ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

T.-J. STIELTJES

Contribution à la théorie des résidus cubiques et biquadratiques

Annales de la faculté des sciences de Toulouse 1re série, tome 11, no 2 (1897), p. C25-C65

<http://www.numdam.org/item?id=AFST_1897_1_11_2_C25_0>

De là résulte donc

$$\mathrm{A} = -a \qquad \text{et} \qquad \mathrm{B} = \pm b.$$

Le signe de B s'obtient par une considération analogue à celle du n° 12.

On trouve aisément

$$\Sigma(z^2+1)^{\frac{1}{4}(\mu-1)} \equiv -1 \equiv 2(h-k) + 2i(j-l) \pmod{\mathrm{M}}.$$

Or

$$2(h-k) = \mathrm{A} - 1, \qquad 2(j-l) = \mathrm{B},$$

donc

$$-1 \equiv \mathrm{A} - 1 + \mathrm{B}i,$$
$$0 \equiv \mathrm{A} + \mathrm{B}i \qquad [\mathrm{mod}(\mathrm{M} = a + bi)].$$

Puisqu'on a déjà trouvé $\mathrm{A} = -a$, il s'ensuit $\mathrm{B} = -b$, de sorte qu'on a finalement

$$8h = 4n - a - 1,$$
$$8j = 4n - a - 2b + 3,$$
$$8k = 4n + 3a + 3,$$
$$8l = 4n - a + 2b + 3,$$
$$8m = 4n + a + 1.$$

15. En rapprochant les résultats obtenus, on voit que, pour $\mu = 8n+1$, le schéma (S) est de la forme

$$\begin{array}{cccc} h & j & k & l \\ j & l & m & m \\ k & m & k & m \\ l & m & m & j, \end{array}$$

où, pour $\mathrm{M} = -q$, on a

$$8h = 4n - 3\mathrm{M} - 5,$$
$$8j = 8k = 8l = 4n + \mathrm{M} - 1,$$
$$8m = 4n - \mathrm{M} + 1,$$

pour $\mathrm{M} = a + bi$

$$8h = 4n - 3a - 5,$$
$$8j = 4n + a - 2b - 1,$$
$$8k = 4n + a - 1,$$
$$8l = 4n + a + 2b - 1,$$
$$8m = 4n - a + 1.$$

Pour $\mu = 8n + 5$, $\mathrm{M} = a + bi$, le schéma (S) a la forme

$$\begin{matrix} h & j & k & l \\ m & m & l & j \\ h & m & h & m \\ m & l & j & m, \end{matrix}$$

où

$$\begin{aligned} 8h &= 4n - a - 1, \\ 8j &= 4n - a - 2b + 3, \\ 8k &= 4n + 3a + 3, \\ 8l &= 4n - a + 2b + 3, \\ 8m &= 4n + a + 1. \end{aligned}$$

Ainsi qu'il ressort de ces formules, le changement de b en $-b$ correspond à une permutation de j et l, tant dans le cas de $\mu = 8n + 1$, que lorsque $\mu = 8n + 5$.

D'après les congruences du n° 5, on a, dans le cas $\mu = 8n + 1$, pour le caractère de $1 + i$ suivant le module 4

$$\text{Caractère } (1+i) \equiv (3,1) + 2(3,2) + 3(3,3) = 3m + 3j \equiv -m - j,$$

et pour celui de $1 - i$

$$\text{Caractère } (1-i) \equiv (1,1) + 2(1,2) + 3(1,3) = l + 5m \equiv l + m;$$

donc, pour $\mathrm{M} = -q$,

$$\text{Caractère } (1+i) \equiv -n = -\frac{q^2-1}{8}.$$

$$\text{Caractère } (1-i) \equiv \quad n = \frac{q^2-1}{8}.$$

Or, $\frac{q+1}{4}$ et $\frac{q-3}{4}$ sont des nombres entiers consécutifs; leur produit est donc pair et $\frac{(q+1)(q-3)}{8}$ est divisible par 4, de sorte qu'on a

$$\frac{q^2-1}{8} \equiv \frac{q^2-1}{8} - \frac{(q+1)(q-3)}{8} = +\frac{q+1}{4},$$

par conséquent

$$\left(\left(\frac{1+i}{\mathrm{M}}\right)\right) = i^{\frac{1}{4}(\mathrm{M}-1)}, \qquad \left(\left(\frac{1-i}{\mathrm{M}}\right)\right) = i^{-\frac{1}{4}(\mathrm{M}-1)},$$

et, vu que -1 est résidu biquadratique,

$$\left(\left(\frac{-1-i}{\mathrm{M}}\right)\right) = i^{\frac{1}{4}(\mathrm{M}-1)}, \qquad \left(\left(\frac{-1+i}{\mathrm{M}}\right)\right) = i^{-\frac{1}{4}(\mathrm{M}-1)},$$

tandis que, de $2 = (1-i)(1+i)$, il suit encore

$$\left(\left(\frac{2}{\mathrm{M}}\right)\right) = \left(\left(\frac{-2}{\mathrm{M}}\right)\right) = 1.$$

Pour $\mathrm{M} = a + bi$, au contraire, on a

$$\begin{aligned} -m-j &= -n+\tfrac{1}{4}b, \\ l+m &= \quad n+\tfrac{1}{4}b, \end{aligned}$$

et

$$n = \frac{a^2+b^2-1}{8}.$$

Mais évidemment $\frac{a-1}{4}\,\frac{a+3}{4}$ est pair, et, par conséquent, $\frac{(a-1)(a+3)}{8}$ est divisible par 4, d'où il suit

$$\frac{a^2-1}{8} \equiv \frac{-a+1}{4} \pmod 4;$$

en outre, b étant divisible par 4, l'un des nombres b, $b \pm 4$ est divisible par 8; $\frac{b(b\mp 4)}{8}$ est donc divisible par 4, et l'on a

$$\frac{b^2}{8} \equiv \frac{b^2}{8} - \frac{b(b\mp 4)}{8} = \pm\frac{1}{2}b,$$

de sorte que

$$n \equiv \tfrac{1}{4}(-a+1\pm 2b) \pmod 4,$$

et finalement

$$\left(\left(\frac{1+i}{\mathrm{M}}\right)\right) = \left(\left(\frac{-1-i}{\mathrm{M}}\right)\right) = i^{\frac{1}{4}(a-1-b)},$$

$$\left(\left(\frac{1-i}{\mathrm{M}}\right)\right) = \left(\left(\frac{-1+i}{\mathrm{M}}\right)\right) = i^{\frac{1}{4}(-a+1-b)}$$

$$\left(\left(\frac{2}{\mathrm{M}}\right)\right) = i^{-\frac{1}{2}b}.$$

Lorsque, enfin, $\mu = 8n+5$, $\mathrm{M} = a+bi$, on a

$$\begin{aligned} &\text{Caractère } (1+i) \equiv (1,1) + 2(1,2) + 3(1,3) = m + 2l + 3j \pmod 4, \\ &\text{Caractère } (1-i) \equiv (3,1) + 2(3,2) + 3(3,3) = l + 2j + 3m \pmod 4, \end{aligned}$$

où, toutes les congruences ayant rapport au module 4, on a

$$\begin{aligned} m + 2l + 3j &= 3n + \tfrac{1}{4}(-2a-b+8), \\ l + 2j + 3m &= 3n + \tfrac{1}{4}(-b+6) \equiv -n + \tfrac{1}{4}(-b+6), \end{aligned}$$

$$n = \frac{a^2+b^2-5}{8}.$$

$\frac{a-3}{4}\,\frac{a+1}{4}$ étant pair, $\frac{(a-3)(a+1)}{8}$ est divisible par 4, et il en est de même de $\frac{(b-2)(b+2)}{8}$; donc

$$n \equiv \frac{a^2+b^2-5}{8} - \frac{(a-3)(a+1)}{8} - \frac{b^2-4}{8} = \frac{1}{4}(+a+1),$$

de sorte qu'on obtient finalement

$$\begin{aligned} m+2l+3j &\equiv \tfrac{1}{4}(a-b+11) \equiv \tfrac{1}{4}(a-b-5), \\ l+2j+3m &\equiv \tfrac{1}{4}(-a-b+5), \end{aligned}$$

par suite

$$\left(\left(\frac{1+i}{a+bi}\right)\right) = i^{\frac{1}{4}(a-b-5)}, \qquad \left(\left(\frac{1-i}{a+bi}\right)\right) = i^{\frac{1}{4}(-a-b+5)},$$

et, le caractère de -1 étant égal à deux,

$$\left(\left(\frac{-1-i}{a+bi}\right)\right) = i^{\frac{1}{4}(a-b+3)}, \qquad \left(\left(\frac{-1+i}{a+bi}\right)\right) = i^{\frac{1}{4}(-a-b-3)},$$

et

$$\left(\left(\frac{2}{a+bi}\right)\right) = i^{-\frac{1}{2}b}.$$

Par là se trouve déterminé, dans chaque cas, le caractère biquadratique de $1+i$, ainsi que celui de $1-i$, $-1-i$, $-1+i$, par rapport à un nombre premier primaire. Les résultats concordent entièrement avec ceux donnés par Gauss dans les Art. 63, 64 de la *Theoria residuorum biquadraticorum commentatio secunda* et démontrés par lui, d'une manière tout à fait différente, dans les Art. 68-76.

16. Relativement à l'analogie qui existe entre une grande partie des considérations précédentes et celles que Gauss a développées dans les Art. 8 et suiv. de son *premier* Mémoire sur la théorie des résidus biquadratiques, il y a à faire les remarques suivantes :

Gauss considère des nombres réels; le module premier p est de la forme $4n+1$, et il faut distinguer les deux cas $p = 8n+1$, $p = 8n+5$; p a donc la même signification que la norme μ dans les cas II et III de notre n° 4.

Les nombres $1, 2, 3, \ldots, p-1$ sont partagés par Gauss en quatre classes (A), (B), (C), (D). Les nombres de ces classes étant représentés par α, β,

γ, δ, cette classification est fondée sur les congruences

$$\begin{aligned} &\alpha^{\frac{\mu-1}{4}} \equiv 1 \qquad (\text{mod}\,\mu = p),\\ &\beta^{\frac{\mu-1}{4}} \equiv f,\\ &\gamma^{\frac{\mu-1}{4}} \equiv -1,\\ &\delta^{\frac{\mu-1}{4}} \equiv -f, \end{aligned}$$

où $f^2 \equiv -1 \pmod p$, et pour $\mu = a^2 + b^2$

$$a \equiv 1 \pmod 4, \qquad a + bf \equiv 0 \pmod p.$$

Pour $p = \mu = 8n + 1$, a et b ont la même signification que ci-dessus; pour $p = 8n + 5$, a et b, chez Gauss, ne diffèrent que par le signe des valeurs qu'ils ont dans ce qui précède, où $M = a + bi$ est un nombre premier complexe *primaire*.

Lorsque, toutefois, on admet aussi des nombres complexes, il est clair que les congruences ci-dessus, qui sont relatives au module $p = \mu$, restent valables pour le module $a+bi$, de sorte qu'on a aussi $a+bf \equiv 0 \pmod{a+bi}$, d'où résulte $f \equiv i \pmod{a+bi}$, et, par conséquent,

$$\alpha^{\frac{\mu-1}{4}} \equiv 1, \qquad \beta^{\frac{\mu-1}{4}} \equiv i, \qquad \gamma^{\frac{\mu-1}{4}} \equiv -1, \qquad \delta^{\frac{\mu-1}{4}} \equiv -i \pmod{a+bi}.$$

La classification de Gauss est donc identique à celle établie suivant le caractère biquadratique 0, 1, 2, 3 par rapport au module $a + bi$.

Effectivement, les nombres réels 1, 2, 3, ..., $p - 1$ forment pour le module $a + bi$ un système complet de résidus incongrus, non divisibles par le module.

Aussi, en remplaçant dans les deux derniers exemples du n° 5 les résidus complexes par les nombres réels congrus, ce qui se fait sans peine à l'aide de $i \equiv 27 \pmod{-3-8i}$ et de $i \equiv 11 \pmod{-5+6i}$, on obtient

$$(\text{mod} -3 - 8i), \qquad \mu = 73.$$

(A) 1, 2, 4, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72.

(B) 5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68.

(C) 3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70.

(D) 11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62.

$$(\mathrm{mod}\ -5+6i), \qquad \mu = 61.$$

(A)	1,	9,	12,	13,	15,	16,	20,	22,	25,	34,	42,	47,	56,	57,	58.
(B)	2,	7,	18,	23,	24,	26,	30,	32,	33,	40,	44,	50,	51,	53,	55.
(C)	3,	4,	5,	14,	19,	27,	36,	39,	41,	45,	46,	48,	49,	52,	60.
(D)	6,	8,	10,	11,	17,	21,	28,	29,	31,	35,	37,	38,	43,	54,	59.

en accord parfait avec les exemples donnés par Gauss dans l'Art. 11 de son premier Mémoire.

Le cas I de notre n° 4 est le seul pour lequel il n'existe rien d'analogue dans la théorie réelle de Gauss, ce qui tient à ce que dans ce cas on ne peut pas former, avec des nombres réels, un système complet de résidus.

L'observation que la division en quatre classes (A), (B), (C), (D), effectuée par Gauss dans son premier Mémoire, est identique à celle faite d'après le caractère biquadratique par rapport au module $a+bi$ fournit aussi le moyen de déduire immédiatement tous les théorèmes que Gauss a trouvés par induction dans son second Mémoire, Art. 28, mais dont, à ma connaissance, aucune démonstration n'a été donnée jusqu'ici.

Ces théorèmes sont relatifs à la présence d'un nombre premier réel m dans les quatre classes (A), (B), (C), (D), ou, d'après ce qui précède, au caractère biquadratique de m par rapport au module $a+bi$.

17. Je vais reproduire maintenant les remarques formulées par Gauss dans l'Art. 28. Le module premier $p=\mu$ étant supposé de la forme $4n+1$, il s'agit maintenant, d'après ce qui a été dit au numéro précédent, de déterminer la valeur du symbole

$$\left(\left(\frac{m}{a+bi}\right)\right),$$

où m est un nombre premier réel; la circonstance que, pour $\mu = 8n+5$, a et b ont, chez Gauss, un signe différent de celui des valeurs du n° 14 n'a aucune influence sur l'énoncé des théorèmes. Le nombre premier m recevra un signe tel qu'il soit toujours $\equiv 1 \pmod 4$, donc le signe *moins* lorsque, pris positivement, il est de la forme $4k+3=Q$; un nombre

premier positif de la forme $4k+1$ sera représenté par P. Les remarques de Gauss peuvent alors être exprimées de cette manière :

I. Lorsque $a \equiv 0 \pmod m$, la valeur de $\left(\left(\frac{m}{a+bi}\right)\right)$ est $= +1$ ou $= -1$; elle est égale à $+1$ si m a la forme $8r \pm 1$, égale à -1 si m a la forme $8r \pm 3$.

II. Lorsque a n'est pas divisible par m, la valeur du symbole dépend uniquement du nombre complètement déterminé x, qui satisfait à

$$b \equiv ax \pmod m.$$

Pour $m = \mathrm{P}$, x peut prendre ici les valeurs suivantes

$$0,\ 1,\ 2,\ 3,\ \ldots,\ \mathrm{P}-1,$$

à l'exception des deux valeurs f et $\mathrm{P}-f$ qui satisfont à $yy \equiv -1 \pmod{\mathrm{P}}$. Ces deux valeurs ne peuvent évidemment pas se présenter, car de $b \equiv ay$ il résulterait

$$b^2 \equiv -a^2 \quad \text{ou} \quad a^2+b^2 = p \equiv 0 \pmod{\mathrm{P}},$$

c'est-à-dire que p devrait être divisible par P.

Pour $m = -\mathrm{Q}$, au contraire, x peut prendre toutes les valeurs

$$0,\ 1,\ 2,\ 3,\ \ldots,\ \mathrm{Q}-1.$$

Ces valeurs de x peuvent être réparties en quatre classes α, β, γ, δ, de telle sorte que

pour $b \equiv a\alpha \pmod m$, la valeur du symbole $\left(\left(\frac{m}{a+bi}\right)\right)$ soit $= 1$,
» $b \equiv a\beta$ » $= i$,
» $b \equiv a\gamma$ » $= -1$,
» $b \equiv a\delta$ » $= -i$,

ou, ce qui revient au même, que dans ces cas m appartienne respectivement aux classes (A), (B), (C), (D).

Or, en ce qui concerne la *quotité* des nombres α, β, γ, δ, existe cette règle : que trois de ces quotités sont égales, tandis que la quatrième est plus petite d'une unité; d'ailleurs, cette quatrième quotité est celle des α lorsque, pour $a \equiv 0$, m appartient à (A), et celle des γ lorsque, pour $a \equiv 0$, m appartient à (C).

18. Soit donc, en premier lieu, $m = -\mathrm{Q}$; d'après la loi de réciprocité, on a alors

$$\left(\left(\frac{-\mathrm{Q}}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{\mathrm{Q}}\right)\right)$$

et, pour $a \equiv 0 \pmod{Q}$,

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{bi}{Q}\right)\right) = \left(\left(\frac{b}{Q}\right)\right)\left(\left(\frac{i}{Q}\right)\right) = i^{\frac{Q^2-1}{4}},$$

vu que $\left(\left(\frac{b}{Q}\right)\right) = 1$; en effet,

$$\left(\left(\frac{b}{Q}\right)\right) \equiv b^{\frac{Q^2-1}{4}} \pmod{Q},$$

et, comme Q est de la forme $4r+3$, donc $\frac{Q^2-1}{4} = (Q-1)\frac{Q+1}{4}$ un multiple de $Q-1$, il suit du théorème de Fermat

$$\left(\left(\frac{b}{Q}\right)\right) = 1.$$

Pour $Q = 8n+3$ on trouve maintenant

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = -1,$$

pour $Q = 8n+7$

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = +1.$$

Lorsque, au contraire, on a

$$m = P = (A+Bi)(A-Bi),$$

où $A+Bi$ et $A-Bi$ sont les facteurs primaires de P, il suit de la loi de réciprocité

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{A+Bi}\right)\right)\left(\left(\frac{a+bi}{A-Bi}\right)\right)$$

et, pour $a \equiv 0 \pmod{P}$,

$$\begin{aligned}\left(\left(\frac{P}{a+bi}\right)\right) &= \left(\left(\frac{bi}{A+Bi}\right)\right)\left(\left(\frac{bi}{A-Bi}\right)\right) \\ &= \left(\left(\frac{-bi}{A+Bi}\right)\right)\left(\left(\frac{+bi}{A-Bi}\right)\right)\left(\left(\frac{-1}{A+Bi}\right)\right).\end{aligned}$$

Or, en général, comme l'on sait,

$$\left(\left(\frac{\alpha+\beta i}{A+Bi}\right)\right)\left(\left(\frac{\alpha-\beta i}{A-Bi}\right)\right) = 1,$$

donc

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{-1}{A+Bi}\right)\right) = (-1)^{\frac{P-1}{4}},$$

ou, pour $P = 8n + 1$,

$$\left(\left(\frac{P}{a+bi}\right)\right) = 1,$$

et, pour $P = 8n + 5$,

$$\left(\left(\frac{P}{a+bi}\right)\right) = -1.$$

Ainsi se trouve complètement démontrée la proposition I énoncée au numéro précédent.

19. Supposons maintenant que a ne soit pas divisible par m, et considérons d'abord le cas le plus simple

$$m = -Q;$$

on a donc alors

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{Q}\right)\right)$$

et, pour $b \equiv ax \pmod{Q}$,

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{a(1+xi)}{Q}\right)\right) = \left(\left(\frac{1+xi}{Q}\right)\right),$$

à cause de l'égalité $\left(\left(\frac{a}{Q}\right)\right) = 1$, déjà démontrée au numéro précédent. Du résultat obtenu

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{1+xi}{Q}\right)\right)$$

il ressort déjà que la valeur du symbole à gauche dépend uniquement du nombre x, lequel peut prendre les Q valeurs

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad Q-1.$$

Nous n'avons donc plus qu'à résoudre cette question : lorsque le module Q est un nombre premier de la forme $4n + 3$, combien, parmi les nombres

$$1, \quad 1+i, \quad 1+2i, \quad 1+3i, \quad \ldots, \quad 1+(Q-1)i,$$

y en a-t-il qui appartiennent respectivement aux classes (A), (B), (C), (D)?

A cet effet, je remarquerai, en premier lieu, qu'on peut prendre, comme système complet de résidus non divisibles par Q, les nombres

$$\alpha + \beta i$$

où α et β parcourent les valeurs 0, 1, 2, 3, ..., $Q-1$, à l'exception de la combinaison $\alpha = 0$, $\beta = 0$; et, en second lieu, que les nombres

$$1, \quad 2, \quad 3, \quad \ldots, \quad Q-1$$

appartiennent tous à (A), de sorte que, lorsque le nombre

$$\alpha' + \beta' i$$

fait partie d'une certaine classe, celle-ci renferme également les nombres

$$2(\alpha' + \beta' i), \quad 3(\alpha' + \beta' i), \quad \ldots, \quad (Q-1)(\alpha' + \beta' i),$$

qui, par l'omission de multiples de Q, peuvent tous être ramenés à la forme $\alpha + \beta i$, où α et β sont plus petits que Q. Or, les résidus de

$$\alpha', \quad 2\alpha', \quad 3\alpha', \quad \ldots, \quad (Q-1)\alpha'$$

sont, tant que α' n'est pas $= 0$, congrus dans un certain ordre, suivant le module Q, avec les nombres

$$1, \quad 2, \quad 3, \quad \ldots, \quad Q-1.$$

Dans le groupe des $Q-1$ nombres

$$\alpha' + \beta' i, \quad 2(\alpha' + \beta' i), \quad \ldots, \quad (Q-1)(\alpha' + \beta' i),$$

appartenant tous à la même classe, il y en a donc un qui est congruent avec un des nombres

$$1 + xi, \qquad x = 0, 1, 2, \ldots, Q-1.$$

Or, la quotité des nombres de chaque classe, $\frac{Q^2-1}{4} = (Q-1) \times \frac{Q+1}{4}$, est un multiple de $Q-1$, et les $Q-1$ nombres sans partie réelle

$$i, \quad 2i, \quad 3i, \quad \ldots, \quad (Q-1)i$$

appartiennent pour $Q = 8n+7$ à (A), pour $Q = 8n+3$ à (C).

Puisque tous les nombres de chaque classe dont la partie réelle n'est pas $= 0$ peuvent être réunis, comme ci-dessus, en groupes de $Q-1$ nombres, de telle sorte que dans chaque groupe il y ait *un* nombre à partie réelle $= 1$, il en résulte que, pour $Q = 8n+7$, il y a dans les classes (A), (B), (C), (D) respectivement

$$\frac{Q-3}{4}, \quad \frac{Q+1}{4}, \quad \frac{Q+1}{4}, \quad \frac{Q+1}{4}$$

nombres $1 + xi$.

Pour $Q = 8n + 3$, ces nombres sont

$$\frac{Q+1}{4}, \quad \frac{Q+1}{4}, \quad \frac{Q-3}{4}, \quad \frac{Q+1}{4};$$

tandis que, d'après le n° 18, dans le cas $a \equiv 0 \pmod{Q}$, pour $Q = 8n + 7$, et $8n + 3$, Q appartenait respectivement aux classes (A) et (C).

Tout ce qui se rapportait au cas $m = -Q$ est donc maintenant connu.

20. Pour $m = P = (A + Bi)(A - Bi)$ nous avons déjà trouvé

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{A+Bi}\right)\right)\left(\left(\frac{a+bi}{A-Bi}\right)\right),$$

et, par conséquent, lorsque $b \equiv ax \pmod{P}$;

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{1+xi}{A+Bi}\right)\right)\left(\left(\frac{1+xi}{A-Bi}\right)\right)\left(\left(\frac{a}{A+Bi}\right)\right)\left(\left(\frac{a}{A-Bi}\right)\right),$$

ou, puisque d'après une remarque déjà faite au n° 18 le produit des deux derniers facteurs à droite est $= 1$,

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{1+xi}{A+Bi}\right)\right)\left(\left(\frac{1+xi}{A-Bi}\right)\right);$$

de là résulte que la valeur du symbole à gauche dépend uniquement du nombre x, de sorte qu'il n'y a plus qu'à résoudre la question suivante : pour combien de valeurs de $1 + xi$ l'expression

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right)\left(\left(\frac{1+xi}{A-Bi}\right)\right)$$

acquiert-elle respectivement les valeurs 1, i, -1, $-i$? On doit donner ici à x les valeurs

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad P-1,$$

à l'exception des deux racines de $y^2 \equiv -1 \pmod{P}$.

Pour résoudre la question qui vient d'être posée, je considère un système complet de résidus incongrus non divisibles par le module $A + Bi$, et je les rapporte, d'après leur caractère biquadratique, à quatre groupes (A), (B), (C), (D). Chacun de ces résidus est supposé choisi de telle sorte que la partie réelle soit $= 1$, et que le facteur de i soit plus petit que P.

Ces suppositions peuvent être représentées ainsi

$$(\mathrm{mod}\ \mathrm{A}+\mathrm{B}i),\quad \mathrm{A}^2+\mathrm{B}^2=\mathrm{P}.$$

$$\begin{aligned}\text{Classe (A)}\quad &\alpha=1+ai,\\ \text{(B)}\quad &\beta=1+bi,\\ \text{(C)}\quad &\gamma=1+ci,\\ \text{(D)}\quad &\delta=1+di.\end{aligned}$$

Les nombres a, b, c, d, dans leur ensemble, concordent avec

$$0,\quad 1,\quad 2,\quad 3,\quad \ldots,\quad (\mathrm{P}-1),$$

sauf que la valeur f, qui est $\equiv i$, manque, vu que $1+fi\equiv 0\ (\mathrm{mod}\ \mathrm{A}+\mathrm{B}i)$.

En opérant de la même manière avec $\mathrm{A}-\mathrm{B}i$, on voit aisément que la classification sera

$$(\mathrm{mod}\ \mathrm{A}-\mathrm{B}i).$$

$$\begin{aligned}\text{Classe (A)}\quad &1+(\mathrm{P}-a)i,\\ \text{(B)}\quad &1+(\mathrm{P}-d)i,\\ \text{(C)}\quad &1+(\mathrm{P}-c)i,\\ \text{(D)}\quad &1+(\mathrm{P}-b)i;\end{aligned}$$

car on a simultanément

$$(1+xi)^{\frac{\mathrm{P}-1}{4}}-i^{\rho}=(\mathrm{A}+\mathrm{B}i)(\mathrm{C}+\mathrm{D}i),$$

$$(1-xi)^{\frac{\mathrm{P}-1}{4}}-i^{3\rho}=(\mathrm{A}-\mathrm{B}i)(\mathrm{C}-\mathrm{D}i).$$

Ainsi, lorsque $1+xi$ a, suivant le module $\mathrm{A}+\mathrm{B}i$, le caractère ρ, $1-xi\equiv 1+(\mathrm{P}-x)i$ a, suivant le module $\mathrm{A}-\mathrm{B}i$, le caractère 3ρ.

21. Pour que

$$\left(\left(\frac{1+xi}{\mathrm{A}+\mathrm{B}i}\right)\right)\left(\left(\frac{1+xi}{\mathrm{A}-\mathrm{B}i}\right)\right)$$

devienne égal à 1, il faut, lorsque

$$\left(\left(\frac{1+xi}{\mathrm{A}+\mathrm{B}i}\right)\right)$$

a l'une des valeurs 1, i, -1, $-i$, que

$$\left(\left(\frac{1+xi}{\mathrm{A}+\mathrm{B}i}\right)\right)$$

prenne une des valeurs 1, $-i$, -1, i; ou, en ayant égard aux deux divisions en classes : lorsque x appartient respectivement à a, b, c, d, il faut que, simultanément, $p-x$ appartienne aux nombres a, b, c, d.

On peut donc dire que le nombre des valeurs de x, pour lesquelles on a

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right)\left(\left(\frac{1+xi}{A-Bi}\right)\right)=1,$$

est égal à la somme des nombres de solutions des congruences

$$\begin{aligned} a+a' &\equiv 0,\\ b+b' &\equiv 0,\\ c+c' &\equiv 0,\\ d+d' &\equiv 0, \end{aligned}$$

par rapport au module P, ou, ce qui revient au même, par rapport au module $A \pm Bi$.

On remarquera que la valeur $p-f$, exclue pour x, entre bien dans a, b, c, d, mais ne peut néanmoins apparaître dans aucune des congruences ci-dessus, parce que cela exigerait que f se trouvât également parmi les nombres a, b, c, d, ce qui n'est pas le cas.

On a $\alpha = 1 + ai$, de sorte que les congruences en question, après multiplication par i, deviennent

$$\begin{aligned} \alpha+\alpha' &\equiv 2 \pmod{A+Bi},\\ \beta+\beta' &\equiv 2,\\ \gamma+\gamma' &\equiv 2,\\ \delta+\delta' &\equiv 2. \end{aligned}$$

Lorsque $\frac{p-1}{2}$ appartient à la classe (A), les congruences précédentes, multipliées par $\frac{p-1}{2}$, se transforment en

$$\begin{aligned} \alpha+\alpha'+1 &\equiv 0 \pmod{A+Bi},\\ \beta+\beta'+1 &\equiv 0,\\ \gamma+\gamma'+1 &\equiv 0,\\ \delta+\delta'+1 &\equiv 0, \end{aligned}$$

de sorte que la somme des nombres de solutions de ces congruences est égale au nombre des valeurs de x qui rendent

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right)\left(\left(\frac{1+xi}{A-Bi}\right)\right)$$

égal à 1.

Mais on peut se convaincre immédiatement que ce résultat reste le même lorsque $\frac{p-1}{2}$ appartient aux classes (B), (C), (D). Si, par exemple, $\frac{p-1}{2}$

appartient à (B), il suit de $\alpha + \alpha' \equiv 2$, en multipliant par $\frac{p-1}{2}$,

$$\beta + \beta' + 1 \equiv 0,$$

et de $\beta + \beta' \equiv \gamma + \gamma' \equiv \delta + \delta' \equiv 2$, respectivement

$$\gamma + \gamma' + 1 \equiv 0, \qquad \delta + \delta' + 1 \equiv 0, \qquad \alpha + \alpha' + 1 \equiv 0.$$

Si l'on désigne par t, u, v, w les nombres des valeurs de x qui rendent

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right)\left(\left(\frac{1+xi}{A-Bi}\right)\right)$$

respectivement égal à 1, i, -1, $-i$, t est donc la somme des nombres de solutions des congruences

$$\begin{aligned} &\alpha + \alpha' + 1 \equiv 0 \pmod{A+Bi},\\ &\beta + \beta' + 1 \equiv 0,\\ &\gamma + \gamma' + 1 \equiv 0,\\ &\delta + \delta' + 1 \equiv 0. \end{aligned}$$

Exactement de la même manière, on trouve que u égale la somme des nombres de solutions des congruences

$$\begin{aligned} &\alpha + \delta + 1 \equiv 0,\\ &\beta + \alpha + 1 \equiv 0,\\ &\gamma + \beta + 1 \equiv 0,\\ &\delta + \gamma + 1 \equiv 0, \end{aligned}$$

tandis que, pour v et w, on a à considérer les congruences

$$\begin{aligned} &\alpha + \gamma + 1 \equiv 0\\ &\beta + \delta + 1 \equiv 0\\ &\gamma + \alpha + 1 \equiv 0\\ &\delta + \beta + 1 \equiv 0 \end{aligned} \qquad \text{et} \qquad \begin{aligned} &\alpha + \beta + 1 \equiv 0,\\ &\beta + \gamma + 1 \equiv 0,\\ &\gamma + \delta + 1 \equiv 0,\\ &\delta + \alpha + 1 \equiv 0. \end{aligned}$$

Dans le cas de $P = 8n + 1$, on a donc, d'après les n^{os} 7 et 8,

$$\begin{aligned} t &= (0,0) + (1,1) + (2,2) + (3,3) = h + l + k + j = 2n - 1,\\ u &= (0,3) + (1,0) + (2,1) + (3,2) = j + m + m + l = 2n,\\ v &= (0,2) + (1,3) + (2,0) + (3,1) = k + m + k + m = 2n,\\ w &= (0,1) + (1,2) + (2,3) + (3,0) = l + j + m + m = 2n, \end{aligned}$$

et dans le cas de $P = 8n + 5$, d'après le n° 13,

$$t = (0,2) + (1,3) + (2,0) + (3,1) = k + j + h + l = 2n + 1,$$
$$u = (0,1) + (1,2) + (2,3) + (3,0) = j + l + m + m = 2n + 1,$$
$$v = (0,0) + (1,1) + (2,2) + (3,3) = h + m + h + m = 2n,$$
$$w = (0,3) + (1,0) + (2,1) + (3,2) = l + m + m + j = 2n + 1.$$

22. En récapitulant tout ce qui précède, on voit donc que les caractères servant à reconnaître si un nombre premier réel appartient aux classes (A), (B), (C), (D), lorsque le module p est de la forme $4n + 1$ et que $a + bi$ est un facteur complexe primaire de p, se laissent exprimer de la manière suivante :

Le nombre premier $P = 8n + 1$ appartient à

(A) pour	$a \equiv 0$,	$b \equiv a\alpha$	(mod P).	Nombre des	$\alpha' = 2n - 1$,
(B) »		$b \equiv a\beta$	»	»	$\beta' = 2n$,
(C) »		$b \equiv a\gamma$	»	»	$\gamma' = 2n$,
(D) »		$b \equiv a\delta$	»	»	$\delta' = 2n$.

Le nombre premier $P = 8n + 5$ appartient à

(A) pour		$b \equiv a\alpha$	(mod P).	Nombre des	$\alpha' = 2n + 1$,
(B) »		$b \equiv a\beta$	»	»	$\beta' = 2n + 1$,
(C) »		$b \equiv a\gamma$,	$a \equiv 0$ »	»	$\gamma' = 2n$,
(D) »		$b \equiv a\delta$	»	»	$\delta' = 2n + 1$.

Le nombre premier $-Q = -(8n + 3)$ appartient à

(A) pour		$b \equiv a\alpha$,	(mod Q).	Nombre des	$\alpha' = 2n + 1$,
(B) »		$b \equiv a\beta$	»	»	$\beta' = 2n + 1$,
(C) »		$b \equiv a\gamma$,	$a \equiv 0$ »	»	$\gamma' = 2n$,
(D) »		$b \equiv a\delta$	»	»	$\delta' = 2n + 1$.

Le nombre premier $-Q = -(8n + 7)$ appartient à

(A) pour		$b \equiv a\alpha$,	$a \equiv 0$ (mod Q).	Nombre des	$\alpha' = 2n + 1$,
(B) »		$b \equiv a\beta$	»	»	$\beta' = 2n + 1$,
(C) »		$b \equiv a\gamma$	»	»	$\gamma' = 2n + 1$,
(D) »		$b \equiv a\delta$	»	»	$\delta' = 2n + 1$.

Je citerai encore les remarques suivantes de Gauss (Art. 28), dont la démonstration, après tout ce qui précède, n'offre pas la moindre difficulté.

1° Le nombre o appartient toujours aux α, et les nombres $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ appartiennent (mod m) respectivement aux α', δ', γ' et β'.

2° Pour $P = 8n+1$, $Q = 8n+7$, les valeurs de $\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\gamma}, \frac{1}{\delta}$ (mod m) appartiennent respectivement aux α', δ', γ', β'; et pour $P = 8n+5$, $Q = 8n+3$, ces valeurs appartiennent respectivement aux γ', β', α', δ'.

Résidus cubiques.

23. En passant aux résidus cubiques, il est nécessaire de rappeler quelques points de la théorie des nombres entiers de la forme $a+b\rho$; ρ est ici une racine cubique complexe de l'unité, de sorte qu'on a

$$1+\rho+\rho^2=0.$$

Dans cette théorie, comme on le sait, il existe au sujet de la divisibilité des nombres, de leur décomposition en facteurs premiers, de l'existence de racines primitives des nombres premiers, etc., des théorèmes tout à fait analogues à ceux que présente la théorie ordinaire des nombres réels; la grande majorité des recherches contenues dans les quatre premières sections des *Disquisitiones arithmeticæ* peuvent être étendues, presque sans changement, à la théorie des nombres entiers $a+b\rho$.

Le produit de deux nombres conjugués $a+b\rho$, $a+b\rho^2$,

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

s'appelle la *norme* du nombre $a+b\rho$ et sera toujours indiqué par μ.

Le nombre 3 n'est pas un nombre premier dans cette théorie, car

$$3=(1-\rho)(1-\rho^2)=-\rho^2(1-\rho)^2,$$

Comme nombres premiers, outre $1-\rho$, se présentent dans cette théorie :

Premièrement les nombres premiers réels de la forme $3n-1$; la norme est alors $=(3n-1)^2$;

Secondement les facteurs premiers complexes des nombres premiers réels de la forme $3n+1$. Ce nombre premier réel est alors en même temps la norme du facteur premier complexe. On a, par exemple,

$$7=(2+3\rho)(2+3\rho^2)=(2+3\rho)(-1-3\rho).$$

Les nombres premiers $2+3\rho$, $-1-3\rho$ ont tous les deux le nombre 7 pour norme.

Dans chacun de ces deux cas la norme est donc de la forme $3k+1$.

Ensuite, il suffit de considérer des nombres premiers *primaires,* ce mot étant pris ici dans la signification que lui donne Eisenstein (*Journal de Crelle,* t. 27, p. 301), de sorte que $a+b\rho$ sera dit *primaire* lorsque $a+1$ et b sont tous les deux divisibles par 3. Les nombres premiers réels de la forme $3n-1$ doivent donc être pris positifs pour être primaires.

Soit donc M un nombre premier primaire, μ la norme de la forme $3n+1$. Un système complet de résidus incongrus, non divisibles par le module M, se compose alors de $\mu-1=3n$ nombres. Ces nombres peuvent être rapportés à trois classes, comprenant chacune n nombres, suivant que leur puissance $\frac{\mu-1}{3}$ est congrue, d'après le module M, avec 1, ρ ou ρ^2. Cette distribution peut être représentée ainsi

(A) $\alpha,\ \alpha',\ \alpha'',\ \ldots,$
(B) $\beta,\ \beta',\ \beta'',\ \ldots,$
(C) $\gamma,\ \gamma',\ \gamma'',\ \ldots,$

où l'on a donc

$$\alpha^{\frac{\mu-1}{3}} \equiv 1, \qquad \beta^{\frac{\mu-1}{3}} \equiv \rho, \qquad \gamma^{\frac{\mu-1}{3}} \equiv \rho^2 \pmod{\mathrm{M}}.$$

Le caractère cubique des nombres $\alpha, \alpha', \alpha'', \ldots = 0$, celui des nombres $\beta, \beta', \ldots = 1$, celui des nombres $\gamma, \gamma', \ldots = 2$.

Il sera d'ailleurs facile aussi de faire usage du symbole d'Eisenstein et d'écrire, par conséquent,

$$\left[\frac{\alpha}{\mathrm{M}}\right] = 1, \qquad \left[\frac{\beta}{\mathrm{M}}\right] = \rho, \qquad \left[\frac{\gamma}{\mathrm{M}}\right] = \rho^2.$$

Il s'agit maintenant, en premier lieu, de déterminer le caractère cubique de $1-\rho$, ou la valeur du symbole $\left[\frac{1-\rho}{\mathrm{M}}\right]$.

24. L'addition de l'unité à tous les nombres de (A), (B), (C) donne naissance aux trois groupes de nombres (A'), (B'), (C')

(A') $\alpha+1,\ \alpha'+1,\ \alpha''+1,\ \ldots,$
(B') $\beta+1,\ \beta'+1,\ \beta''+1,\ \ldots,$
(C') $\gamma+1,\ \gamma'+1,\ \gamma''+1,\ \ldots,$

et je représente par (0,0), (0,1), (0,2) les quotités des nombres de (A')

qui sont respectivement congrus avec des nombres de (A), (B), (C); par (1,0), (1,1), (1,2) les quotités des nombres de (B′) qui sont respectivement congrus avec des nombres de (A), (B), (C); enfin par (2,0), (2,1), (2,2) les quotités des nombres de (C′) qui sont respectivement congrus avec des nombres de (A), (B), (C).

Tous ces nombres peuvent être réunis dans le schéma (S)

$$\begin{array}{ccc} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,0) & (2,1) & (2,2); \end{array}$$

et avec la détermination de ces nombres est aussi trouvé immédiatement le caractère cubique de $1-\rho$. Car les congruences manifestement identiques

$$\begin{aligned} (x-\alpha)(x-\alpha')(x-\alpha'')\ldots &\equiv x^{\frac{\mu-1}{3}}-1 \qquad (\text{mod } \mathbf{M}), \\ (x-\beta)(x-\beta')(x-\beta'')\ldots &\equiv x^{\frac{\mu-1}{3}}-\rho, \\ (x-\gamma)(x-\gamma')(x-\gamma'')\ldots &\equiv x^{\frac{\mu-1}{3}}-\rho^2 \end{aligned}$$

donnent pour $x=-1$, vu que $\frac{\mu-1}{3}$ est pair (sauf pour $\mathbf{M}=2$, cas qui doit être excepté),

$$\begin{aligned} (\beta+1)(\beta'+1)(\beta''+1)\ldots &\equiv 1-\rho \qquad (\text{mod } \mathbf{M}), \\ (\gamma+1)(\gamma'+1)(\gamma''+1)\ldots &\equiv 1-\rho^2; \end{aligned}$$

d'où il suit immédiatement

$$\begin{aligned} \left[\frac{1-\rho}{\mathbf{M}}\right] &= \rho^{(1,1)+2(1,2)}, \\ \left[\frac{1-\rho^2}{\mathbf{M}}\right] &= \rho^{(2,1)+2(2,2)}. \end{aligned}$$

25. Le nombre -1 appartient, comme cube parfait, à la classe (A), et les nombres α et $-\alpha$, β et $-\beta$, γ et $-\gamma$ entrent à la fois dans les classes (A), (B), (C).

A l'aide de cette remarque, il est facile de voir que

Le signe	Représente le nombre des solutions de	
(0,0)	$\alpha+\alpha'+1\equiv 0$	(mod M),
(0,1)	$\alpha+\beta+1\equiv 0$,	
(0,2)	$\alpha+\gamma+1\equiv 0$,	
(1,0)	$\beta+\alpha+1\equiv 0$,	
(1,1)	$\beta+\beta'+1\equiv 0$,	
(1,2)	$\beta+\gamma+1\equiv 0$,	
(2,0)	$\gamma+\alpha+1\equiv 0$,	
(2,1)	$\gamma+\beta+1\equiv 0$,	
(2,2)	$\gamma+\gamma'+1\equiv 0$,	

de sorte qu'on a

$$(0,1)=(1,0), \qquad (0,2)=(2,0), \qquad (1,2)=(2,1).$$

Si $xy\equiv 1 \pmod{M}$ et que x appartienne à (A), il est évident que y appartient également à (A); mais lorsque x appartient à (B) ou à (C), y appartient respectivement à (C) ou à (B), ce qu'on peut exprimer en écrivant

$$\alpha\alpha'\equiv 1, \qquad \beta\gamma\equiv 1 \qquad (\text{mod } M).$$

De

$$\gamma(\alpha+\beta+1)\equiv\gamma'+1+\gamma,$$
$$\beta(\alpha+\gamma+1)\equiv\beta'+1+\beta$$

on conclut aux relations

$$(0,1)=(2,2), \qquad (0,2)=(1,1),$$

de sorte que le schéma (S) a cette forme

$$\begin{matrix} h & j & k, \\ j & k & l, \\ k & l & j. \end{matrix}$$

Comme -1 appartient à (A) et, par conséquent, 0 à (A'), mais que, sauf ce nombre 0 de (A'), tous les nombres de (A'), (B'), (C') sont congrus avec un nombre de (A), (B) ou (C), on a

$$h+j+k=n-1,$$
$$j+k+l=n.$$

Enfin, la considération du nombre des solutions de la congruence

$$\alpha+\beta+\gamma+1\equiv 0 \qquad (\text{mod } M),$$

où α, β, γ doivent être choisis respectivement dans les classes (A), (B), (C), fournit encore une relation entre h, j, k, l. En effet, si l'on prend d'abord pour α les nombres de (A), on obtient pour le nombre en question

$$hl+jj+kk.$$

En prenant, au contraire, pour β successivement tous les nombres de (B), on trouve pour ce même nombre

$$jk+kl+lj,$$

donc

$$0=hl+jj+kk-jk-kl-lj.$$

26. En éliminant h de cette dernière équation, à l'aide de $h=l-1$, on a

$$0=l(l-1)+jj+kk-jk-kl-lj,$$

équation qui, multipliée par 4, prend, à cause de

$$(j+k)^2+3(j-k)^2=4(jj+kk-jk),$$

la forme

$$0=4l^2-4l+(j+k)^2+3(j-k)^2-4l(k+j),$$

ou bien, en ayant égard à $l=n-(j+k)$ et en multipliant par 9,

$$36n=36l^2+9(j+k)^2+27(j-k)^2-36l(j+k)+36(j+k),$$

et

$$24n=24(j+k+l);$$

donc, par soustraction,

$$12n=36l^2+9(j+k)^2+27(j-k)^2-36l(j+k)+12(j+k)-24l,$$

ou

$$12n+4=4\mu=(6l-3j-3k-2)^2+27(j-k)^2.$$

Si l'on pose

$$\mathrm{A}=6l-3j-3k-2,$$
$$\mathrm{B}=3j-3k,$$

on a donc

$$4\mu=\mathrm{A}^2+3\mathrm{B}^2,$$

et h, j, k, l se laissent alors facilement exprimer au moyen de A et B, de la manière suivante

$$9h=3n+\mathrm{A}-7,$$
$$18j=6n-\mathrm{A}+3\mathrm{B}-2,$$
$$18k=6n-\mathrm{A}-3\mathrm{B}-2,$$
$$9l=3n+\mathrm{A}+2.$$

Il reste encore à déterminer A et B, et pour cela deux cas doivent être distingués.

27. Si, en premier lieu, M est réel et de la forme $3n-1$, donc $\mu = M^2$, il suit de

$$4\mu = 4M^2 = A^2 + 3B^2$$

que $A = \pm 2M$, $B = 0$. Car, si B n'était pas égal à 0, on pourrait déterminer un nombre entier x de telle sorte que

$$A \equiv Bx \pmod{M},$$

d'où résulterait

$$A^2 \equiv -3B^2 \equiv B^2x^2 \pmod{M},$$

donc

$$x^2 \equiv -3 \pmod{M},$$

ce qui est impossible, puisqu'on sait que -3 est non-résidu de M.

On a donc indubitablement

$$B = 0, \qquad A = \pm 2M.$$

Quant au signe de A, il se déduit immédiatement de la remarque que A est $\equiv 1 \pmod 3$, et M, comme nombre premier *primaire*, $\equiv -1 \pmod 3$; on a donc

$$A = 2M$$

et finalement

$$\begin{aligned} 9h &= 3n + 2M - 7, \\ 9j = 9k &= 3n - M - 1, \\ 9l &= 3n + 2M + 2. \end{aligned}$$

28. Soit, en second lieu, $M = a + b\rho$ un facteur complexe primaire d'un nombre premier réel p de la forme $3n+1$; on a alors

$$4\mu = (2a-b)^2 + 3b^2 = A^2 + 3B^2$$

et, puisque $a + b\rho$ est primaire, $a + 1 \equiv b \equiv 0 \pmod 3$.

B aussi est maintenant divisible par 3, et comme il est facile de démontrer que 4μ ne peut être représenté que d'une seule manière par la somme d'un carré et du multiple par 27 d'un second carré, il s'ensuit

$$A = 2a - b, \qquad B = \pm b.$$

Le signe de A, en effet, est de nouveau déterminé par $A \equiv 1 \pmod 3$.

Quant au signe de B, il s'obtient par la considération suivante : Si z parcourt tous les nombres de (A), (B) et (C), on trouve, exactement de

la même manière qu'au n° 12,

$$\Sigma(z^3+1)^{\frac{\mu-1}{3}} \equiv -2 \equiv 3(h+j\rho+k\rho^2) \qquad (\mathrm{mod}\,\mathrm{M}),$$

ou

$$-2 \equiv 3[(h-k)+\rho(j-k)],$$

puis, en exprimant h, j, k par A et B, et écrivant pour A la valeur $2a-b$, après quelques réductions,

$$0 \equiv 2a-b+\mathrm{B}+2\mathrm{B}\rho \qquad [\mathrm{mod}\,(\mathrm{M}=a+b\rho)],$$

d'où il résulte $\mathrm{B}=b$.

A et B étant ainsi trouvés, on a

$$\begin{aligned} 9h &= 3n+2a-b-7,\\ 9j &= 3n-a+2b-1,\\ 9k &= 3n-a-b-1,\\ 9l &= 3n+2a-b+2. \end{aligned}$$

29. D'après le n° 24, le caractère cubique de $1-\rho$, suivant le module 3, est

$$\equiv (1,1)+2(1,2) \equiv k-l,$$

et celui de $1-\rho^2$

$$\equiv (2,1)+2(2,2) \equiv l-j;$$

lorsque M est réel de la forme $3n-1$, on a donc, d'après le n° 27,

$$\text{Caractère } (1-\rho) \equiv -\frac{\mathrm{M}+1}{3},$$

$$\text{» } \qquad (1-\rho^2) \equiv +\frac{\mathrm{M}+1}{3},$$

ou bien

$$\left[\frac{1-\rho}{\mathrm{M}}\right] = \rho^{-\frac{\mathrm{M}+1}{3}}, \qquad \left[\frac{1-\rho^2}{\mathrm{M}}\right] = \rho^{+\frac{\mathrm{M}+1}{3}};$$

d'où il suit encore

$$\left[\frac{3}{\mathrm{M}}\right] = 1.$$

Quand, au contraire, $\mathrm{M}=a+b\rho$ est un facteur complexe d'un nombre premier réel de la forme $3n+1$, on a, d'après les valeurs trouvées au n° 28,

$$\text{Caractère } (1-\rho) \equiv \frac{1}{3}(-a-1),$$

$$\text{» } \qquad (1-\rho^2) \equiv \frac{1}{3}(a-b+1),$$

ou

$$\left[\frac{1-\rho}{a+b\rho}\right]=\rho^{-\frac{a+1}{3}},\qquad \left[\frac{1-\rho^2}{a+b\rho}\right]=\rho^{\frac{a-b+1}{3}},\qquad \left[\frac{3}{a+b\rho}\right]=\rho^{-\frac{1}{3}b}.$$

Ces résultats ne diffèrent pas, au fond, de ceux donnés par Eisenstein dans le *Journal de Crelle*, t. 28, p. 28 et suivantes.

30. A l'égard du cas où le nombre premier M est un facteur d'un nombre premier réel p, de la forme $3n+1$, je présenterai encore les remarques suivantes.

Comme, dans $M=a+b\rho$, a et b n'ont pas de diviseur commun, et que par conséquent b et $a-b$ sont aussi premiers entre eux, on peut toujours trouver deux nombres entiers α et β satisfaisant à la relation

$$b\alpha+(a-b)\beta=1,$$

et l'on a alors

$$(a+b\rho)(\alpha+\beta\rho)=a\alpha-b\beta+\rho,$$

donc

$$\rho\equiv b\beta-a\alpha \qquad [\mathrm{mod}(M=a+b\rho)].$$

De là résulte immédiatement que tout nombre entier $c+d\rho$ est congru suivant le module $a+b\rho$ à un nombre entier réel, lequel nombre réel peut être pris plus petit que le module $\mu=p$, de sorte que les nombres réels

$$0,\quad 1,\quad 2,\quad 3,\quad \ldots,\quad \mu-1$$

forment un système complet de résidus. En divisant ces nombres réels (à l'exception de 0), suivant leur caractère cubique, en trois classes

(A) $\alpha,\ \alpha',\ \alpha'',\ \ldots,$
(B) $\beta,\ \beta',\ \beta'',\ \ldots,$
(C) $\gamma,\ \gamma',\ \gamma'',\ \ldots,$

et, en désignant par f le nombre réel qui est $\equiv\rho\,(\mathrm{mod}\,M)$, on a donc

$$\alpha^{\frac{\mu-1}{3}}-1\equiv\beta^{\frac{\mu-1}{3}}-f\equiv\gamma^{\frac{\mu-1}{3}}-f^2\equiv 0 \qquad [\mathrm{mod}(M=a+b\rho)],$$

et comme

$$\alpha^{\frac{\mu-1}{3}}-1,\quad \beta^{\frac{\mu-1}{3}}-f,\quad \gamma^{\frac{\mu-1}{3}}-f^2$$

sont des nombres réels, ils doivent être divisibles non seulement par $a+b\rho$,

mais aussi par le module

$$p = \mu = (a + b\rho)(a + b\rho^2),$$

de sorte qu'on a

$$\alpha^{\frac{\mu-1}{3}} \equiv 1 \qquad [\mathrm{mod}(p = \mu)],$$
$$\beta^{\frac{\mu-1}{3}} \equiv f,$$
$$\gamma^{\frac{\mu-1}{3}} \equiv f^2.$$

On voit donc que la classification des nombres

$$1, \quad 2, \quad 3, \quad \ldots, \quad p-1,$$

à l'aide de ces trois congruences, coïncide avec celle qui a pour base leur caractère cubique par rapport au module $a + b\rho$.

Le résultat

$$\left[\frac{3}{a + b\rho}\right] = \rho^{-\frac{1}{3}b}$$

peut être énoncé ainsi : le nombre 3 appartient à la classe (A), (B) ou (C), suivant que $-\frac{1}{3}b$ est de la forme $3m$, $3m+1$ ou $3m+2$.

Voici quelques exemples :

		Schéma (S).	
	$p = 7, \quad a = 2, \quad b = 3, \quad f = 4.$		
(A)	1, 6.	$h\ j\ k$	0 1 0
(B)	2, 5.	$j\ k\ l$	1 0 1
(C)	3, 4.	$k\ l\ j$	0 1 1
	$p = 13, \quad a = -1, \quad b = 3, \quad f = 9.$		
(A)	1, 5, 8, 12.		0 2 1
(B)	4, 6, 7, 9.		2 1 1
(C)	2, 3, 10, 11.		1 1 2
	$p = 19, \quad a = 5, \quad b = 3, \quad f = 11.$		
(A)	1, 7, 8, 11, 12, 18.		2 2 1
(B)	4, 6, 9, 10, 13, 15.		2 1 3
(C)	2, 3, 5, 14, 16, 17.		1 3 2
	$p = 31, \quad a = 5, \quad b = 6, \quad f = 25.$		
(A)	1, 2, 4, 8, 15, 16, 23, 27, 29, 30.		3 4 2
(B)	3, 6, 7, 12, 14, 17, 19, 24, 25, 28.		4 2 4
(C)	5, 9, 10, 11, 13, 18, 20, 21, 22, 26.		2 4 4

$p = 37, \quad a = -4, \quad b = 3, \quad f = 26.$

(A)	1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36.	2 5 4
(B)	2, 9, 12, 15, 16, 17, 20, 21, 22, 25, 28, 35.	5 4 3
(C)	3, 4, 5, 7, 13, 18, 19, 24, 30, 32, 33, 34.	4 3 5

$p = 43, \quad a = -1, \quad b = 6, \quad f = 36.$

(A)	1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42.	3 6 4
(B)	3, 5, 6, 10, 12, 19, 20, 23, 24, 31, 33, 37, 38, 40.	6 4 4
(C)	7, 9, 13, 14, 15, 17, 18, 25, 26, 28, 29, 30, 34, 36.	4 4 6

$p = 61, \quad a = 5, \quad b = 9, \quad f = 13.$

(A)	1, 3, 8, 9, 11, 20, 23, 24, 27, 28, 33, 34, 37, 38, 41, 50, 52, 53, 58, 60.	6 8 5 8 5 7
(B)	4, 10, 12, 14, 17, 19, 25, 26, 29, 30, 31, 32, 35, 36, 42, 44, 47, 49, 51, 57.	5 7 8
(C)	2, 5, 6, 7, 13, 15, 16, 18, 21, 22, 39, 40, 43, 45, 46, 48, 54, 55, 56, 59.	

La question de la présence du nombre 3 dans l'un des groupes (A), (B), (C) étant tranchée d'avance, comme il vient d'être dit, on peut facilement, à l'aide de la loi de réciprocité dans la théorie des résidus cubiques, établir les caractères nécessaires pour reconnaître aussi la présence d'autres nombres dans ces classes. Il suffit évidemment de considérer, à ce point de vue, les nombres premiers.

En ce qui concerne le nombre premier 2, ces caractères peuvent aussi être déduits sans le secours de la loi de réciprocité, ainsi que nous allons le faire voir.

31. Le nombre $p - 1$ appartenant toujours à (A), il en résulte immédiatement que 2 appartiendra à la classe (A), (B) ou (C) suivant que $\frac{p-1}{2}$ appartient à la classe (A), (C) ou (B).

Les nombres h, k, j sont respectivement les nombres de solutions des congruences

$$\alpha + \alpha' + 1 \equiv 0 \pmod{p},$$
$$\beta + \beta' + 1 \equiv 0,$$
$$\gamma + \gamma' + 1 \equiv 0,$$

et comme on peut échanger entre eux α et α', β et β', γ et γ', ces trois nombres sont pairs, à l'exception du premier, lorsque $\alpha = \alpha' = \frac{p-1}{2}$ appartient à (A), ou à l'exception du deuxième, lorsque $\beta = \beta' = \frac{p-1}{2}$ appartient à (B), ou à l'exception du troisième, lorsque $\gamma = \gamma' = \frac{p-1}{2}$ appartient à (C).

On voit donc que 2 appartient à la classe (A), (B) ou (C), suivant que, des trois nombres h, j, k, le premier, le deuxième ou le troisième est impair.

Comme on a $p = 3n + 1$ (n pair) et, d'après le n° 28,

$$\begin{aligned} 9h &= 3n + 2a - b - 7, \\ 9j &= 3n - a + 2b - 1, \\ 9k &= 3n - a - b - 1, \end{aligned}$$

h est impair lorsque b est pair, j est impair lorsque a est pair, enfin k est impair lorsque a et b sont tous les deux impairs. Puisque a et b n'ont pas de diviseur commun, aucun autre cas n'est possible, et, par conséquent, 2 appartient à

$$\begin{aligned} &(\mathrm{A}) \text{ lorsque } b \equiv 0 \pmod 2, \\ &(\mathrm{B}) \quad \text{»} \quad a \equiv 0 \pmod 2, \\ &(\mathrm{C}) \quad \text{»} \quad a \equiv b \equiv 1 \pmod 2. \end{aligned}$$

32. En ce qui regarde la présence de 5 dans l'une des trois classes, on a, d'après la loi de réciprocité cubique,

$$\left[\frac{5}{a+b\rho}\right] = \left[\frac{a+b\rho}{5}\right],$$

car 5 est aussi un nombre premier dans la théorie des nombres entiers $a + b\rho$.

Pour $a \equiv 0 \pmod 5$, on a donc

$$\left[\frac{5}{a+b\rho}\right] = \left[\frac{b\rho}{5}\right] = \left[\frac{\rho}{5}\right] = \rho^8 = \rho^2,$$

et, par conséquent, 5 appartient à (C).

Lorsque a n'est pas divisible par 5, on peut déterminer x par

$$b \equiv ax \pmod 5,$$

et x peut prendre les valeurs 0, 1, 2, 3, 4; on a

$$\left[\frac{5}{a+b\rho}\right]=\left[\frac{a(1+x\rho)}{5}\right]=\left[\frac{1+x\rho}{5}\right],$$

et l'on trouve ensuite

$$x=0, \qquad \left[\frac{5}{a+b\rho}\right]=1,$$
$$x=1, \qquad \left[\frac{5}{a+b\rho}\right]=\rho,$$
$$x=2, \qquad \left[\frac{5}{a+b\rho}\right]=1,$$
$$x=3, \qquad \left[\frac{5}{a+b\rho}\right]=\rho^2,$$
$$x=4, \qquad \left[\frac{5}{a+b\rho}\right]=\rho,$$

de sorte que 5 appartient à

(A) lorsque $b\equiv 0, \quad b\equiv 2a \pmod 5$,
(B) » $b\equiv a, \quad b\equiv 4a$,
(C) » $b\equiv 3a, \quad a\equiv 0$.

Pour juger de la classe de 7, on a

$$\left[\frac{a+b\rho}{7}\right]=\left[\frac{2+3\rho}{a+b\rho}\right]\left[\frac{2+3\rho^2}{a+b\rho}\right],$$

puis, d'après la loi de réciprocité,

$$\left[\frac{7}{a+b\rho}\right]=\left[\frac{a+b\rho}{2+3\rho}\right]\left[\frac{a+b\rho}{2+3\rho^2}\right].$$

Pour $a\equiv 0 \pmod 7$, attendu qu'on a, en général,

$$\left[\frac{\alpha+\beta\rho}{a+b\rho}\right]\left[\frac{\alpha+\beta\rho^2}{a+b\rho^2}\right]=1,$$

il vient

$$\left[\frac{7}{a+b\rho}\right]=\left[\frac{\rho}{2+3\rho}\right]\left[\frac{\rho}{2+3\rho^2}\right]=\left[\frac{2+3\rho}{\rho^2}\right]=\rho^4=\rho,$$

de sorte que 7 appartient à (B).

Lorsque a n'est pas divisible par 7, mais qu'on a

$$b\equiv ax \pmod 7,$$

il s'ensuit

$$\left[\frac{7}{a+b\rho}\right]=\left[\frac{1+x\rho}{2+3\rho}\right]\left[\frac{1+x\rho}{2+3\rho^2}\right],$$

et x peut présenter les valeurs

0, 1, 2, 4, 6,

mais non les valeurs $x = 3$ et $x = 5$, car celles-ci rendraient

$$p = a^2 - ab + b^2 \equiv a^2(1 - x + x^2)$$

divisible par 7.

On trouve maintenant

$$x = 0, \quad \left[\frac{7}{a + b\rho}\right] = 1,$$
$$x = 1, \quad \left[\frac{7}{a + b\rho}\right] = \rho^2,$$
$$x = 2, \quad \left[\frac{7}{a + b\rho}\right] = 1,$$
$$x = 4, \quad \left[\frac{7}{a + b\rho}\right] = \rho,$$
$$x = 6, \quad \left[\frac{7}{a + b\rho}\right] = \rho^2,$$

de sorte que 7 appartient à

(A) lorsque $b \equiv 0$, $b \equiv 2a$ (mod 7),
(B) » $b \equiv 4a$, $a \equiv 0$,
(C) » $b \equiv a$, $b \equiv 6a$,

De la même manière, ou par induction, on reconnaîtra que 11 appartient à

(A) pour $b \equiv 0$, $b \equiv 2a$, $b \equiv 4a$, $b \equiv 5a$, (mod 11);
(B) » $b \equiv 3a$, $b \equiv 6a$, $b \equiv 9a$, $a \equiv 0$,
(C) » $b \equiv a$, $b \equiv 7a$, $b \equiv 8a$, $b \equiv 10a$,

13 appartient à

(A) pour $b \equiv 0$, $b \equiv 2a$, $b \equiv 3a$, $b \equiv 8a$ (mod 13);
(B) » $b \equiv a$, $b \equiv 6a$, $b \equiv 11a$, $b \equiv 12a$,
(C) » $b \equiv 5a$, $b \equiv 7a$, $b \equiv 9a$, $a \equiv 0$,

17 appartient à

(A) pour $b \equiv 0$, $b \equiv a$, $b \equiv 2a$, $b \equiv 9a$, $b \equiv 16a$, $a \equiv 0$ (mod 17);
(B) » $b \equiv 3a$, $b \equiv 7a$, $b \equiv 8a$, $b \equiv 12a$, $b \equiv 13a$, $b \equiv 14a$,
(C) » $b \equiv 4a$, $b \equiv 5a$, $b \equiv 6a$, $b \equiv 10a$, $b \equiv 11a$, $b \equiv 15a$,

19 appartient à

(A) pour $b \equiv 0$, $b \equiv a$, $b \equiv 2a$, $b \equiv 10a$, $b \equiv 18a$, $a \equiv 0$ (mod 19);
(B) » $b \equiv 5a$, $b \equiv 11a$, $b \equiv 13a$, $b \equiv 14a$, $b \equiv 16a$, $b \equiv 17a$,
(C) » $b \equiv 3a$, $b \equiv 4a$, $b \equiv 6a$, $b \equiv 7a$, $b \equiv 9a$, $b \equiv 15a$,

23 appartient à

(A) pour $b \equiv 0$ $b \equiv 2a$, $b \equiv 5a$, $b \equiv 6a$, $b \equiv 7a$, $b \equiv 8a$, $b \equiv 11a$, $b \equiv 15a$ (mod 23);
(B) » $b \equiv a$, $b \equiv 9a$, $b \equiv 13a$, $b \equiv 16a$, $b \equiv 17a$, $b \equiv 18a$, $b \equiv 19a$, $b \equiv 22a$,
(C) » $b \equiv 3a$, $b \equiv 4a$, $b \equiv 10a$, $b \equiv 12a$, $b \equiv 14a$, $b \equiv$ $b \equiv 21a$, $a \equiv 0$.

33. La considération de ces théorèmes particuliers donne lieu aux remarques suivantes :

Pour la commodité, les nombres premiers réels de la forme $3n - 1$, qui restent aussi nombres premiers dans la théorie complexe, seront désignés ici par Q, les nombres premiers de la forme $3n + 1$ par P.

1° Un nombre premier Q appartient, lorsque $a \equiv 0 \pmod{Q}$, aux classes (A), (B), (C) suivant que $\frac{Q+1}{3}$ est de la forme $3m$, $3m+1$, $3m+2$.

2° Un nombre premier P appartient, lorsque $a \equiv 0 \pmod{P}$ aux classes (A), (B), (C) suivant que $\frac{P-1}{6}$ est de la forme $3m$, $3m+1$, $3m+2$.

3° Dans les cas $b \equiv 0$, $b \equiv 2a$, le nombre premier P ou Q appartient toujours à la classe (A).

4° Quand le nombre premier appartient à (A) pour $a \equiv 0$, il appartient aussi à (A) pour $b \equiv a$ et pour $b \equiv -a$. Si, au contraire, le nombre premier fait partie de la classe (B) ou (C) lorsque $a \equiv 0$, il fait partie, pour $b \equiv a$ et $b \equiv -a$, de la classe (C) ou (B).

5° En général, les critères sont de la forme suivante :

Si a est $\equiv 0$, le nombre premier appartient à une classe déterminée.

Si a n'est pas $\equiv 0$, on a $b \equiv ax$, et pour chaque valeur de x le nombre premier appartient à une classe déterminée, de sorte qu'on peut distribuer les valeurs de x en trois groupes, tels que

pour	$b \equiv a\alpha$,	le nombre premier appartienne à (A),
»	$b \equiv a\beta$,	» (B),
»	$b \equiv a\gamma$,	» (C).

Il faut encore ajouter le cas $a \equiv 0$, qui correspond aussi à une classe déterminée.

Or, le nombre total des congruences qu'on trouve de cette manière est le même pour chacune des trois classes et $= \frac{Q+1}{3}$ ou $= \frac{P-1}{3}$.

6° Lorsque x et y sont deux nombres satisfaisant à la congruence

$$x + y - xy \equiv 0,$$

et que x appartient aux α, y appartient également aux α. Mais si $x = \beta$ ou $x = \gamma$, y appartient respectivement aux γ ou aux β.

Si $xy \equiv 1$ et que 1 appartienne aux α, on a

$$\begin{aligned} &\text{pour } x = \alpha', \quad y = \alpha'', \\ &\text{» } x = \beta', \quad y = \gamma', \\ &\text{» } x = \gamma', \quad y = \beta'. \end{aligned}$$

Si $xy \equiv 1$ et $1 = \beta$, on a

$$\begin{aligned} &\text{pour } x = \alpha, \quad y = \gamma, \\ &\text{» } x = \beta', \quad y = \beta'', \\ &\text{» } x = \gamma', \quad y = \alpha'. \end{aligned}$$

Si $xy \equiv 1$ et $1 = \gamma$, on a

$$\begin{aligned} &\text{pour } x = \alpha, \quad y = \beta, \\ &\text{» } x = \beta, \quad y = \alpha, \\ &\text{» } x = \gamma, \quad y = \gamma'. \end{aligned}$$

34. Quant à la *démonstration* de ce qui vient d'être dit, la remarque 5° est la seule qui demande quelques considérations nouvelles; tout le reste n'offre, après ce qui précède, aucune difficulté.

Je vais donc prouver, d'une manière générale, la vérité de cette remarque 5°. Il faut pour cela distinguer les cas où le nombre premier est égal à Q ou à P; commençons par le premier de ces cas, qui est de beaucoup le plus simple.

35. Lorsque le nombre premier Q est de la forme $3n-1$, et qu'il reste, par conséquent, premier aussi dans la théorie des nombres complexes de la forme $a + b\rho$, on a, d'après la loi de réciprocité,

$$\left[\frac{Q}{a+b\rho}\right] = \left[\frac{a+b\rho}{Q}\right].$$

Soit d'abord $a \equiv 0 \pmod{Q}$; dans ce cas

$$\left[\frac{Q}{a+b\rho}\right] = \left[\frac{b\rho}{Q}\right] = \left[\frac{\rho}{Q}\right] = \rho^{\frac{Q^2-1}{3}}.$$

Mais

$$\frac{Q+1}{3} \times (Q-2)$$

est un multiple de 3, et

$$\frac{Q^2-1}{3} - \frac{(Q+1)(Q-2)}{3} = \frac{Q+1}{3};$$

on a, par conséquent

$$\text{Pour } a \equiv 0 \pmod{Q}, \qquad \left[\frac{a+b\rho}{Q}\right] = \rho^{\frac{Q+1}{3}},$$

d'où ressort l'exactitude de ce qui a été dit au n° 33 (1°).

Si a n'est pas divisible par Q, x est complètement déterminé par

$$b \equiv a.x \pmod{Q},$$

et

$$\left[\frac{Q}{a+b\rho}\right] = \left[\frac{a(1+x\rho)}{Q}\right] = \left[\frac{1+x\rho}{Q}\right],$$

ce qui montre déjà que la classe à laquelle appartient Q dépend uniquement de x; pour x on peut d'ailleurs avoir évidemment les nombres

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad Q-1.$$

Il ne reste plus qu'à résoudre cette question : parmi les Q quantités

$$\left[\frac{1+x\rho}{Q}\right], \qquad x = 0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad Q-1,$$

combien y en a-t-il d'égales à 1, combien d'égales à ρ, combien d'égales à ρ^2? Nous considérons un système complet de nombres non divisibles par le module, système pour lequel on peut prendre les nombres

$$\alpha+\beta\rho, \qquad \frac{\alpha}{\beta} = 0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad Q-1,$$

la combinaison $\alpha = 0$, $\beta = 0$ devant seule être omise. Si nous rapportons ces Q^2-1 nombres d'après leur caractère cubique à trois groupes (A), (B), (C)

(A) $\alpha_0+\beta_0\rho, \quad \ldots,$
(B) $\alpha_1+\beta_1\rho, \quad \ldots,$
(C) $\alpha_2+\beta_2\rho, \quad \ldots,$

chacun de ces groupes contient

$$\frac{Q^2-1}{3} = (Q-1) \times \frac{Q+1}{3}$$

nombres, quotité qui est donc un multiple de $Q-1$: et les nombres réels qui correspondent à $\beta = 0$, savoir

$$1, \quad 2, \quad 3, \quad \ldots, \quad Q-$$

appartiennent tous à (A), d'où il découle que lorsque $\alpha+\beta\rho$ fait partie d'une certaine classe, les nombres congrus à

$$1(\alpha+\beta\rho),\quad 2(\alpha+\beta\rho),\quad \ldots,\quad (Q-1)(\alpha+\beta\rho)$$

font aussi partie de cette classe. Si α n'est pas égal à 0, les nombres

$$\alpha,\quad 2\alpha,\quad 3\alpha,\quad \ldots,\quad (Q-1)\alpha,$$

pris dans un certain ordre, sont congrus, suivant le module Q, à

$$1,\quad 2,\quad 3,\quad \ldots,\quad Q-1.$$

Les nombres d'une classe, dont la partie réelle n'est pas égale à 0, peuvent donc être divisés en groupes de $Q-1$ nombres, de telle sorte que dans chaque groupe se trouve *un* nombre de la forme $1+x\rho$.

Il ressort de là que les quotités des nombres $1+x\rho$, qui rendent $\left[\frac{1+x\rho}{Q}\right]=1$, égal à ρ, et à ρ^2, sont

$$\begin{array}{llll}
\frac{Q-2}{3},\ \frac{Q+1}{3},\ \frac{Q+1}{3} & \text{lorsque} & \left[\frac{\rho}{Q}\right]=1,\\
\frac{Q+1}{3},\ \frac{Q-2}{3},\ \frac{Q+1}{3} & \text{»} & \left[\frac{\rho}{Q}\right]=\rho,\\
\frac{Q+1}{3},\ \frac{Q+1}{2},\ \frac{Q-2}{3} & \text{»} & \left[\frac{\rho}{Q}\right]=\rho^2,
\end{array}$$

et comme, en outre, nous avons trouvé ci-dessus que, pour

$$a\equiv 0 \pmod{Q},$$

Q appartient aux classes (A), (B) ou (C) suivant que $\left[\frac{\rho}{Q}\right]$ est égal à 1, à ρ ou à ρ^2, l'énoncé 5° du n° 33 se trouve entièrement démontré pour le cas où le nombre premier est de la forme $3n-1$.

36. Lorsque le nombre premier dont on veut reconnaître la présence dans les classes (A), (B), (C) est de la forme $P=3n+1$, il s'agit de déterminer la valeur de

$$\left[\frac{P}{a+b\rho}\right];$$

P n'étant pas un nombre premier dans la théorie complexe, on doit, avant de pouvoir appliquer la loi de réciprocité, décomposer P en ses facteurs.

premiers primaires

$$P = (A + B\rho)(A + B\rho^2),$$

et l'on a alors

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{A+B\rho}{a+b\rho}\right]\left[\frac{A+B\rho^2}{a+b\rho}\right].$$

Donc :

Pour $a \equiv 0 \pmod P$

$$\left[\frac{a+b\rho}{P}\right] = \left[\frac{\rho}{A+B\rho}\right]\left[\frac{\rho}{A+B\rho^2}\right] = \rho^{2\frac{P-1}{3}} = \rho^{\frac{P-1}{6}};$$

Pour $ax \equiv b \pmod P$

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{1+x\rho}{A+B\rho}\right]\left[\frac{1+x\rho}{A+B\rho^2}\right].$$

Du premier résultat, pour $a \equiv 0$, ressort la justesse de la seconde remarque du n° 33.

Comme P est de la forme $3n+1$, la congruence

$$x^3 \equiv 1 \pmod P$$

a trois racines différentes, 1, f, g (où $f \equiv g^2$).

Les deux valeurs $-f$, $-g$ ne peuvent maintenant être égales à x dans la congruence

$$b \equiv ax,$$

car de $b \equiv -af$ il résulterait

$$a^2 - ab + b^2 \equiv a^2(1 + f + f^2) \equiv 0 \pmod P,$$

de sorte que le nombre premier

$$p = a^2 - ab + b^2$$

serait divisible par P.

D'après cela, les valeurs que x peut prendre sont

$$0,\ 1,\ 2,\ 3,\ \ldots,\ P-1,$$

sauf omission des nombres $P - f$ et $P - g$. Leur nombre est donc $P - 2$, et il s'agit de rechercher pour combien de ces $P - 2$ valeurs de x l'expression

$$\left[\frac{1+x\rho}{A+B\rho}\right]\left[\frac{1+x\rho}{A+B\rho^2}\right]$$

acquiert les valeurs 1, ρ et ρ^2.

Je fais remarquer encore que

$$\left[\frac{\rho}{A+B\rho}\right]=\rho^{\frac{P-1}{3}}$$

et que, pour $a\equiv 0 \pmod P$, on avait

$$\left[\frac{P}{a+b\rho}\right]=\rho^{2\frac{P-1}{3}}.$$

Ainsi, lorsque ρ, pour le module $A+B\rho$, appartient à la classe (A), (B) ou (C), il arrive simultanément que P, pour le module $a+b\rho$ (ou, ce qui est la même chose, pour le module réel p), appartient à la classe (A), (C) ou (B).

37. Un nombre arbitraire $\alpha+\beta\rho$ étant donné, on peut toujours trouver un autre nombre qui soit congru avec lui suivant le module $A+B\rho$ et dont la partie réelle soit égale à 1.

La division d'un système complet de nombres non divisibles par le module, en trois classes, d'après leur caractère cubique, peut donc être représentée de cette manière :

$$(\mathrm{mod}\, A+B\rho),$$

(A)	$\alpha=1+a\rho,$	$\alpha'=1+a'\rho,$	$\alpha''=1+a''\rho,$	$\ldots,$
(B)	$\beta=1+b\rho,$	$\beta'=1+b'\rho,$	$\beta''=1+b''\rho,$	$\ldots,$
(C)	$\gamma=1+c\rho,$	$\gamma'=1+c'\rho,$	$\gamma''=1+c''\rho,$	$\ldots,$

et comme, de

$$(1+a\rho)^{\frac{P-1}{3}}-\rho^k\equiv(A+B\rho)(C+D\rho),$$

il suit

$$(1+a\rho^2)^{\frac{P-1}{3}}-\rho^{2k}\equiv(A+B\rho^2)(C+D\rho^2),$$

la classification pour le module $A+B\rho^2$ peut simultanément être représentée de cette manière :

$$(\mathrm{mod}\, A+B\rho^2),$$

(A)	$1+a\rho^2,$	$1+a'\rho^2,$	$1+a''\rho^2,$	$\ldots,$
(B)	$1+c\rho^2,$	$1+c'\rho^2,$	$1+c''\rho^2,$	$\ldots,$
(C)	$1+b\rho^2,$	$1+b'\rho^2,$	$1+b''\rho^2,$	$\ldots.$

Les nombres $a, b, c, a', b', c', a'', b'', c'', \ldots$ forment, dans leur ensemble,

tous les nombres du groupe

$$0,\ 1,\ 2,\ 3,\ \ldots,\ P-1,$$

à l'exception du seul nombre qui est $\equiv -\rho^2 \pmod{A+B\rho}$ et qui est congru suivant le module P avec un des nombres $-f$, $-g$. Les cas où l'on a

$$\left[\frac{1+x\rho}{A+B\rho}\right]\left[\frac{1+x\rho}{A+B\rho^2}\right]=1$$

sont évidemment

$$\left[\frac{1+x\rho}{A+B\rho}\right]=1 \qquad \text{et simultanément} \qquad \left[\frac{1+x\rho}{A+B\rho^2}\right]=1,$$

$$\left[\frac{1+x\rho}{A+B\rho}\right]=\rho \qquad\qquad\qquad \left[\frac{1+x\rho}{A+B\rho^2}\right]=\rho^2,$$

$$\left[\frac{1+x\rho}{A+B\rho}\right]=\rho^2 \qquad\qquad\qquad \left[\frac{1+x\rho}{A+B\rho^2}\right]=\rho.$$

Or, $\left[\frac{1+x\rho}{A+B\rho}\right]$ est égal à 1 pour $x=a, a', a'', \ldots$, et pour qu'on ait en même temps $\left[\frac{1+x\rho}{A+B\rho^2}\right]=1$, il faut donc que $1+a\rho$ soit congru suivant le module $A+B\rho^2$ avec un des nombres $1+a\rho^2$, $1+a'\rho^2$, ..., c'est-à-dire

$$1+a\rho \equiv 1+a'\rho^2 \pmod{A+B\rho^2};$$

réciproquement, si l'on a satisfait à cette congruence, on a

$$\left[\frac{1+a\rho}{A+B\rho}\right]=1, \qquad \left[\frac{1+a\rho}{A+B\rho^2}\right]=1.$$

Le nombre de fois où ce cas se présente est donc égal au nombre des solutions de la congruence ci-dessus. En raisonnant d'une manière analogue pour les deux autres cas

$$\left[\frac{1+x\rho}{A+B\rho}\right]=\rho, \qquad \left[\frac{1+x\rho}{A+B\rho^2}\right]=\rho^2$$

et

$$\left[\frac{1+x\rho}{A+B\rho}\right]=\rho^2, \qquad \left[\frac{1+x\rho}{A+B\rho^2}\right]=\rho,$$

on trouve que le nombre de fois où

$$\left[\frac{1+x\rho}{A+B\rho}\right]\left[\frac{1+x\rho}{A+B\rho^2}\right]$$

devient égal à 1, est représenté par la somme des nombres de solutions des congruences

$$\begin{aligned} 1 + a\rho &\equiv 1 + a'\rho^2 \pmod{A + B\rho^2}, \\ 1 + b\rho &\equiv 1 + b'\rho^2, \\ 1 + c\rho &\equiv 1 + c'\rho^2. \end{aligned}$$

On reconnaîtra, de même, que le nombre des fois où l'expression précédente devient égale à ρ et égale à ρ^2 est exprimé, dans le premier cas, par la somme des nombres de solutions des congruences

$$\begin{aligned} 1 + b\rho &\equiv 1 + a\rho^2 \pmod{A + B\rho^2}. \\ 1 + c\rho &\equiv 1 + b\rho^2, \\ 1 + a\rho &\equiv 1 + c\rho^2, \end{aligned}$$

et, dans le second cas, par la somme des nombres de solutions des congruences

$$\begin{aligned} 1 + c\rho &\equiv 1 + a\rho^2 \pmod{A + B\rho^2}, \\ 1 + a\rho &\equiv 1 + b\rho^2, \\ 1 + b\rho &\equiv 1 + c\rho^2. \end{aligned}$$

Pour pouvoir appliquer directement les développements des n^{os} 25-28, il est un peu plus facile de considérer seulement des congruences suivant le module $A + B\rho$, de sorte que, remplaçant partout dans les formules précédentes ρ par ρ^2, et désignant par t, u, v les nombres de fois que

$$\left[\frac{1 + x\rho}{A + B\rho}\right] \times \left[\frac{1 + x\rho}{A + B\rho^2}\right]$$

est respectivement égal à 1, à ρ et à ρ^2, nous écrirons : t égale la somme des nombres de solutions de

$$\begin{aligned} 1 + a\rho^2 &\equiv 1 + a'\rho \pmod{A + B\rho}, \\ 1 + b\rho^2 &\equiv 1 + b'\rho, \\ 1 + c\rho^2 &\equiv 1 + c'\rho, \end{aligned}$$

u égale la somme des nombres de solutions de

$$\begin{aligned} 1 + b\rho^2 &\equiv 1 + a\rho \pmod{A + B\rho}, \\ 1 + c\rho^2 &\equiv 1 + b\rho, \\ 1 + a\rho^2 &\equiv 1 + c\rho, \end{aligned}$$

v égale la somme des nombres de solutions de

$$\begin{aligned} 1 + c\rho^2 &\equiv 1 + a\rho \pmod{A + B\rho}, \\ 1 + a\rho^2 &\equiv 1 + b\rho, \\ 1 + b\rho^2 &\equiv 1 + c\rho. \end{aligned}$$

38. A ce sujet, il convient encore de remarquer ce qui suit. Parmi les nombres $a, b, c, a', b', c', \ldots$, ne se trouve pas l'un des deux nombres $-f$, $-g$. Supposons que ce soit $-f$, de sorte que $-g$ s'y trouve. Il n'en est alors pas moins évident que cette valeur $-g$ ne peut se présenter nulle part dans l'une des congruences ci-dessus; car, de $1+a\rho^2\equiv 1+a'\rho$ ou $a\rho^2\equiv a'\rho$, par exemple, il suivrait, pour $a=-g$, $a'\equiv a\rho\equiv -\rho^2\equiv -f$ [puisque $f=\rho^2$ et $g=\rho \pmod{A+B\rho}$]; or, la valeur $a'\equiv -f$ ne se présente pas. Comme, parmi les valeurs à prendre pour x, ne se trouvaient ni $-f$, ni $-g$, il en ressort avec évidence que les expressions ci-dessus données pour t, u et v sont réellement exactes, lorsque les nombres a, a', b, b', c, c', qui entrent dans les congruences, sont choisis de toutes les manières possibles dans les groupes $a, a', a'', \ldots, b, b', b'', \ldots, c, c', c'', \ldots$.

En introduisant, au lieu de $a, b, \ldots$, les nombres $\alpha=1+a\rho, \beta=1+b\rho, \ldots$, on trouve, par exemple, que

$$a\rho^2\equiv a'\rho \qquad \text{se transforme en} \qquad \rho(\alpha-1)\equiv\alpha'-1,$$

ou

$$\alpha'-\rho\alpha=1-\rho,$$

et, en agissant de même avec les autres congruences, on obtient les conclusions suivantes : t égale la somme des nombres de solutions de

$$\begin{aligned}&\alpha'-\rho\alpha\equiv 1-\rho \pmod{A+B\rho},\\ &\beta'-\rho\beta\equiv 1-\rho,\\ &\gamma'-\rho\gamma\equiv 1-\rho;\end{aligned}$$

u égale la somme des nombres de solutions de

$$\begin{aligned}&\alpha-\rho\beta\equiv 1-\rho \pmod{A+B\rho};\\ &\beta-\rho\gamma\equiv 1-\rho,\\ &\gamma-\rho\alpha\equiv 1-\rho;\end{aligned}$$

v égale la somme des nombres de solutions de

$$\begin{aligned}&\alpha-\rho\gamma\equiv 1-\rho \pmod{A+B\rho},\\ &\beta-\rho\alpha\equiv 1-\rho,\\ &\gamma-\rho\beta\equiv 1-\rho.\end{aligned}$$

Dans le premier membre de ces congruences le signe $-$ peut partout être remplacé par $+$, puisque deux nombres λ et $-\lambda$ appartiennent toujours à la même classe. Ce remplacement étant effectué, et toutes les con-

gruences étant, en outre, multipliées par le nombre entier

$$\frac{P-1}{1-\rho}=\frac{3n}{1-\rho}=n(1-\rho^2),$$

alors : t égale la somme des nombres de solutions de

$$\begin{aligned}&\alpha'+\rho\alpha+1\equiv 0 \qquad (\text{mod } A+B\rho),\\ &\beta'+\rho\beta+1\equiv 0,\\ &\gamma'+\rho\gamma+1\equiv 0;\end{aligned}$$

u égale la somme des nombres de solutions de

$$\begin{aligned}&\alpha+\rho\beta+1\equiv 0 \qquad (\text{mod } A+B\rho),\\ &\beta+\rho\gamma+1\equiv 0,\\ &\gamma+\rho\alpha+1\equiv 0;\end{aligned}$$

v égale la somme des nombres de solutions de

$$\begin{aligned}&\alpha+\rho\gamma+1\equiv 0 \qquad (\text{mod } A+B\rho),\\ &\beta+\rho\alpha+1\equiv 0,\\ &\gamma+\rho\beta+1\equiv 0.\end{aligned}$$

On arrive à ce résultat dans chacune des trois suppositions qui peuvent être faites, à savoir : que $n(1-\rho^2)$ fait partie de la classe (A), (B) ou (C). Cela tient évidemment à ce que les groupes de trois congruences, qui viennent d'être trouvés, sont tels qu'ils n'éprouvent aucun changement par une permutation cyclique de α, β, γ.

Il y a maintenant trois cas à distinguer :

I. ρ appartient à (A), ou

$$\left[\frac{\rho}{A+B\rho}\right]=1.$$

Dans ce cas, on a

$$\rho\alpha=\alpha'', \qquad \rho\beta=\beta'', \qquad \rho\gamma=\gamma'',$$

et, par conséquent, t, u, v sont les sommes des nombres de solutions des congruences suivantes :

t.	u.	v.
$\alpha+\alpha'+1\equiv 0$	$\alpha+\beta+1\equiv 0$	$\alpha+\gamma+1\equiv 0$
$\beta+\beta'+1\equiv 0$	$\beta+\gamma+1\equiv 0$	$\beta+\alpha+1\equiv 0$
$\gamma+\gamma'+1\equiv 0$	$\gamma+\alpha+1\equiv 0$	$\gamma+\beta+1\equiv 0$

ou, d'après le n° 25, si les résultats trouvés à cet endroit pour le nombre

premier $a+b\rho$ sont transportés au module $A+B\rho$ avec la norme $3n+1$,

$$t=h+k+j=n-1,$$
$$u=j+l+k=n,$$
$$v=k+j+l=n.$$

D'après le n° 36, on a dans ce cas, pour $a\equiv 0$,

$$\left[\frac{P}{a+b\rho}\right]=1.$$

II. ρ appartient à (B), ou

$$\left[\frac{\rho}{A+B\rho}\right]=\rho.$$

t, u, v sont alors les sommes des nombres de solutions des congruences suivantes :

t.	u.	v.
$\alpha+\beta+1\equiv 0$	$\alpha+\gamma+1\equiv 0$	$\alpha+\alpha'+1\equiv 0$
$\beta+\gamma+1\equiv 0$	$\beta+\alpha+1\equiv 0$	$\beta+\beta'+1\equiv 0$
$\gamma+\alpha+1\equiv 0$	$\gamma+\beta+1\equiv 0$	$\gamma+\gamma'+1\equiv 0$

ou bien

$$t=n,$$
$$u=n,$$
$$v=n-1.$$

D'après le n° 36, on a dans ce cas, pour $a\equiv 0$

$$\left[\frac{P}{a+b\rho}\right]=\rho^2.$$

III. ρ appartient à C, ou

$$\left[\frac{\rho}{A+B\rho}\right]=\rho^2.$$

t, u, v sont alors les sommes des nombres de solutions de

t.	u.	v.
$\alpha+\gamma+1\equiv 0$	$\alpha+\alpha'+1\equiv 0$	$\alpha+\beta+1\equiv 0$
$\beta+\alpha+1\equiv 0$	$\beta+\beta'+1\equiv 0$	$\beta+\gamma+1\equiv 0$
$\gamma+\beta+1\equiv 0$	$\gamma+\gamma'+1\equiv 0$	$\gamma+\alpha+1\equiv 0$

ou bien

$$t = n,$$
$$u = n - 1,$$
$$v = n.$$

D'après le n° 36, on a dans ce cas, pour $a \equiv 0$

$$\left[\frac{P}{a + b\rho}\right] = \rho.$$

Par là se trouve démontré tout ce qui a été dit au n° 33 concernant la forme générale des caractères qui permettent de reconnaître à laquelle des trois classes appartient un nombre premier donné.

39. Quant aux autres énoncés du n° 33, il suffira de remarquer que ce qui a été dit dans la remarque 6° résulte immédiatement des formules

$$\left[\frac{1 + x\rho}{Q}\right]\left[\frac{1 + y\rho}{Q}\right] = \left[\frac{1 - xy + (x + y - xy)\rho}{Q}\right]$$

et

$$\left[\frac{1 + x\rho}{A + B\rho}\right]\left[\frac{1 + x\rho}{A + B\rho^2}\right]\left[\frac{1 + y\rho}{A + B\rho}\right]\left[\frac{1 + y\rho}{A + B\rho^2}\right]$$
$$= \left[\frac{1 - xy + (x + y - xy)\rho}{A + B\rho}\right]\left[\frac{1 - xy + (x + y - xy)\rho}{A + B\rho^2}\right].$$

De la remarque que, pour $b \equiv 2a$, le nombre premier (2, 5, 7, 11, ...) appartient toujours à la classe (A), on peut encore déduire une conséquence qu'il paraît utile de noter ici. Puisque, à cause de

$$4p = 4(a^2 - ab + b^2) = (2a - b)^2 + 3b^2,$$

3 ne fait *pas* partie des facteurs premiers de $2a - b$, il s'ensuit que tous les facteurs premiers de $2a - b$ sont des résidus cubiques de p, et, par conséquent, $2a - b$ lui-même est résidu cubique de p.

40. A ce même résultat conduit aussi la considération suivante, de tout autre nature.

Soit $p = 3n + 1$ et supposons que z parcoure un système complet de nombres incongrus, non divisibles par le module $a + b\rho$; de l'équation

$$(z^3 + 1)^{2n} = z^{6n} + \ldots + \frac{2n(2n - 1)\ldots(n + 1)}{1.2.3\ldots n} z^{3n} + \ldots + 1$$

il suit alors

$$\Sigma(z^3 + 1)^{2n} \equiv -2 - \frac{2n(2n - 1)\ldots(n + 1)}{1.2.3\ldots n} \pmod{a + b\rho}.$$

Mais, d'un autre côté, les nombres z^3, ... forment tous des résidus cubiques de $a+b\rho$, chaque résidu étant écrit trois fois, et parmi les nombres z^3+1 il y en a donc $3h$ qui appartiennent à la classe (A), $3j$ à (B), $3k$ à (C); par conséquent, on a aussi

$$\Sigma(z^3+1)^{2n} \equiv 3h + 3k\rho + 3j\rho^2 \qquad (\text{mod } a+b\rho),$$

ou, d'après les valeurs du n° 28,

$$\Sigma(z^3+1)^{2n} \equiv a - b - 2 - b\rho.$$

Il en résulte

$$-\frac{2n(2n-1)\ldots(n+1)}{1.2.3\ldots n} \equiv a - b - b\rho \equiv 2a - b \qquad (\text{mod } a+b\rho),$$

de sorte qu'on a aussi

$$2a - b \equiv -\frac{2n(2n-1)\ldots(n+1)}{1.2.3\ldots n} \qquad (\text{mod } p = 3n+1),$$

congruence remarquable, donnée pour la première fois par Jacobi, dans le *Journal de Crelle*, t. II, et dont la démonstration est ordinairement déduite de formules employées dans la théorie de la division du cercle.

En écrivant cette congruence sous la forme

$$(1.2.3\ldots n)^2(2a-b) \equiv -1.2.3\ldots(2n) \qquad (\text{mod } p),$$

et en observant que

$$\begin{aligned} 2n+1 &\equiv -n, \\ 2n+2 &\equiv -(n-1), \\ 2n+3 &\equiv -(n-2), \\ &\ldots\ldots\ldots\ldots, \\ 3n &\equiv -1, \end{aligned}$$

que n est pair et $1.2.3\ldots(3n) \equiv -1$, on obtient

$$(1.\,2.\,3.\,\ldots.\,n)^3(2a-b) \equiv 1 \qquad (\text{mod } p),$$

d'où il ressort immédiatement que $2a-b$ est résidu cubique de p, ainsi que nous l'avions déjà trouvé ci-dessus, par une voie toute différente. Cette première démonstration nous avait appris, en outre, que tous les diviseurs de $2a-b$ sont des résidus cubiques.