CONTRIBUTION A LA THÉORIE

DES

RÉSIDUS CUBIQUES ET BIQUADRATIQUES,

PAR T.-J. STIELTJES (1).

Le théorème fondamental de la théorie des résidus quadratiques (la loi dite de *réciprocité*) est relatif au rapport réciproque de deux nombres premiers *impairs*, et dans une théorie complète le caractère du nombre 2, comme résidu ou non-résidu quadratique d'un autre nombre premier impair, doit donc être déterminé séparément. Il ressort de là que le nombre 2 occupe une place à part parmi tous les nombres premiers.

Les théorèmes par lesquels est déterminé le caractère de 2 ont été énoncés pour la première fois par Fermat (2) et démontrés par Lagrange (3). Il convient de remarquer, toutefois, que la démonstration de Lagrange s'appuie sur des considérations tout à fait semblables à celles par lesquelles, antérieurement, Euler (4) avait démontré les théorèmes, également énoncés par Fermat, qui fixent le caractère de 3 comme résidu ou non-résidu quadratique. L'insuccès d'Euler dans tous ses efforts pour démontrer les théorèmes concernant le caractère de 2 (Voir *Disq. arithm.*, Art. 120) est donc d'autant plus surprenant.

Un phénomène entièrement analogue se présente dans la théorie des résidus biquadratiques. Ici également, la loi générale de réciprocité a rapport à deux nombres premiers *impairs*, c'est-à-dire, non divisibles par $1+i$, et le caractère de ce nombre premier particulier doit être déterminé séparément.

(1) Extrait des *Archives néerlandaises*, t. XVIII, 1883.
(2) *Op. mathem.*, p. 168.
(3) *Nouv. Mém. de l'Acad. de Berlin*, 1775. *Œuvres*, t. III, p. 759.
(4) *Comment. nov. Petrop.*, t. VIII, p. 105.

Dans le Mémoire de Gauss : *Theoria residuorum biquadraticorum, commentatio secunda,* où les nombres complexes entiers de la forme $a + bi$ furent introduits pour la première fois dans la théorie des nombres, le caractère biquadratique de $1 + i$ est déterminé complètement. La démonstration y est de nature purement arithmétique et s'appuie essentiellement sur le théorème de l'Art. 71, théorème analogue au lemme formant la base tant de la troisième que de la cinquième démonstration de Gauss pour la loi de réciprocité dans la théorie des résidus quadratiques [*Theorematis arithmetici demonstratio nova* (*Werke,* t. II, p. 1), et *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novæ* (*Werke,* t. II, p. 47)].

Comme on le sait, le troisième Mémoire, dans lequel Gauss s'était proposé de donner la démonstration de la loi générale de réciprocité, déjà énoncée dans son second Mémoire sur cette théorie, n'a jamais paru.

Les deux premières démonstrations publiées de ce théorème fondamental sont celles d'Eisenstein, dans le tome XXVIII du *Journal für Mathematik* de Crelle, p. 53 et 223. Dans le premier article : *Lois de réciprocité,* il n'a pas traité du caractère de $1 + i$, mais bien dans le second article : *Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste.* Eisenstein fait usage, dans l'établissement du caractère de $1 + i$, de la loi générale de réciprocité démontrée antérieurement, ce qui en tout cas paraît peu élégant, vu que le passage du simple au composé demande nécessairement que le caractère de $1 + i$ soit déduit d'une façon entièrement indépendante du théorème fondamental.

La même remarque est plus ou moins applicable à toutes les autres méthodes qui ont été employées postérieurement pour traiter la théorie des résidus biquadratiques; la marche suivie par Gauss pour démontrer le caractère de $1 + i$ est, à mon avis, la seule qui puisse être dite *purement arithmétique* et *complètement indépendante* de la loi générale de réciprocité, de sorte qu'elle satisfait, sous ce rapport, aux conditions qui devront être imposées à tout développement méthodique de la théorie des résidus biquadratiques, prise dans son ensemble.

Des remarques tout à fait analogues peuvent être faites au sujet de la théorie des résidus cubiques. La première démonstration de la loi de réciprocité dans cette théorie, loi énoncée par Jacobi, est celle d'Eisenstein, publiée dans le tome 27 du *Journal für Mathematik* de Crelle, p. 289.

La détermination particulière du caractère de $1-\rho$ (où ρ est une racine cubique complexe de l'unité) n'a été donnée par Eisenstein que plus tard, dans le tome 28, p. 28 et suiv., du même Journal. Pour cette détermination il fait encore usage de la loi générale de réciprocité, et je ne sache pas qu'on ait donné jusqu'ici un mode de déduction du caractère cubique de $1-\rho$ dont la même chose ne puisse être dite.

Comme il est à désirer, toutefois, qu'on possède une démonstration du caractère de $1+i$ et de $1-\rho$ entièrement indépendante de la loi générale de réciprocité, il y aura peut-être quelque intérêt à faire voir comment tous ces théorèmes relatifs aux nombres premiers 2, $1+i$ et $1-\rho$, théorèmes nécessaires pour compléter les lois de réciprocité, peuvent être démontrés suivant une *méthode uniforme*.

Le principe de cette méthode consiste à remplacer le nombre premier dont il s'agit de déterminer le caractère par un produit congruent de facteurs. On détermine alors le caractère de ces facteurs par des considérations tout à fait analogues à celles dont Gauss s'est servi dans les Art. 15-20 de son *premier* Mémoire sur la théorie des résidus biquadratiques (*Werke*, t. II, p. 78-87). Gauss n'y a en vue que les nombres réels, et l'objet de son Mémoire est la détermination du caractère de 2 dans la théorie réelle. Mais j'ai reconnu que tous les raisonnements de Gauss se laissent reproduire aussi, presque sans changement, dans la théorie des nombres complexes, et la détermination du caractère biquadratique de $1+i$ s'obtient alors immédiatement au moyen d'une considération très simple, suivant laquelle $1+i$ est congruent avec un produit dont on connaît le caractère des facteurs.

A l'aide de ces remarques extrêmement simples, et étant données les recherches du premier Mémoire de Gauss, la détermination du caractère de $1+i$ par rapport à un nombre premier de la forme $a+bi$ (où b n'est pas égal à zéro) n'offre plus aucune difficulté; une méthode entièrement analogue peut d'ailleurs être employée dans le cas où le module est un nombre premier réel de la forme $4n+3$. Bien que ce dernier cas permette une démonstration beaucoup plus simple (*voir*, par exemple, Gauss, t. II, Art. 68), j'ai cru devoir le traiter de la même manière que les autres cas, pour faire ressortir que la méthode en question suffit à établir l'ensemble des théorèmes.

Après avoir effectué la détermination du caractère biquadratique de $1+i$, je démontre, à l'aide des développements antérieurs, tous les théorèmes

que Gauss a trouvés par induction et énoncés dans l'Art. 28 de la *Theoria residuorum biquadraticorum, commentatio secunda*. Si je ne me trompe, cette démonstration est donnée ici pour la première fois (1). Elle est entièrement fondée sur la théorie des nombres complexes, théorie qui joue donc ici un rôle purement auxiliaire, les théorèmes eux-mêmes ayant seulement rapport à des nombres réels. Outre la loi de réciprocité dans la théorie des résidus biquadratiques, la démonstration complète exigeait encore les considérations des Art. 19-21.

Je vais maintenant commencer par déduire le caractère de 2 dans la théorie des

Résidus quadratiques.

1. Soit p un nombre premier impair, les nombres

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

seront alors divisés en deux groupes. Dans le premier groupe

$$(A) \qquad \alpha, \quad \alpha', \quad \alpha'', \quad \ldots$$

sont rapportés tous les résidus quadratiques; dans le second groupe

$$(B) \qquad \beta, \quad \beta', \quad \beta'', \quad \ldots$$

tous les non-résidus, pour le module p. Chacun des groupes (A) et (B) se compose de $\frac{p-1}{2}$ nombres incongrus par rapport au module p, et il est facile de voir que les deux congruences

$$(x-\alpha)(x-\alpha')(x-\alpha'')\ldots \equiv x^{\frac{p-1}{2}} - 1 \pmod{p},$$
$$(x-\beta)(x-\beta')(x-\beta'')\ldots \equiv x^{\frac{p-1}{2}} + 1$$

sont des congruences identiques; car elles sont de degré inférieur à $\frac{p-1}{2}$ et toutes les deux possèdent manifestement $\frac{p-1}{2}$ racines, à savoir, la première, les racines $x=\alpha$, $x=\alpha'$, $x=\alpha''$, ...; la seconde, les racines $x=\beta$, $x=\beta'$, $x=\beta''$, ...

(1) *Une partie* de ces théorèmes a été démontrée par M. Lebesgue, dans le *Journal de Liouville*, t. VI, p. 51, 52, remarque 1°.

En ajoutant l'unité aux nombres de (A) et (B), on obtient les groupes de nombres suivants :

$$(A') \qquad \alpha+1, \quad \alpha'+1, \quad \alpha''+1, \quad \ldots,$$
$$(B') \qquad \beta+1, \quad \beta'+1, \quad \beta''+1, \quad \ldots.$$

Les nombres de nombres du groupe (A') qui font partie de (A) et de (B) seront désignés respectivement par (0,0), (0,1), et les nombres de nombres de (B') qui entrent dans (A) et (B) respectivement par (1,0), (1,1).

Ces quatre nombres peuvent être réunis dans le Tableau S suivant :

$$\begin{matrix}(0,0) & (0,1)\\ (1,0) & (1,1)\end{matrix}$$

Comme les nombres premiers des formes $p=4n+1$ et $p=4n+3$ se comportent d'une manière différente, ces deux cas doivent être traités séparément. Commençons par le premier.

2. Pour $p=4n+1$, -1 est résidu quadratique, de sorte que les nombres α et $p-\alpha$ entrent simultanément dans (A). De même, les nombres β et $p-\beta$ entrent simultanément dans (B).

Or (0,0) est évidemment égal au nombre de solutions de la congruence

$$\alpha+1\equiv\alpha' \pmod p,$$

où α et α' doivent être choisis dans le groupe (A); et comme on a $\alpha'=p-\alpha''$, on peut dire aussi que (0,0) représente le nombre de solutions de la congruence

$$\alpha+\alpha''+1\equiv 0 \pmod p.$$

En raisonnant de la même manière par rapport aux nombres (0,1), (1,0), (1,1), on reconnaît que

Le signe	Représente le nombre des solutions de
(0,0)	$\alpha+\alpha'+1\equiv 0$
(0,1)	$\alpha+\beta+1\equiv 0$
(1,0)	$\beta+\alpha+1\equiv 0$
(1,1)	$\beta+\beta'+1\equiv 0$, le tout (mod p).

Il en ressort immédiatement

$$(0,1)=(1,0);$$

une seconde relation entre les nombres du schéma S est fournie par la considération suivante. A chaque nombre β du groupe (B) correspond, dans ce même groupe, un nombre déterminé unique β'', tel qu'on a

$$\beta\beta'' \equiv 1 \pmod{p},$$

et, en outre, $\beta'\beta''$ est alors congru avec un nombre α du groupe (A). La multiplication de la congruence

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

par β'' donne donc

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

et, en multipliant cette dernière congruence par β, on retrouve la première. De là se déduit immédiatement $(1,1) = (0,1)$, de sorte que le schéma S a la forme

$$\begin{matrix} h & j \\ j & j \end{matrix}$$

Or, dans le groupe (A) se trouve le nombre $p-1$, et, par conséquent, dans (A') le nombre p, qui n'entre ni dans (A), ni dans (B). Mais tous les autres nombres de (A') et (B') font partie soit de (A), soit de (B).

Il en résulte

$$h + j = \frac{p-1}{2} - 1,$$

$$2j = \frac{p-1}{2},$$

donc

$$h = \frac{p-5}{4}, \qquad j = \frac{p-1}{4}.$$

La congruence identique

$$(x-\beta)(x-\beta')(x-\beta'')\ldots \equiv x^{\frac{p-1}{2}} + 1 \pmod{p}$$

donne maintenant pour $x = -1$, puisque $\frac{p-1}{2}$ est pair,

$$(\beta+1)(\beta'+1)(\beta''+1)\ldots \equiv 2 \pmod{p}.$$

Le nombre des non-résidus parmi les nombres $\beta+1$, $\beta'+1$, $\beta''+1$, ..., est $(1,1) = j = \frac{p-1}{4}$.

Si donc j est *pair*, ou si

$$p = 8n + 1,$$

2 est résidu quadratique de p.

Si, au contraire, j est *impair*, ou si

$$p = 8n + 5,$$

2 est non-résidu de p.

3. Pour $p = 4n + 3$, -1 est non-résidu, et le groupe (B) est identique au groupe des nombres $p - \alpha$, $p - \alpha'$, $p - \alpha''$, ...

Le signe (0,0) représente alors le nombre des solutions de la congruence $\alpha + 1 \equiv \alpha' \pmod p$ ou aussi, puisque $\alpha' = p - \beta$, le nombre des solutions de $\alpha + \beta + 1 \equiv 0$.

On voit ainsi que

Le signe	Représente le nombre des solutions de	
(0,0)	$\alpha + \beta + 1 \equiv 0$,	
(0,1)	$\alpha + \alpha' + 1 \equiv 0$,	
(1,0)	$\beta + \beta' + 1 \equiv 0$,	
(1,1)	$\beta + \alpha + 1 \equiv 0$	$(\mathrm{mod}\ p)$,

de sorte que $(0,0) = (1,1)$. Si, en outre, on a de nouveau $\beta\beta'' \equiv 1$, $\beta'\beta'' \equiv \alpha$, la conguence $\beta + \beta' + 1 \equiv 0$, étant multipliée par β'', donne

$$1 + \alpha + \beta'' \equiv 0;$$

d'où résulte, d'une manière analogue à celle indiquée dans le cas précédent, la relation $(1,0) = (0,0)$. Le schéma (S) a donc pour $p = 4n + 3$ la forme

$$\begin{matrix} h & j \\ h & h \end{matrix}$$

Comme le nombre $p - 1$ entre dans le groupe (B), et, par conséquent, p dans (B'), mais que d'ailleurs tous les autres nombres de (A') et (B') entrent soit dans (A), soit dans (B), on trouve

$$h + j = \frac{p-1}{2},$$

$$2h = \frac{p-1}{2} - 1,$$

donc

$$h = \frac{p-3}{4}, \qquad j = \frac{p+1}{4}.$$

De la congruence identique

$$(x-\alpha)(x-\alpha')(x-\alpha'')\ldots \equiv x^{\frac{p-1}{2}} - 1 \pmod p$$

il résulte pour $x = -1$, vu que $\frac{p-1}{2}$ est impair,

$$(\alpha+1)(\alpha'+1)(\alpha''+1)\ldots \equiv 2 \pmod{p},$$

et le nombre des non-résidus, parmi les nombres $\alpha+1$, $\alpha'+1$, $\alpha''+1$, ..., est égal à $j = \frac{p+1}{4}$.

Si l'on a donc j *pair*, ou si

$$p = 8n+7,$$

2 est résidu quadratique de p.

Si, au contraire, j est *impair*, ou si

$$p = 8n+3,$$

2 est non-résidu de p.

Ayant ainsi déterminé le caractère de 2 comme résidu quadratique ou non-résidu, par rapport à un nombre premier impair quelconque, je vais établir le théorème correspondant dans la théorie des

Résidus biquadratiques.

4. Le nombre premier impair (c'est-à-dire non divisible par $1+i$) $m = a+bi$ sera toujours supposé *primaire*, ce mot étant pris dans l'acception qui lui est donnée par Gauss, de sorte que $a-1$ et b, suivant le module 4, soient ou bien tous les deux $\equiv 0$, ou bien tous les deux $\equiv 2$.

On sait que, dans la théorie des nombres complexes entiers de la forme $a+bi$, les nombres premiers se composent :

Premièrement, des nombres premiers réels q de la forme $4n+3$, nombres qui doivent être pris négativement pour être primaires;

Secondement, des facteurs premiers complexes des nombres premiers réels de la forme $4n+1$. Ces nombres premiers complexes sont de la forme $a+bi$, où b n'est pas égal à zéro, et deviennent primaires lorsqu'on les multiplie par l'une des quatre unités 1, i, -1, $-i$, convenablement choisie. Ils peuvent à leur tour être distingués en deux espèces, suivant que, lorsque $a+bi$ est primaire, $a-1$ et b sont tous les deux divisibles par 4, ou tous les deux le double d'un nombre impair.

D'après cela, je partage les nombres premiers primaires en ces trois classes :

I. Les nombres premiers réels q de la forme $4r+3$, pris négativement.

II. Les nombres premiers complexes de la forme $4r+1+4si$.

III. Les nombres premiers complexes de la forme $4r+3+(4s+2)i$.

Le nombre premier (dans la théorie complexe) sera toujours désigné ici par M, la norme de M par μ. En outre, p représentera toujours un nombre premier réel (positif) de la forme $4r+1$, q un nombre premier réel (positif) de la forme $4r+3$. Pour les nombres premiers de la première espèce, on a donc $M=-q$, $\mu=q^2$, pour ceux de la deuxième et de la troisième espèce, $\mu=p$.

Je remarquerai encore que pour les deux espèces I et II la norme μ est de la forme $8r+1$, et pour III de la forme $8r+5$. Cette circonstance fait que les deux premières espèces de nombres premiers peuvent, jusqu'à un certain point, être traitées conjointement.

Les considérations de l'article suivant, 5, s'appliquent encore, à titre égal, aux trois classes de nombres premiers.

5. Soient donc M le nombre premier, μ la norme. Un système complet de nombres incongrus et non divisibles par le module se compose de $\mu-1$ nombres, qui, suivant leur caractère biquadratique par rapport à M, peuvent être distribués en quatre classes, comprenant chacune $\frac{\mu-1}{4}$ nombres :

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

Dans la première classe (A) sont rangés tous les nombres α, α', α'', ... à caractère biquadratique 0; dans les groupes (B), (C), (D), les nombres à caractère biquadratique 1, 2, 3.

Disons encore, par surcroît, que le caractère biquadratique est pris ici dans le sens adopté par Gauss, de sorte que les nombres des quatre classes sont caractérisés par les congruences

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

Pour plus de commodité, je me servirai toutefois aussi du symbole introduit par Jacobi, et pourrai donc écrire

$$\left(\left(\frac{\alpha}{M}\right)\right)=1,\qquad \left(\left(\frac{\beta}{M}\right)\right)=i,\qquad \left(\left(\frac{\gamma}{M}\right)\right)=-1,\qquad \left(\left(\frac{\delta}{M}\right)\right)=-i.$$

Notons enfin, une fois pour toutes, que dans la suite toutes les congruences auront rapport au module premier M, tant qu'un autre module ne sera pas expressément indiqué.

Je donne ici un exemple de la distribution des résidus module M, à l'exception du résidu o, dans les quatre classes (A), (B), (C), (D), pour chacune des trois espèces de nombres premiers qui ont été distinguées dans le n° 4.

$$M = -7, \qquad \mu = 49.$$

(A) $1,\ 3i,\ -2,\ i,\ -3,\ -2i,\ -1,\ -3i,\ 2,\ -i,\ 3,\ 2i.$

(B) $1-2i,\ -1+3i,\ -2-3i,\ 2+i,\ -3-i,\ 3-2i,\ -1+2i,$
$1-3i,\ 2+3i,\ -2-i,\ 3+i,\ -3+2i.$

(C) $-3+3i,\ -2-2i,\ -1+i,\ -3-3i,\ 2-2i,\ -1-i,\ 3-3i,$
$2+2i,\ 1-i,\ 3+3i,\ -2+2i,\ 1+i.$

(D) $3+2i,\ 1+2i,\ 1+3i,\ -2+3i,\ -2+i,\ -3+i,\ -3-2i,$
$-1-2i,\ -1-3i,\ 2-3i,\ 2-i,\ 3-i.$

$$M = -3-8i, \qquad \mu = 73.$$

(A) $1,\ 3+2i,\ -1-4i,\ -3i,\ 1+2i,\ -4,\ -1-3i,\ -2,\ -3+4i,$
$-1,\ -3-2i,\ 1+4i,\ 3i,\ -1-2i,\ 4,\ 1+3i,\ 2,\ 3-4i.$

(B) $1-2i,\ -1-i,\ 2+3i,\ 5+2i,\ -3+3i,\ 1-3i,\ 1-4i,\ -2+4i,$
$2+2i,\ -1+2i,\ 1+i,\ -2-3i,\ -5-2i,\ 3-3i,\ -1+3i,$
$-1+4i,\ 2-4i,\ -2-2i.$

(C) $4i,\ -3+i,\ 2i,\ 4+3i,\ i,\ -2+3i,\ 4-i,\ 3,\ -2+i,\ -4i,$
$3-i,\ -2i,\ -4-3i,\ -i,\ 2-3i,\ -4+i,\ -3,\ 2-i.$

(D) $-3-i,\ -4-i,\ 4+2i,\ 2-2i,\ 2+i,\ 1-i,\ -3+2i,\ -2+5i,$
$-3-3i,\ 3+i,\ 4+i,\ -4-2i,\ -2+2i,\ -2-i,\ -1+i,$
$3-2i,\ 2-5i,\ 3+3i.$

$$M = -5+6i, \qquad \mu = 61.$$

(A) $1,\ -4,\ -1-4i,\ -3,\ 1+i,\ 2+i,\ -2+i,\ 3+2i,\ 2i,\ 1+3i,$
$-3-i,\ -5,\ -2+2i,\ 3-2i,\ 4+i.$

(B) $1-i,\ 1-2i,\ 1+2i,\ 2-3i,\ 2,\ 3-i,\ -1+3i,\ 5i,\ 2+2i,$
$-2-3i,\ 1-4i,\ -i,\ 4i,\ -4+i,\ 3i.$

$$(C)\quad \begin{cases} -2i, & -1-3i, & 3+i, & 5, & 2-2i, & -3+2i, & -4-i, & -1, & 4, \\ 1+4i, & 3, & -1-i, & -2-i, & 2-i, & -3-2i. \end{cases}$$

$$(D)\quad \begin{cases} -2-2i, & 2+3i, & -1+4i, & i, & -4i, & 4-i, & -3i, & -1+i, \\ -1+2i, & -1-2i, & -2+3i, & -2, & -3+i, & 1-3i, & -5i. \end{cases}$$

De même que dans le n° 1, on se convainc immédiatement de l'identité de chacune des congruences suivantes :

$$\begin{aligned} &(x-\alpha)(x-\alpha')(x-\alpha'')\ldots \equiv x^{\frac{\mu-1}{4}}-1 \pmod{\mathbf{M}},\\ &(x-\beta)(x-\beta')(x-\beta'')\ldots \equiv x^{\frac{\mu-1}{4}}-i,\\ &(x-\gamma)(x-\gamma')(x-\gamma'')\ldots \equiv x^{\frac{\mu-1}{4}}+1,\\ &(x-\delta)(x-\delta')(x-\delta'')\ldots \equiv x^{\frac{\mu-1}{4}}+i; \end{aligned}$$

d'où il suit pour $x=-1$, en distinguant les cas $\mu=8n+1$ et $\mu=8n+5$:

$$\begin{aligned} \mu=8n+1,\quad &(\beta+1)(\beta'+1)(\beta''+1)\ldots \equiv 1-i \pmod{\mathbf{M}},\\ &(\gamma+1)(\gamma'+1)(\gamma''+1)\ldots \equiv 2,\\ &(\delta+1)(\delta'+1)(\delta''+1)\ldots \equiv 1+i.\\ \mu=8n+5,\quad &(\alpha+1)(\alpha'+1)(\alpha''+1)\ldots \equiv 2 \pmod{\mathbf{M}}.\\ &(\beta+1)(\beta'+1)(\beta''+1)\ldots \equiv 1+i,\\ &(\delta+1)(\delta'+1)(\delta''+1)\ldots \equiv 1-i. \end{aligned}$$

6. Considérons maintenant les nouveaux groupes de nombres (A'), (B'), (C') et (D') qui résultent de l'addition de l'unité aux nombres de (A), (B), (C) et (D) :

$$\begin{aligned} &(A')\quad \alpha+1,\ \alpha'+1,\ \alpha''+1,\ \ldots,\\ &(B')\quad \beta+1,\ \beta'+1,\ \beta''+1,\ \ldots,\\ &(C')\quad \gamma+1,\ \gamma'+1,\ \gamma''+1,\ \ldots,\\ &(D')\quad \delta+1,\ \delta'+1,\ \delta''+1,\ \ldots; \end{aligned}$$

désignons les nombres de nombres de (A') qui sont congrus avec des nombres de (A), (B), (C), (D) respectivement par

$$(0,0),\quad (0,1),\quad (0,2),\quad (0,3),$$

et les nombres de nombres de (B') qui sont congrus avec des nombres de (A), (B), (C), (D) respectivement par

$$(1,0),\quad (1,1),\quad (1,2),\quad (1,3).$$

De même, les nombres (2,0), (2,1), (2,2), (2,3) auront rapport au groupe (C′), et (3,0), (3,1), (3,2), (3,3) au groupe (D′).

Ces 16 nombres (0,0), (0,1), ... peuvent être tous réunis dans le Tableau quadratique (S) suivant

$$\begin{matrix} (0,0) & (0,1) & (0,2) & (0,3) \\ (1,0) & (1,1) & (1,2) & (1,3) \\ (2,0) & (2,1) & (2,2) & (2,3) \\ (3,0) & (3,1) & (3,2) & (3,3) \end{matrix}$$

et pour les exemples donnés dans le n° 5, j'obtiens

(S)

$M=-7$, $\mu=49$.	$M=-3-8i$, $\mu=73$.	$M=-5+6i$, $\mu=61$.
5 2 2 2	5 6 4 2	4 3 2 6
2 2 4 4	6 2 5 5	3 3 6 3
2 4 2 4	4 5 4 5	4 3 4 3
2 4 4 2	2 5 5 6	3 6 3 3

D'après les congruences de l'article précédent, on a, pour $\mu = 8n+1$,

$$(\delta+1)(\delta'+1)(\delta''+1)\ldots \equiv 1+i,$$

et pour $\mu = 8n+5$

$$(\beta+1)(\beta'+1)(\beta''+1)\ldots \equiv 1+i.$$

Or, les nombres de nombres de

$$\delta+1, \quad \delta'+1, \quad \delta''+1, \quad \ldots,$$

qui appartiennent respectivement aux classes (A), (B), (C), (D), étant (3,0), (3,1), (3,2), (3,3), il s'ensuit immédiatement que pour $\mu = 8n+1$ le caractère biquadratique de $1+i$, suivant le module 4, sera congru avec

$$(3,1)+2(3,2)+3(3,3),$$

et de même, dans le cas de $\mu = 8n+5$, avec

$$(1,1)+2(1,2)+3(1,3).$$

Dès que les nombres (0,0), (0,1) ... seront déterminés, le caractère biquadratique de $1+i$ sera donc aussi immédiatement connu.

Il s'agit donc, étant donné le nombre premier primaire $M = a + bi$, d'en déduire directement les nombres du Tableau (S). Les considérations nécessaires à cet effet sont essentiellement les mêmes que celles développées par Gauss dans les Art. 16-20 de la *Theoria residuorum biquadraticorum commentatio prima.*

Gauss traite, dans ce Mémoire, de la théorie des nombres réels, mais il est facile de voir que ce qu'il y donne est dans un étroit rapport avec la question dont nous nous occupons en ce moment.

Pour avoir sous les yeux le développement complet, il sera nécessaire de reproduire ici l'argumentation de Gauss, avec les légères modifications réclamées par la différence des sujets.

Il faut remarquer, à cet égard, que pour un nombre premier $M = -q$ appartenant à la première classe du n° 4, il n'existe, dans la théorie réelle de Gauss, rien d'analogue à ce qui sera exposé ici dans la théorie des nombres complexes entiers.

Pour ce qui va suivre, il est nécessaire de traiter séparément le cas où la norme μ est de la forme $8n + 1$ et celui où elle est de la forme $8n + 5$. Je commence par le premier, dans lequel le nombre premier M appartient donc à l'une des deux premières classes du n° 4.

7. Pour $\mu = 8n + 1$, on a

$$(-1)^{\frac{\mu-1}{4}} = +1,$$

de sorte que -1 est résidu biquadratique de M et fait partie de la classe (A), ou, à proprement parler, est congru suivant le module M avec un nombre de (A). Mais, dans ce genre de considérations, il est permis, attendu que les nombres congrus peuvent se remplacer entre eux, de les regarder comme égaux, et pour la commodité je ferai usage de cette observation, dont il ne pourra résulter aucune obscurité.

Le caractère biquadratique de -1 étant donc égal à zéro, il s'ensuit que lorsque α, β, γ, δ appartiennent respectivement aux classes (A), (B), (C), (D), les nombres $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ entrent aussi dans ces mêmes classes, $-\alpha$ dans (A), $-\beta$ dans (B), $-\gamma$ dans (C), $-\delta$ dans (D).

Or, le nombre (o, o) est évidemment égal au nombre des solutions de la congruence

$$\alpha + 1 \equiv \alpha' \pmod{M},$$

où α et α' sont à prendre arbitrairement dans le groupe (A); mais, comme

à chaque nombre α' correspond un nombre $\alpha'' = p - \alpha'$, ce nombre de solutions est le même que celui de la congruence

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

où α et α'' doivent également être pris dans (A).

En raisonnant exactement de la même manière au sujet des nombres (0,1), (0,2), etc., on trouve 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)	$\alpha + \gamma + 1 \equiv 0,$	
(0,3)	$\alpha + \delta + 1 \equiv 0,$	
(1,0)	$\beta + \alpha + 1 \equiv 0,$	
(1,1)	$\beta + \beta' + 1 \equiv 0,$	
(1,2)	$\beta + \gamma + 1 \equiv 0,$	
(1,3)	$\beta + \delta + 1 \equiv 0,$	
(2,0)	$\gamma + \alpha + 1 \equiv 0,$	
(2,1)	$\gamma + \beta + 1 \equiv 0,$	
(2,2)	$\gamma + \gamma' + 1 \equiv 0,$	
(2,3)	$\gamma + \delta + 1 \equiv 0,$	
(3,0)	$\delta + \alpha + 1 \equiv 0,$	
(3,1)	$\delta + \beta + 1 \equiv 0,$	
(3,2)	$\delta + \gamma + 1 \equiv 0,$	
(3,3)	$\delta + \delta' + 1 \equiv 0.$	

Il en résulte donc immédiatement ces six relations

$$(0,1) = (1,0), \quad (0,2) = (2,0), \quad (0,3) = (3,0),$$
$$(1,2) = (2,1), \quad (1,3) = (3,1), \quad (2,3) = (3,2).$$

Cinq autres relations entre les nombres (0,0), (0,1), ... s'obtiennent par la considération suivante : Si α, β, γ sont des nombres de (A), (B), (C), et qu'on détermine x, y, z de telle sorte qu'on ait

$$\alpha x \equiv 1, \quad \beta y \equiv 1, \quad \gamma z \equiv 1 \quad (\text{mod M}),$$

x appartient évidemment à la classe (A), y à (D), z à (C), de sorte qu'on peut écrire

$$\alpha\alpha' \equiv 1, \quad \beta\delta \equiv 1, \quad \gamma\gamma' \equiv 1.$$

Si l'on multiplie maintenant, en considérant une solution déterminée de

$\alpha + \beta + 1 \equiv 0$, cette congruence par δ, on obtient

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

où $\delta' \equiv \alpha\delta$ appartient à (D). Réciproquement, $\delta' + 1 + \delta \equiv 0$, multipliée par β, donne de nouveau

$$\alpha + \beta + 1 \equiv 0.$$

Il ressort de là que les deux congruences

$$\alpha + \beta + 1 \equiv 0 \qquad \text{et} \qquad \delta + \delta' + 1 \equiv 0$$

ont le même nombre de solutions, ou $(0, 1) = (3, 3)$.

Exactement de la même manière, on a

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

d'où l'on conclut pareillement

$$(0,2) = (2,2), \qquad (0,3) = (1,1), \qquad (1,2) = (1,3) = (2,3).$$

En tout, il existe donc *onze* relations entre les seize nombres du schéma (S), et ces nombres sont ainsi ramenés à *cinq*, différents entre eux, qui seront désignés par h, j, k, l, m. Le schéma (S) prend alors cette forme

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

8. Le nombre -1 entre dans (A) et correspond donc au nombre 0 de (A'). Ce nombre 0 de (A') ne se trouve dans aucune des classes (A), (B), (C), (D), mais tout autre nombre de (A') entre évidemment dans l'un des groupes (A), (B), (C) ou (D). Comme

$$\mu = 8n + 1, \qquad \frac{\mu - 1}{4} = 2n,$$

on a donc

$$(0,0) + (0,1) + (0,2) + (0,3) = 2n - 1.$$

Tous les nombres de (B'), (C'), (D') font partie d'une des classes (A),

(B), (C), (D), de sorte qu'on a

$$(1,0)+(1,1)+(1,2)+(1,3)=2n,$$
$$(2,0)+(2,1)+(2,2)+(2,3)=2n,$$
$$(3,0)+(3,1)+(3,2)+(3,3)=2n.$$

Ces quatre équations se réduisent aux trois relations suivantes entre h, j, k, l et m :

$$h+j+k+l=2n-1, \qquad j+l+2m=2n, \qquad k+m=n.$$

9. Enfin, une nouvelle relation, non linéaire, entre h, j, k, l, m s'obtient encore par la considération du nombre des solutions de la congruence

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

où α, β, γ doivent être choisis de toutes les manières possibles dans les classes (A), (B), (C).

Si l'on prend d'abord pour α successivement tous les nombres de (A), il arrive respectivement h, j, k, l fois que $\alpha+1$ appartienne à (A), (B), (C), (D), et le cas unique de $\alpha+1\equiv 0$ peut être négligé, vu que la congruence $\beta+\gamma\equiv 0$ n'admet aucune solution.

Pour chacune des h valeurs qui rendent $\alpha+1\equiv\alpha_0$, β et γ doivent alors être choisis de façon qu'on ait

$$\alpha_0+\beta+\gamma\equiv 0.$$

Le nombre des solutions de cette congruence (pour une valeur donnée de α_0) est $=m$, comme on le reconnaît immédiatement en la multipliant par α_0', ce qui la transforme, à cause de $\alpha_0\alpha_0'\equiv 1 \pmod{M}$, en

$$1+\beta'+\gamma'\equiv 0.$$

Comme ce raisonnement est applicable à chacune des h valeurs qui font que $\alpha+1$ appartient de nouveau à (A), on obtient de cette manière hm solutions de la congruence

$$1+\alpha+\beta+\gamma\equiv 0.$$

Il arrive ensuite j fois que $\alpha+1$ appartienne à (B), et pour chaque valeur déterminée $\alpha+1\equiv\beta_0$ la congruence

$$\beta_0+\beta+\gamma\equiv 0$$

a le même nombre de solutions que celle-ci

$$1 + \alpha + \beta' \equiv 0;$$

ce nombre est donc égal à j. Cela ressort immédiatement de

$$\delta_0(\beta_0 + \beta + \gamma) \equiv 1 + \alpha + \beta',$$

lorsque $\beta_0\delta_0 \equiv 1$.

Ces valeurs de α, qui font appartenir $\alpha + 1$ à (B), donnent donc en tout jj solutions de la congruence considérée.

Pour $\alpha + 1 \equiv \gamma_0$, ce qui arrive k fois, la congruence

$$\gamma_0 + \beta + \gamma \equiv 0$$

a l solutions, car

$$\gamma_0'(\gamma_0 + \beta + \gamma) \equiv 1 + \delta + \alpha.$$

Les valeurs de α qui font appartenir $\alpha + 1$ à (C) fournissent donc en tout kl solutions.

A-t-on enfin $\alpha + 1 = \delta_0$, ce qui arrive l fois; alors la congruence

$$\delta_0 + \beta + \gamma \equiv 0$$

a, en raison de

$$\beta_0(\delta_0 + \beta + \gamma) \equiv 1 + \gamma + \delta,$$

m solutions, et ces valeurs de α donnent donc lm solutions.

Le nombre total des solutions de la congruence

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

est donc

$$= hm + jj + kl + lm.$$

Mais ce nombre peut encore être calculé d'une autre manière. Si l'on prend pour β successivement tous les nombres de (B), il arrive j, l, m, m fois que $\beta + 1$ appartienne aux groupes (A), (B), (C), (D). Or, pour chacun de ces quatre nombres, on trouve qu'il y a respectivement k, m, k, m solutions de la congruence donnée, de sorte que le nombre total des solutions est

$$jk + lm + mk + mm.$$

10. En égalant entre elles ces deux expressions du nombre des solutions de $\alpha + \beta + \gamma + 1 \equiv 0$, on a

$$0 = hm + jj + kl - jk - km - mm,$$

ou, si l'on élimine h à l'aide de la valeur $h = 2m - k - 1$, qui se déduit facilement des équations obtenues dans le n° 8 entre h, j, k, l, m,

$$0 = (k-m)^2 + jj + kl - jk - kk - m.$$

D'après les relations du n° 8, on a

$$k = \tfrac{1}{2}(j+l),$$

et, cette valeur étant substituée dans $jj + kl - jk - kk$, cette expression devient $= \frac{1}{4}(l-j)^2$, de sorte que l'équation précédente, après multiplication par 4, se transforme en

$$0 = 4(k-m)^2 + (l-j)^2 - 4m;$$

mais

$$4m = 2(k+m) - 2(k-m) = 2n - 2(k-m),$$

par conséquent

$$2n = 4(k-m)^2 + 2(k-m) + (l-j)^2,$$

ou bien

$$\mu = 8n+1 = [4(k-m)+1]^2 + 4(l-j)^2;$$

en posant

$$4(k-m)+1 = \mathrm{A}, \qquad 2(l-j) = \mathrm{B},$$

il vient donc

$$\mu = \mathrm{A}^2 + \mathrm{B}^2.$$

Dans cette équation on a

$$\mathrm{A} \equiv 1 \pmod 4 \qquad \text{et} \qquad \mathrm{B} \text{ pair.}$$

Il est maintenant facile d'exprimer h, j, k, l, m au moyen de A et de B, ce qui donne

$$\begin{aligned} 8h &= 4n - 3\mathrm{A} - 5, \\ 8j &= 4n + \mathrm{A} - 2\mathrm{B} - 1, \\ 8k &= 4n + \mathrm{A} - 1, \\ 8l &= 4n + \mathrm{A} + 2\mathrm{B} - 1, \\ 8m &= 4n - \mathrm{A} + 1. \end{aligned}$$

Jusqu'ici nous avons seulement supposé que la norme μ avait la forme $8n+1$; mais, pour la détermination ultérieure de A et B, il faut maintenant traiter séparément les cas I et II du n° 4.

11. Soit donc, en premier lieu,

$$\mathrm{M} = -q = -(4r+3).$$

Dans ce cas, on a

$$\mu = \mathrm{M}^2 = q^2$$

et, par conséquent,

$$q^2 = \mathrm{A}^2 + \mathrm{B}^2.$$

q étant un nombre premier de la forme $4r + 3$, on sait que q^2 ne peut être représenté que d'une seule manière comme la somme de deux carrés, savoir, en prenant pour la base de l'un des carrés (impair) $\pm q$, et, pour la base de l'autre carré, 0; effectivement, si aucun des deux nombres A et B n'était égal à 0 ou divisible par q, on pourrait déterminer un nombre x, différent de 0, de telle sorte que

$$\mathrm{A}x \equiv \mathrm{B} \pmod{q}.$$

Mais, de

$$q^2 = \mathrm{A}^2 + \mathrm{B}^2,$$

il suit

$$\mathrm{A}^2 \equiv -\mathrm{B}^2 \pmod{q}$$

et aussi

$$\mathrm{A}^2x^2 \equiv \mathrm{B}^2 \quad \text{par conséquent} \quad x^2 \equiv -1 \pmod{q}.$$

Or, cette dernière congruence est impossible, parce que -1 est non-résidu quadratique de q.

De $q^2 = \mathrm{A}^2 + \mathrm{B}^2$, il suit donc nécessairement

$$\mathrm{A} = \pm q, \qquad \mathrm{B} = 0,$$

et comme $\mathrm{A} \equiv 1 \pmod 4$ le signe de A se trouve complètement déterminé et l'on a

$$\mathrm{A} = -q = \mathrm{M}.$$

A et B étant ainsi trouvés, on a finalement

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

où $8n + 1 = \mathrm{M}^2$.

Par ces formules, la dépendance entre les nombres du Tableau S et le nombre premier M est donc exprimée de la manière la plus simple, dans le cas où M appartient à la première classe du n° 4.

12. Si, en second lieu, on suppose $M = a + bi$, où $a - 1 \equiv b \equiv 0 \pmod 4$ et où la norme $\mu = a^2 + b^2$ est un nombre premier réel, on a donc

$$\mu = a^2 + b^2 = A^2 + B^2.$$

Or, un nombre premier de la forme $4k + 1$ ne peut être représenté que d'une seule manière par la somme de deux carrés, et comme a et A sont tous les deux $\equiv 1 \pmod 4$, il s'ensuit $A = a$, $B = \pm b$.

Le signe de (B) est déterminé par les considérations suivantes, qui demandent la démonstration préalable de cette proposition auxiliaire :

Lorsque z parcourt un système complet de résidus (mod M), à l'exception du terme divisible par M, on a

$$\Sigma z^t \equiv -1 \quad \text{ou} \quad \equiv 0 \pmod M,$$

suivant que t est divisible ou non par $\mu - 1$.

La première partie de cette proposition est évidente, car, si t est divisible par $\mu - 1$, on a

$$z^t \equiv 1, \quad \text{donc} \quad \Sigma z^t \equiv \mu - 1 \equiv -1 \pmod M.$$

Pour démontrer aussi la seconde partie, soit g une racine primitive pour le nombre premier M, de sorte que les valeurs parcourues par z soient congrues avec

$$g^0, \quad g^1, \quad g^2, \quad g^3, \quad \ldots, \quad g^{\mu-2}.$$

Il en résulte

$$\Sigma z^t \equiv 1 + g^t + g^{2t} + \ldots + g^{(\mu-2)t} \pmod M$$

ou

$$(1 - g^t)\Sigma z^t \equiv 1 - g^{(\mu-1)t} \equiv 0 \pmod M.$$

Or, si t n'est pas divisible par $\mu - 1$, $1 - g^t$ n'est pas divisible par M, et l'on a, par conséquent,

$$\Sigma z^t \equiv 0 \qquad \text{C. Q. F. D.}$$

Cette proposition auxiliaire est évidemment valable pour un nombre premier M quelconque.

D'après le développement binomial, on a maintenant

$$(z^2 + 1)^{\frac{\mu-1}{4}} = z^{\frac{\mu-1}{2}} + \ldots + 1,$$

d'où il suit, lorsque le signe Σ se rapporte aux mêmes valeurs de z que tout à l'heure,

$$\Sigma (z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1 \pmod M.$$

Mais, d'un autre côté, les nombres z^2, dans leur ensemble, forment évidemment tous les nombres des groupes (A) et (C), chacun de ces nombres étant pris deux fois. Des nombres

$$z^2+1$$

il y en a donc

$$\begin{aligned} &2(0,0)+2(2,0) \text{ qui appartiennent à (A),}\\ &2(0,1)+2(2,1) \quad\quad\ \text{» (B),}\\ &2(0,2)+2(2,2) \quad\quad\ \text{» (C),}\\ &2(0,3)+2(2,3) \quad\quad\ \text{» (D),} \end{aligned}$$

et comme les puissances $\left(\frac{\mu-1}{4}\right)^{\text{ièmes}}$ des nombres de (A), (B), (C), (D) sont respectivement congrues avec $1, i, -1, -i$, on a donc

$$\begin{aligned} \Sigma(z^2+1)^{\frac{\mu-1}{4}} &\equiv 2[(0,0)+(2,0)-(0,2)-(2,2)]\\ &\quad +2i[(0,1)+(2,1)-(0,3)-(2,3)]\\ &\equiv 2(h-k)+2i(j-l), \end{aligned}$$

ou, en introduisant les valeurs du n° 10 et remarquant que $A = a$,

$$\Sigma(z^2+1)^{\frac{\mu-1}{4}} \equiv -a-1-Bi.$$

De la comparaison avec le premier résultat

$$\Sigma(z^2+1)^{\frac{\mu-1}{4}} \equiv -1,$$

il suit

$$a+Bi \equiv 0 \qquad [\mathrm{mod}(M=a+bi)],$$

donc

$$B = b.$$

Par là, les valeurs de h, j, k, l, m du n° 10 se transforment finalement en

$$\begin{aligned} 8h &= 4n-3a-5,\\ 8j &= 4n+a-2b-1,\\ 8k &= 4n+a-1,\\ 8l &= 4n+a+2b-1,\\ 8m &= 4n-a+1, \end{aligned}$$

où $8n+1 = a^2+b^2$ est donc la norme du nombre premier M.

13. Après avoir traité les deux cas dans lesquels $\mu = 8n+1$, il faut maintenant considérer le cas $\mu = 8n+5$.

Puisque $\frac{\mu-1}{4}$ est alors impair, -1 appartient au groupe (C), et, comme il est facile de le voir, les nombres

$$\begin{array}{llll} p-\alpha, & p-\alpha', & p-\alpha'', & \ldots \text{ appartiennent tous à (C),} \\ p-\beta, & p-\beta', & p-\beta'', & \ldots \qquad\quad \text{» (D).} \end{array}$$

Moyennant ces remarques, on reconnaît sans peine que

Le signe	Représente le nombre des solutions de
(0,0)	$\alpha+\gamma+1\equiv 0,$
(0,1)	$\alpha+\delta+1\equiv 0,$
(0,2)	$\alpha+\alpha'+1\equiv 0,$
(0,3)	$\alpha+\beta+1\equiv 0,$
(1,0)	$\beta+\gamma+1\equiv 0,$
(1,1)	$\beta+\delta+1\equiv 0,$
(1,2)	$\beta+\alpha+1\equiv 0,$
(1,3)	$\beta+\beta'+1\equiv 0,$
(2,0)	$\gamma+\gamma'+1\equiv 0,$
(2,1)	$\gamma+\delta+1\equiv 0,$
(2,2)	$\gamma+\alpha+1\equiv 0,$
(2,3)	$\gamma+\beta+1\equiv 0,$
(3,0)	$\delta+\gamma+1\equiv 0,$
(3,1)	$\delta+\delta'+1\equiv 0,$
(3,2)	$\delta+\alpha+1\equiv 0,$
(3,3)	$\delta+\beta+1\equiv 0,$

d'où découlent les six relations

$$\begin{array}{lll} (0,0)=(2,2), & (0,1)=(3,2), & (0,3)=(1,2), \\ (1,0)=(2,3), & (1,1)=(3,3), & (2,1)=(3,0). \end{array}$$

Comme, de même que précédemment, $\alpha\alpha'\equiv\beta\delta\equiv\gamma\gamma'\equiv 1$, on a

$$\begin{array}{l} \gamma'(\alpha+\gamma+1)\equiv\gamma''+1+\gamma', \\ \beta\ (\alpha+\delta+1)\equiv\beta'+1+\beta, \\ \delta\ (\alpha+\beta+1)\equiv\delta'+1+\delta, \\ \delta\ (\beta+\gamma+1)\equiv 1+\beta'+\delta, \\ \gamma'(\beta+\gamma+1)\equiv\delta+1+\gamma', \end{array}$$

d'où l'on conclut

$$\begin{array}{lll} (0,0)=(2,0), & (0,1)=(1,3), & (0,3)=(3,1) \\ & (1,0)=(1,1)=(2,1). & \end{array}$$

Par suite de ces onze relations, le schéma (S) prend cette forme

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

Comme -1 entre dans le groupe (C), donc 0 dans (C'), on trouve, exactement de la même manière qu'au n° 8,

$$h+j+k+l=\frac{\mu-1}{4}=2n+1,$$
$$2m+l+j=2n+1,$$
$$h+m=n.$$

Enfin, la considération du nombre des solutions de la congruence

$$\alpha+\beta+\gamma+1\equiv 0$$

fournit encore une relation entre h, j, k, l, m. Si l'on prend d'abord pour α toutes les valeurs qui appartiennent à (A), il arrive respectivement h, j, k, l fois que $\alpha+1$ appartient aux groupes (A), (B), (C), (D). On trouve en outre, de la même manière qu'au n° 9, que pour chacun de ces cas la congruence a respectivement m, l, j, m solutions, de sorte que le nombre total des solutions est

$$hm+jl+kj+lm.$$

Prend-on, au contraire, d'abord pour β toutes les valeurs (B); alors il arrive respectivement m, m, l, j fois que $\beta+1$ appartient aux groupes (A), (B), (C), (D). Pour chacun de ces cas, on trouve alors que la congruence a respectivement h, m, h, m solutions, ce qui donne pour le nombre total des solutions

$$mh+mm+lh+jm.$$

14. Égalons maintenant entre elles les deux expressions trouvées pour le nombre des solutions de la congruence

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

il vient

$$0=m^2+lh+jm-jl-kj-lm,$$

ou, à cause de la valeur $k=2m-h$, qui résulte immédiatement des rela-

tions linéaires établies entre h, j, k, l, m au n° 13,

$$0 = m^2 + lh + hj - jl - jm - lm.$$

A l'aide de $j + l = 1 + 2h$, on peut exprimer j et l en fonction de leur différence, ce qui donne

$$2j = 1 + 2h + (j - l),$$
$$2l = 1 + 2h - (j - l),$$

et, par l'introduction de ces valeurs dans l'équation précédente, celle-ci se transforme en

$$0 = 4m^2 - 4m - 1 + 4h^2 - 8hm + (j - l)^2,$$

ou, à cause de

$$4m = 2(h + m) - 2(h - m) = 2n - 2(h - m),$$

en

$$0 = 4(h - m)^2 - 2n + 2(h - m) - 1 + (j - l)^2$$

et finalement en

$$\mu = 8n + 5 = [4(h - m) + 1]^2 + 4(j - l)^2;$$

pour

$$\mathrm{A} = 4(h - m) + 1, \qquad \mathrm{B} = 2j - 2l,$$

on a donc

$$\mu = \mathrm{A}^2 + \mathrm{B}^2.$$

Au moyen de A et B il est maintenant facile d'exprimer h, j, k, l, m, de la manière suivante

$$8h = 4n + \mathrm{A} - 1,$$
$$8j = 4n + \mathrm{A} + 2\mathrm{B} + 3,$$
$$8k = 4n - 3\mathrm{A} + 3,$$
$$8l = 4n + \mathrm{A} - 2\mathrm{B} + 3,$$
$$8m = 4n - \mathrm{A} + 1.$$

Reste encore à déterminer A et B. Or μ, nombre premier réel de la forme $4n + 1$, ne peut être représenté que d'une seule manière par la somme de deux carrés, et comme

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

on a

$$\mu = a^2 + b^2,$$

où

$$a \equiv -1, \qquad b \equiv 2 \pmod 4.$$