ nombre pair,}$$

et par suite

$$\begin{array}{ccc}
 E \frac{a}{b} & \text{est de même parité que} & E \frac{(b-1)a}{b} \\
 E \frac{2a}{b} & \dots \dots \dots & E \frac{2a}{b} \\
 E \frac{3a}{b} & \dots \dots \dots & E \frac{(b-2)a}{b} \\
 E \frac{4a}{b} & \dots \dots \dots & E \frac{4a}{b} \\
 \dots & \dots \dots \dots & \dots \\
 E \frac{(b-1)a}{2b} & \dots \dots \dots & E \frac{(b \pm 1)a}{2b} \quad (b = 4 \mp 1)
 \end{array}$$

d'où on déduit, en se rappelant la notation du n° 4, que $f(a, b)$ est de même parité que $f(2a, b)$. Or si on construit



le parallélogramme $\frac{a}{2}, \frac{b}{2}$, on voit que $f(a, b)$ et $f(b, a)$ représentent respectivement les nombres des intersections comprises dans les triangles ONM, ONP. On conclut de là que

$$f(a, b) + f(b, a) = \alpha\beta,$$

et que par suite $f(2a, b) + f(2b, a)$ est de même parité que $\alpha\beta$, ce qui, rapproché de (8), fournit la démonstration de (20).

2° *Démonstration de Voigt.* Divisons par b les β premiers multiples de a , et posons

$$ga < kb < (g + 1)a, \quad ha < (k + 1)b < (h + 1)a;$$

celles de ces divisions donnant le quotient k correspondent aux multiples $(g + 1)a, (g + 2)a, \dots, (h - 1)a, ha$; et parmi ces $h - g$ divisions, celles qui fournissent des restes plus grands que $\frac{b}{2}$ sont déterminés par la relation

$$(g + x)a - kb > \frac{b}{2},$$

d'où

$$(\alpha) \quad h \geq g + x > \frac{2k + 1}{2a}b;$$

elles sont donc au nombre de

$$E \frac{k + 1}{a}b - E \frac{2k + 1}{2a}b = E \frac{k + 1}{a}b - \beta - E \left(\frac{1}{2} - \frac{a - 2k - 1}{2a}b \right).$$

Mais le plus petit multiple de a qui, divisé par b , donne un quotient $k = \alpha$, et un reste $> \frac{b}{2}$, est supérieur, d'après (α), à

$$(\beta) \quad \frac{2k + 1}{2}b = \frac{ab}{2} > \frac{b - 1}{2}a = \beta a;$$

et le plus grand multiple de a qui, divisé par b , donne un quotient $k = \alpha - 1$ avec un reste $> \frac{b}{2}$, est, également d'après (α), au plus égal à

$$ha = \left(E \frac{k + 1}{a}b \right)a < \left(\frac{k + 1}{a}b \right)a = (k + 1)b = \frac{a - 1}{2}b < \frac{b - 1}{2}a = \beta a,$$

si on suppose $b > a$.

D'après le lemme fondamental (*E. M.*, 1907, p. 287), les restes sont tous différents, et par suite on aura le nombre $\varphi(a, b)$ des restes supérieurs à $\frac{b}{2}$ en faisant successivement $k = 0, 1, 2, 3, \dots, \alpha - 1$ dans (β) et additionnant.

Il vient ainsi, en groupant convenablement les résultats :

$$(\gamma) \left\{ \begin{aligned} & \varphi(a, b) + \alpha\beta \\ & = \left[E \frac{b}{a} - E \left(\frac{1}{2} - \frac{b}{a} \right) \right] + \left[E \frac{2b}{a} - E \left(\frac{1}{2} - \frac{2b}{a} \right) \right] \\ & \quad + \dots + \left[E \frac{a-1}{2a} b - E \left(\frac{1}{2} - \frac{a-1}{2a} b \right) \right] \\ & \equiv E \frac{b}{a} + E \left(\frac{1}{2} - \frac{b}{a} \right) + E \frac{2b}{a} + E \left(\frac{1}{2} - \frac{2b}{a} \right) \\ & \quad + \dots + E \frac{a-1}{2a} b + E \left(\frac{1}{2} - \frac{a-1}{2a} b \right). \quad (\text{mod } 2) \end{aligned} \right.$$

Or la valeur de $E \frac{c}{a} + E \left(\frac{1}{2} - \frac{c}{a} \right)$ est 0 ou -1 selon que le reste de la division de c par a est $\geq \frac{a}{2}$. En effet, soit $c = a\alpha + r$, on aura $E \frac{c}{a} = \alpha$, d'où

$$E \frac{c}{a} + E \left(\frac{1}{2} - \frac{c}{a} \right) = E \left(\alpha + \frac{1}{2} - \alpha - \frac{r}{a} \right) = E \left(\frac{1}{2} - \frac{r}{a} \right),$$

de sorte que, selon que $r = \frac{a}{2} \pm \omega$, il vient

$$E \frac{c}{a} + E \left(\frac{1}{2} - \frac{c}{a} \right) = E(\mp \omega).$$

Le dernier membre de (γ) représente donc, au signe près, le nombre $\varphi(b, a)$ des restes $> \frac{a}{2}$ provenant de la division par a des α premiers multiples de b ; d'où

$$(\delta) \quad \varphi(a, b) + \varphi(b, a) \equiv \alpha\beta. \quad (\text{mod } 2)$$

3° *Démonstration de Kronecker.* Le reste de la division de ha par b est $> \frac{b}{2}$ si on peut trouver un entier k tel qu'on ait :

$$(\alpha) \quad ha < bk < ha + \frac{b}{2},$$

d'où

$$(\beta) \left\{ \begin{aligned} & (ha - bk) \left(ha - bk + \frac{b}{2} \right) < 0 \\ \text{ou} & (ha - bk) \left(ha + \frac{a+1-2k}{2} b - \frac{ab}{2} \right) < 0. \end{aligned} \right.$$

