ARKIV FÖR MATEMATIK Band 3 nr 16

Communiqué le 1 Décembre 1954

Sur quelques problèmes dans la théorie des restes quadratiques et cubiques

Par TRYGVE NAGELL

§ 1.

Soit $\boldsymbol{E}$ un ensemble infini de nombres premiers, et désignons par $A(x)$ le nombre des nombres premiers $\leqq x$ qui appartiennent à $\boldsymbol{E}$. Alors, si $\pi(x)$ désigne le nombre de tous les nombres premiers $\leqq x$, nous dirons que les nombres premiers de $\boldsymbol{E}$ ont la *densité*

$$\lim_{x\to\infty}\frac{A(x)}{\pi(x)}.$$

Si m et r sont deux nombres entiers positifs tels que $(m, r)=1$, il est bien connu que les nombres premiers qui sont $\equiv r \pmod m$, ont la densité $\frac{1}{\varphi(m)}$.

Soit p un nombre premier impair. Désignons par $\psi^*(p; 2)$ le plus petit nombre premier impair qui est un non-reste quadratique modulo p; et désignons par $\pi^*(p; 2)$ le plus petit nombre premier impair qui est un reste quadratique modulo p. Dans des travaux antérieurs j'ai déterminé des bornes supérieures de $\psi^*(p; 2)$ et $\pi^*(p; 2)$ en fonctions de p; voir [1], [2] et [3].[1] Les fonctions $\psi^*(p; 2)$ et $\pi^*(p; 2)$ ne sont pas bornées. En effet, nous avons établi les relations suivantes (voir [4]):

$$\limsup_{p\to\infty}\psi^*(p; 2)=\infty$$

et

$$\limsup_{p\to\infty}\pi^*(p; 2)=\infty.$$

Ces résultats sont contenus dans les suivants qui sont plus généraux:

Théorème 1. *Soit p_n le $n^{\text{ième}}$ nombre premier $(n>1)$. Alors la densité des nombres premiers p ayant la propriété que $\psi^*(p; 2)=p_n$, est égale à $\frac{1}{2^{n-1}}$.*

[1] Les numéros figurant entre crochets renvoient à la Bibliographie placée à la fin de Mémoire.

Théorème 2. *Soit p_n le $n^{ième}$ nombre premier $(n>1)$. Alors la densité des nombres premiers p ayant la propriété que $\pi^*(p; 2)=p_n$, est égale à $\frac{1}{2^{n-1}}$.*

Démonstration de théorème 1. Quand $\psi^*(p; 2)=p_n$, le nombre premier p doit satisfaire aux conditions suivantes

$$\left(\frac{3}{p}\right)=\left(\frac{5}{p}\right)=\cdots=\left(\frac{p_{n-1}}{p}\right)=+1, \quad \left(\frac{p_n}{p}\right)=-1. \tag{1}$$

Ainsi

$$p\equiv\pm 1 \pmod{12}, \quad p\equiv\pm 1 \pmod 5 \text{ etc. ...}$$

Si nous posons $N=3\cdot 5\cdot 7 \ldots p_n$, il est évident qu'il existe $\nu=\frac{\varphi(4N)}{2^{n-1}}$ nombres entiers a_i tels que $0<a_i<4N$ et $(4N, a_i)=1$, et tels que tout nombre premier p satisfaisant aux conditions (1) appartienne à quelqu'une des progressions arithmétiques

$$4Nt+a_1, \ 4Nt+a_2, \ldots, 4Nt+a_\nu.$$

Inversement, tout nombre premier p représentable par l'une de ces progressions satisfait aux conditions (1). Vu que la densité des nombres premiers dans chacune de ces progressions est égale à $\frac{1}{\psi(4N)}$, on voit ainsi que la densité des nombres premiers p est égale à $\frac{1}{2^{n-1}}$.

La démonstration de théorème 2 est tout à fait analogue. Dans ce cas le nombre premier p doit satisfaire aux conditions suivantes

$$\left(\frac{3}{p}\right)=\left(\frac{5}{p}\right)=\cdots=\left(\frac{p_{n-1}}{p}\right)=-1, \quad \left(\frac{p_n}{p}\right)=+1. \tag{2}$$

§ 2.

Dans cette section nous avons besoin du résultat suivant qui est du à LANDAU (voir [5]):

Soit F une forme binaire quadratique de discriminant D et jouissant des propriétés suivantes: Les coefficients sont entiers; F est irréductible et proprement primitive; si $D<0$, F est positive.

Désignons par h le nombre des classes des formes binaires quadratiques, à coefficients entiers, proprement primitives de discriminant D (positives pour $D<0$).

Cela étant, le nombre des nombres premiers représentables par F et $\leqq x$ est égal à

$$\frac{1}{2h}Li(x)+0\left(xe^{-\sqrt[d]{\log x}}\right)$$

pour une classe ambiguë, et égal à

$$\frac{1}{h} Li(x) + 0\left(xe^{-\sqrt[d]{\log x}}\right)$$

pour toute autre classe. d est un constant positif.

Nous allons appliquer ce théorème à quelques questions dans la théorie des restes cubiques.

Tout nombre premier $p \equiv 1 \pmod 6$ peut s'écrire sous la forme

$$p = \tfrac{1}{4}(A^2 + 27B^2), \tag{3}$$

où A et B sont des entiers tels que $A \equiv B \pmod 2$. Dans un travail antérieur (voir [4]) j'ai établi le résultat suivant:

Théorème 3. *Dans la représentation du nombre premier p sous la forme* (3) *tout diviseur premier du produit AB est un reste cubique modulo p.*

Dans cette section les démonstrations reposent sur la théorie du corps quadratique imaginaire $\boldsymbol{K}(\varrho)$ engendré par le nombre $\varrho = \frac{1}{2}(-1+\sqrt{-3})$. Les propriétés des entiers de ce corps sont supposées connues; voir [6], p. 185–195 et p. 223.

Nous commençons par démontrer les théorèmes suivants:

Théorème 4. *La condition nécessaire et suffisante pour que le nombre 2 soit un reste cubique du nombre premier*

$$p = \tfrac{1}{4}(x^2 + 27y^2), \tag{4}$$

est que les nombres entiers x et y soient tous les deux pairs.

La densité des nombres premiers p en question est égale à $\frac{1}{6}$.

Théorème 5. *La condition nécessaire et suffisante pour que le nombre 3 soit un reste cubique du nombre premier* (4), *est que le nombre entier y soit divisible par 3.*

La densité des nombres premiers p en question est égale à $\frac{1}{6}$.

Théorème 6. *La condition nécessaire et suffisante pour que le nombre 5 soit un reste cubique du nombre premier* (4), *est que l'un des nombres entiers x et y soit divisible par 5.*

La densité des nombres premiers en question est égale à $\frac{1}{4}$.

Théorème 7. *La condition nécessaire et suffisante pour que le nombre 7 soit un reste cubique du nombre premier* (4), *est que l'un des nombres entiers x et y soit divisible par 7.*

La densité des nombres premiers en question est égale à $\frac{1}{4}$.

Remarque. Dans la forme $\frac{1}{4}(x^2 + 27y^2)$ qui représente p, les entiers x et y doivent satisfaire à la congruence $x \equiv y \pmod 2$. Pour appliquer le théorème de LANDAU il faut une forme à coefficients entiers. Par la transformation $x = 2u + v$, $y = v$ nous aurons la forme

$$u^2+uv+7v^2$$

avec le discriminant $D=-27$.

Démonstration de théorème 4. Il suit de théorème 3 que la condition est suffisante. Supposons que les nombres x et y dans la représentation (4) de p soient tous les deux impairs. En employant la loi de réciprocité cubique nous aurons alors

$$\varepsilon=\left[\frac{2}{\frac{1}{2}(x+3y\sqrt{-3})}\right]=\left[\frac{\frac{1}{2}(x+3y\sqrt{-3})}{2}\right]=\left[\frac{\frac{1}{2}(\pm 1\pm\sqrt{-3})}{2}\right].$$

Le nombre $\frac{1}{2}(\pm 1\pm\sqrt{-3})$ a l'une des valeurs $\pm\varrho$, $\pm\varrho^2$, où $\varrho=\frac{1}{2}(-1+\sqrt{-3})$. Or, il est évident que

$$\left[\frac{\varrho}{2}\right]=\varrho \quad \text{et} \quad \left[\frac{\varrho^2}{2}\right]=\varrho^2.$$

Donc on a ou $\varepsilon=\varrho$ ou $\varepsilon=\varrho^2$. Ainsi 2 n'est pas un reste cubique de p.

Pour montrer que la densité est égale à $\frac{1}{6}$, on a seulement à appliquer la théorème de LANDAU à la forme u^2+27v^2, ayant le discriminant -108.

Démonstration de théorème 5. D'après le théorème 3 la condition est suffisante. Vu que

$$\left[\frac{3}{\frac{1}{2}(x+3y\sqrt{-3})}\right]=\varrho^{2y}$$

il faut que le nombre y soit divisible par 3. Seulement dans ce cas 3 est un reste cubique de p.

Pour montrer que la densité est $=\frac{1}{6}$ il faut appliquer le théorème de LANDAU à la forme

$$u^2+3uv+63v^2,$$

dont le discriminant a la valeur -243.

Démonstration de théorème 6. D'après le théorème 3 la condition est suffisante. Supposons qu'aucun des nombres x et y ne soit divisible par 5. En employant la loi de réciprocité cubique nous aurons

$$\varepsilon=\left[\frac{5}{\frac{1}{2}(x+3y\sqrt{-3})}\right]=\left[\frac{\frac{1}{2}(x+3y\sqrt{-3})}{5}\right].$$

Si $x\equiv\pm 1 \pmod 5$ et $y\equiv\pm 1 \pmod 5$, on aura

$$\varepsilon=\left[\frac{5}{\frac{1}{2}(\pm 1\pm 3\sqrt{-3})}\right].$$

Or, on vérifie aisément que 5 n'est pas un reste cubique de 7.

Si $x\equiv\pm 1 \pmod 5$ et $y\equiv\pm 2 \pmod 5$, on aura

$$\varepsilon = \left[\frac{\pm 3 \pm 3\sqrt{-3}}{5}\right] = \left[\frac{\varrho^s}{5}\right],$$

où $s = 1$ ou $= 2$. Or, il est évident qu'aucun des nombres ϱ et ϱ^2 n'est un reste cubique de 5.

Si $x \equiv \pm 2 \pmod 5$ et $y \equiv \pm 1 \pmod 5$, on aura

$$\varepsilon = \left[\frac{\frac{1}{2}(\pm 3 \pm 3\sqrt{-3})}{5}\right] = \left[\frac{\varrho^s}{5}\right],$$

où $s = 1$ ou $= 2$. Ainsi on conclut comme dans le cas précédent.

Si $x \equiv \pm 2 \pmod 5$ et $y \equiv \pm 2 \pmod 5$, on aura

$$\varepsilon = \left[\frac{5}{\frac{1}{2}(\pm 1 \pm 3\sqrt{-3})}\right].$$

Or, il est évident que 5 n'est pas un reste cubique de 7.

On trouve aisément à l'aide du théorème de LANDAU que la densité est $= \frac{1}{4}$. On l'appliquera aux formes

$$13u^2 + uv + 25v^2 \quad \text{et} \quad u^2 + uv + 169v^2,$$

qui ont toutes les deux le discriminant -675.

Démonstration de théorème 7. D'après le théorème 3 la condition est suffisante. Supposons qu'aucun des nombres x et y ne soit divisible par 7. A l'aide de la loi de réciprocité cubique nous aurons

$$\varepsilon = \left[\frac{7}{\frac{1}{2}(x+3y\sqrt{-3})}\right] = \left[\frac{\frac{1}{2}(1+3\sqrt{-3})}{\frac{1}{2}(x+3y\sqrt{-3})}\right]\left[\frac{\frac{1}{2}(1-3\sqrt{-3})}{\frac{1}{2}(x+3y\sqrt{-3})}\right]$$

$$= \left[\frac{\frac{1}{2}(x+3y\sqrt{-3})}{\frac{1}{2}(1+3\sqrt{-3})}\right]\left[\frac{\frac{1}{2}(x+3y\sqrt{-3})}{\frac{1}{2}(1-3\sqrt{-3})}\right] = \left[\frac{\frac{1}{2}(x+3y\sqrt{-3})}{\frac{1}{2}(1+3\sqrt{-3})}\right]\left[\frac{\frac{1}{2}(x-3y\sqrt{-3})}{\frac{1}{2}(1+3\sqrt{-3})}\right]^2$$

$$= \left[\frac{p}{\frac{1}{2}(1+3\sqrt{-3})}\right]\left[\frac{\frac{1}{2}(x-3y\sqrt{-3})}{\frac{1}{2}(1+3\sqrt{-3})}\right] = \left[\frac{p}{\frac{1}{2}(1+3\sqrt{-3})}\right]\left[\frac{\frac{1}{2}(x+y)}{\frac{1}{2}(1+3\sqrt{-3})}\right].$$

On ne peut pas avoir $x \equiv \pm y \pmod 7$, comme p n'est pas divisible par 7. Il faut distinguer six cas.

Si $x \equiv \pm 1$ et $y \equiv \pm 2 \pmod 7$, nous aurons $\frac{1}{2}(x+y) \equiv \pm 4$ ou $\equiv \pm 2 \pmod 7$ et $p \equiv 1 \pmod 7$. Donc

$$\varepsilon = \left[\frac{2^s}{\frac{1}{2}(1+3\sqrt{-3})}\right],$$

où $s = 1$ ou $= 2$. Mais les nombres 2 et 4 ne sont pas restes cubiques de 7.

Si $x \equiv \pm 1$ et $y \equiv \pm 3 \pmod 7$, nous aurons $\frac{1}{2}(x+y) \equiv \pm 1$ ou $\equiv \pm 2 \pmod 7$ et $p \equiv -2 \pmod 7$. Donc ε aura la même valeur que dans le ces précédent, et ainsi $\varepsilon \neq 1$.

Si $x \equiv \pm 2$ et $y \equiv \pm 1 \pmod 7$, nous aurons $\frac{1}{2}(x+y) \equiv \pm 2$ ou $\equiv \pm 4 \pmod 7$ et $p \equiv -1 \pmod 7$. Comme dans le premier cas nous voyons donc que $\varepsilon \neq 1$.

Si $x \equiv \pm 2$ et $y \equiv \pm 3 \pmod 7$, nous aurons $\frac{1}{2}(x+y) \equiv \pm 1$ ou $\equiv \pm 4 \pmod 7$ et $p \equiv 4 \pmod 7$. Donc $\varepsilon \neq 1$.

Si $x \equiv \pm 3$ et $y \equiv \pm 1 \pmod 7$, nous aurons $\frac{1}{2}(x+y) \equiv \pm 1$ ou $\equiv \pm 2 \pmod 7$ et $p \equiv 2 \pmod 7$. Donc $\varepsilon \neq 1$.

Si $x \equiv \pm 3$ et $y \equiv \pm 2 \pmod 7$, nous aurons $\frac{1}{2}(x+y) \equiv \pm 4$ ou $\equiv \pm 1 \pmod 7$ et $p \equiv -4 \pmod 7$. Donc $\varepsilon \neq 1$.

Cela démontre la première partie du théorème 7. La seconde partie est une conséquence du théorème de LANDAU. Il faut l'appliquer aux formes

$$u^2 + uv + 331\,v^2 \quad \text{et} \quad 9\,u^2 + uv + 49\,v^2,$$

qui ont toutes les deux le discriminant -1323.

Des théorèmes 4–7 nous aurons évidemment aussi les conditions nécessaires et suffisantes pour qu'un quelconque des nombres 2, 3, 5 ou 7 soit un non-reste cubique d'un nombre premier p représenté par (4). Il faut observer que tout nombre entier, non divisible par p, est un reste cubique d'un nombre premier $\equiv -1 \pmod 3$. Nous aurons spécialement:

Théorème 8. *Les nombres premiers dont le nombre* 2 *est un non-reste cubique, ont la densité* $\frac{1}{3}$.

Les nombres premiers dont le nombre 3 *est un non-reste cubique, ont la densité* $\frac{1}{3}$.

Les nombres premiers dont le nombre 5 *est un non-reste cubique, ont la densité* $\frac{1}{4}$.

Les nombres premiers dont le nombre 7 *est un non-reste cubique, ont la densité* $\frac{1}{4}$.

Dans le théorème 7, on ne peut pas remplacer le nombre 7 par 11. En effet, on vérifie aisément que le nombre 11 est un reste cubique du nombre premier 19 quoique celui-ci ait la représentation $19 = \frac{1}{4}(7^2 + 27)$.

Soit p un nombre premier > 3, et soit n un nombre entier impair $\geqq 3$, tel que le plus grand commun diviseur de n et $p-1$ soit > 1. Désignons par $\psi(p; n)$ le plus petit nombre premier qui est un non-reste $n^{\text{ième}}$ modulo p; et désignons par $\pi(p; n)$ le plus petit nombre premier qui est un reste $n^{\text{ième}}$ modulo p. Dans un travail antérieur j'ai donné des bornes supérieures de $\psi(p; n)$ et de $\pi(p; 3)$ en fonctions de p; voir [4]. Nous avons aussi établi les relations suivantes

$$\limsup_{p \to \infty} \psi(p; 3) = \infty \tag{5}$$

et

$$\limsup_{p \to \infty} \pi(p; 3) = \infty. \tag{6}$$

Nous allons y ajouter les résultats plus généraux que voici:

Théorème 9. *Il y a une infinité de nombres premiers* p *tels que le nombre* $\psi(p; 3)$ *soit égal à un nombre premier* r *donné d'avance. La densité de ces nombres premiers* p *est positive.*

Théorème 10. *Il y a une infinité de nombres premiers* $p \equiv 1 \pmod 6$ *tels que le nombre* $\pi(p; 3)$ *soit égal à un nombre premier* r *donné d'avance. La densité de ces nombres premiers* p *est positive.*

Démonstration de théorème 9. Pour $r=2$ le théorème est une conséquence de théorème 8; la densité est $=\frac{1}{3}$. Il suit des théorèmes 4 et 5 que les nombres premiers p pour lesquels $\psi(p; 3)=3$ sont ceux qui ont la représentation

$$p = u^2 + 27 v^2,$$

où v n'est pas divisible par 3. La densité de ces nombres premiers est évidemment positive. En effet, la forme u^2+27v^2 sera transformée par la transformation $u=3u_1+v_1$, $v=v_1$ en la forme

$$9u_1^2 + 6u_1v_1 + 28v_1^2.$$

Quand celle-ci représente un nombre premier, v_1 n'est pas divisible par 3. Donc la valeur corréspondante de v n'est pas divisible par 3 non plus.

Ainsi nous pouvons supposer $r \geqq 5$. Choisissons le nombre premier p tel que

$$p = x^2 + 27 Q^2 y^2, \tag{7}$$

où x et y sont des entiers rationnels, et où Q est le produit de tous les nombres premiers $<r$. En vertu de théorème 3 tous les nombres premiers $<r$ sont des restes cubiques modulo p. Soit $p=\omega\omega'$ la décomposition de p en nombres premiers primaires en $\boldsymbol{K}(\varrho)$ et

$$\omega = x + 3Qy\sqrt{-3}.$$

Supposons d'abord que $r \equiv -1 \pmod 6$. Alors nous aurons par la loi de réciprocité cubique

$$\left[\frac{r}{\omega}\right] = \left[\frac{\omega}{r}\right] = \left[\frac{x+3Qy\sqrt{-3}}{r}\right]. \tag{8}$$

Soit μ un non-reste cubique de r dans $\boldsymbol{K}(\varrho)$. Vu que 2 est un reste cubique de r, on peut supposer que $\mu = c + d\sqrt{-3}$, où c et d sont des entiers rationnels. Déterminons le nombre entier rationnel b tel que $3Qb \equiv d \pmod r$ et puis le nombre entier rationnel a tel que $a \equiv c \pmod r$ et tel que $a \equiv 1 \pmod{Qb}$. Cela est possible vu que aucun des nombres $3Q$, d et b n'est divisible par r. Alors le nombre $\alpha = a + 3Qb\sqrt{-3}$ est un non-reste cubique de r dans $\boldsymbol{K}(\varrho)$. La forme $x^2+27Q^2y^2$ sera transformée par la transformation

$$x = au + rv, \quad y = bu + rv$$

en la forme

$$(a^2 + 27Q^2b^2)u^2 + (2ar + 54brQ^2)uv + 27Q^2r^2v^2. \tag{9}$$

Cette forme est primitive puisque $(a, 3Qb)=1$. Elle représente p, et alors u n'est pas divisible par r. Il suit de (8) que

$$\left[\frac{x+3Qy\sqrt{-3}}{r}\right]=\left[\frac{u(a+3Qb\sqrt{-3})}{r}\right]=\left[\frac{\alpha}{r}\right]\neq 1.$$

Pour tous les nombres premiers p représentables par la forme (9) on a donc

$$\psi(p;\,3)=r.$$

D'après la théorème de LANDAU cette forme représente une infinité de nombres premiers dont la densité est positive.

Supposons ensuite que $r\equiv 1 \pmod 6$. Soit $r=\alpha\alpha'$ la décomposition de r en nombres premiers primaires en $\boldsymbol{K}(\varrho)$. Alors nous aurons par la loi de réciprocité cubique

$$\left[\frac{r}{\omega}\right]=\left[\frac{\alpha}{\omega}\right]\left[\frac{\alpha'}{\omega}\right]=\left[\frac{\omega}{\alpha}\right]\left[\frac{\omega}{\alpha'}\right]=\left[\frac{\omega}{\alpha}\right]\left[\frac{\omega'}{\alpha}\right]^2. \tag{10}$$

Soit μ un non-reste cubique modulo α et ν un reste cubique modulo α'. Soit ξ un entier déterminé par les congruences

$$\xi\equiv\mu \pmod\alpha,\quad \xi\equiv\nu \pmod{\alpha'}.$$

Supposons que $\xi=\frac{1}{2}(c+d\sqrt{-3})$, où c et d sont des entiers rationnels. Déterminons le nombre entier rationnel b tel que $6Qb\equiv d \pmod r$, et puis le nombre entier rationnel a tel que $2a\equiv c \pmod r$ et $a\equiv 1 \pmod{Qb}$. Cela est possible puisque aucun des nombres $6Q$, d et b n'est divisible par r. Alors le nombre $\beta=a+3Qb\sqrt{-3}$ est un non-reste cubique modulo α et un reste cubique modulo α' dans $\boldsymbol{K}(\varrho)$. La forme $x^2+27Q^2y^2$ sera transformée par la transformation

$$x=au+rv,\quad y=bu+rv$$

en la forme (9). Cette forme est primitive comme $(a, 3Qb)=1$. Elle représente p, et alors u n'est pas divisible par r. Il suit de (10) que

$$\left[\frac{\omega}{\alpha}\right]\left[\frac{\omega'}{\alpha}\right]^2=\left[\frac{u(a+3Qb\sqrt{-3})}{\alpha}\right]\left[\frac{u(a-3Qb\sqrt{-3})}{\alpha}\right]^2=\left[\frac{\beta}{\alpha}\right]\left[\frac{\beta'}{\alpha}\right]\neq 1.$$

Donc, pour tous les nombres premiers p représentables par la forme (9) on a donc

$$\psi(p;\,3)=r.$$

D'après le théorème de LANDAU cette forme représente une infinité de nombres premiers dont la densité est positive.

Le théorème 9 se trouve ainsi démontré.

Démonstration de théorème 10. Pour $r=2$ le théorème est une conséquence de théorème 8; la densité est $=\frac{1}{4}$. Il suit des théorèmes 4 et 5 que les nombres premiers p pour lesquels $\pi(p;3)=3$ sont ceux qui ont la représentation

$$p=\tfrac{1}{4}(a^2+243\,y^2),$$

où les nombres x et y sont impairs. La densité de ces nombres premiers est évidemment positive. En effet, la forme $\frac{1}{4}(x^2+243\,y^2)$ sera transformée par la transformation $x=4\,u+v$, $y=v$, en la forme

$$4\,u^2+2\,u\,v+61\,v^2.$$

Quand celle-ci représente un nombre premier, v est impair. Donc les valeurs corréspondantes de x et y sont aussi impaires.

Ainsi nous pouvons supposer $r\geqq 5$. Désignons par $3\,Q$ le produit de tous les nombres premiers $<r$. Soient $q_1, q_2, \ldots, q_t$ tous les nombres premiers $\equiv -1 \pmod 3$ qui sont $<r$. Désignons par $f_1, f_2, \ldots, f_s$ tous les nombres premiers $\equiv 1 \pmod 3$ qui sont $<r$. Soit $f_i=\alpha_i\,\alpha_i'$ la décomposition de f_i en nombres premiers primaires dans le corps $\boldsymbol{K}(\varrho)$. Si $r\equiv 1 \pmod 6$, nous supposons que $r=\beta\,\beta'$ soit la décomposition de r en nombres premiers primaires dans $\boldsymbol{K}(\varrho)$.

Choisissons les nombres μ_i, ν_i, τ_j et σ de la manière suivante:

μ_i est un reste cubique modulo α_i dans $\boldsymbol{K}(\varrho)$, pour $i=1, 2, \ldots, s$.
ν_i est un non-reste cubique modulo α_i' dans $\boldsymbol{K}(\varrho)$, pour $i=1, 2, \ldots, s$.
τ_j est un non-reste cubique modulo q_j dans $\boldsymbol{K}(\varrho)$, pour $j=1, 2, \ldots, t$.
σ est un reste cubique modulo r dans $\boldsymbol{K}(\varrho)$ quand $r\equiv -1 \pmod 6$,
σ est un reste cubique modulo chacun des nombres β et β' dans $\boldsymbol{K}(\varrho)$ quand $r\equiv 1 \pmod 6$.

L'existence des nombres μ_i, ν_i, τ_j et σ se vérifie sans peine par la théorie du corps $\boldsymbol{K}(\varrho)$.

Alors il est évident que le système des $2s+t+1$ congruences simultanées

$$\begin{cases} \xi\equiv\mu_i \pmod{\alpha_i}, & (i=1, 2, \ldots, s), \\ \xi\equiv\nu_i \pmod{\alpha_i'}, & (i=1, 2, \ldots, s), \\ \xi\equiv\tau_j \pmod{q_j}, & (j=1, 2, \ldots, t), \\ \xi\equiv\sigma \pmod{r}, \end{cases} \tag{11}$$

admet une solution ξ modulo $Q\,r$ dans $\boldsymbol{K}(\varrho)$. Car les modules sont premiers entr'eux deux à deux.

En employant le symbole d'Eisenstein nous avons donc

$$\left[\frac{\xi}{\alpha_i}\right]=1, \quad \left[\frac{\xi}{\alpha_i'}\right]\neq 1, \quad \left[\frac{\xi}{q_j}\right]\neq 1. \tag{12}$$

Nous pouvons supposer que le nombre ξ ne soit pas divisible par $\sqrt{-3}$. En effet, si ξ est divisible par $\sqrt{-3}$, le nombre $\xi+Q\,r$ est une autre solution du

système (11) qui n'est pas divisible par $\sqrt{-3}$. Si $\xi = \frac{1}{2}(a_1 + b_1\sqrt{-3})$, où a_1 et b_1 sont des entiers rationnels, on peut supposer que b_1 soit divisible par 3 et non par 9. En effet, soit c un nombre entier rationnel tel que

$$b_1 + 2Qrc \equiv 3 \pmod 9.$$

Ce nombre c existe, vu que Q n'est pas divisible par 3. Alors, le nombre

$$\xi + Qrc\sqrt{-3} = \tfrac{1}{2}\left(a_1 + (b_1 + 2Qrc\sqrt{-3})\right)$$

est une solution du système (11) telle que $b_1 + 2Qrc$ soit divisible par 3 et non par 9. Par conséquent, nous pouvons supposer que

$$\xi = \tfrac{1}{2}(a + 3b\sqrt{-3}), \tag{13}$$

où a et b sont des entiers rationnels, tels que ab ne soit pas divisible par 3.

Considérons maintenant la forme quadratique en u et v

$$\tfrac{1}{4}[(au + 3Qrv)^2 + 27(bu + 3Qrv)^2]. \tag{14}$$

Cette forme représente une infinité de nombres premiers, quand u et v prennent des valeurs entières. La densité de ces nombres premiers est positive (théorème de LANDAU).

Soit p un de ces nombres premiers, et soit $p = \omega\omega'$ la décomposition de p en nombres premiers primaires, donc

$$\omega = \tfrac{1}{2}(au + 3Qrv + (3bu + 9Qrv)\sqrt{-3}).$$

Quand q_j est un nombre premier $\equiv -1 \pmod 3$, nous aurons à l'aide de la loi de réciprocité cubique

$$\left[\frac{q_j}{\omega}\right] = \left[\frac{\omega}{q_j}\right],$$

d'où, vu que Q est divisible par q_j,

$$\left[\frac{\omega}{q_j}\right] = \left[\frac{\xi u}{q_j}\right] = \left[\frac{\xi}{q_j}\right].$$

D'après (8) le dernier symbole a une valeur $\neq 1$. Il en résulte que le nombre premier q_j est un non-reste cubique modulo ω et donc aussi modulo p.

Soit f_i un nombre premier $\equiv 1 \pmod 3$, et soit $f_i = \alpha_i\alpha_i'$ la décomposition comme ci-dessus. D'après la loi de réciprocité cubique on aura alors

$$\left[\frac{f_i}{\omega}\right] = \left[\frac{\alpha_i}{\omega}\right]\left[\frac{\alpha_i'}{\omega}\right] = \left[\frac{\omega}{\alpha_i}\right]\left[\frac{\omega}{\alpha_i'}\right].$$

Q étant divisible par f_i il vient

$$\left[\frac{\omega}{\alpha_i}\right]\left[\frac{\omega}{\alpha_i'}\right] = \left[\frac{\xi u}{\alpha_i}\right]\left[\frac{\xi u}{\alpha_i'}\right] = \left[\frac{\xi}{\alpha_i}\right]\left[\frac{\xi}{\alpha_i'}\right]\left[\frac{u}{\alpha_i}\right]\left[\frac{u}{\alpha_i}\right]^2 = \left[\frac{\xi}{\alpha_i}\right]\left[\frac{\xi}{\alpha_i'}\right].$$

D'après (8) le symbole $\left[\frac{\xi}{\alpha_i}\right]$ a la valeur 1, tandis que le symbole $\left[\frac{\xi}{\alpha_i'}\right]$ est $\neq 1$. Il en résulte que le nombre premier f_i est un non-reste cubique modulo ω et donc aussi modulo p.

De plus, il est facile de voir que le nombre 3 est aussi un non-reste cubique modulo p. En effet, on a

$$\left[\frac{3}{\omega}\right] = \varrho^{2bu+6Qrv} = \varrho^{2bu} \neq 1.$$

Car, le nombre b dans (13) n'est pas divisible par 3, et il est évident que le nombre u ne l'est non plus.

Supposons ensuite que $r \equiv -1 \pmod 6$. Dans ce cas on aura, d'après (8)

$$\left[\frac{r}{\omega}\right] = \left[\frac{\omega}{r}\right] = \left[\frac{\xi u}{r}\right] = \left[\frac{\xi}{r}\right] = 1.$$

Finalement, soit $r \equiv 1 \pmod 6$ et $r = \beta\beta'$. Dans ce cas on aura

$$\left[\frac{r}{\omega}\right] = \left[\frac{\beta}{\omega}\right]\left[\frac{\beta'}{\omega}\right] = \left[\frac{\omega}{\beta}\right]\left[\frac{\omega}{\beta'}\right] = \left[\frac{\xi u}{\beta}\right]\left[\frac{\xi u}{\beta'}\right] = \left[\frac{\xi}{\beta}\right]\left[\frac{u}{\beta}\right]\left[\frac{\xi}{\beta'}\right]\left[\frac{u}{\beta}\right]^2 = \left[\frac{\xi}{\beta}\right]\left[\frac{\xi}{\beta'}\right] = 1,$$

vu que, d'après (8), les symboles $\left[\frac{\xi}{\beta}\right]$ et $\left[\frac{\xi}{\beta'}\right]$ ont la valeur 1.

Par conséquent, le nombre r est toujours un reste cubique modulo ω, et donc aussi modulo p.

Il résulte de ce qui précède que tous les nombres premiers rationnels $< r$ sont des non-restes cubiques modulo p, tandis que r est un reste cubique modulo p. Donc, on a

$$\pi(p; 3) = r.$$

Le théorème 10 se trouve ainsi démontré.

Dans la démonstration des théorèmes 9 et 10 nous nous sommes contentés de montrer que la densité des nombres premiers en question est positive. Il serait naturellement possible, par un perfectionnement de la méthode, de déterminer de la valeur exacte de la densité.

Table des nombres $\psi(p; 3)$ et $\pi(p; 3)$ pour les nombres premiers $p \equiv 1 \pmod 6$ qui sont < 200; a et b sont les entiers dans la représentation $p = \frac{1}{4}(a^2 + 27b^2)$.

p	ψ	π	a	b
7	2	13	1	1
13	2	5	5	1
19	2	7	7	1
31	3	2	4	2
37	2	11	11	1
43	3	2	8	2
61	2	3	1	3
67	2	3	5	3
73	2	3	7	3
79	2	17	17	1
97	2	19	19	1
103	2	3	13	3
109	3	2	2	4
127	3	2	20	2
139	2	23	23	1
151	2	3	19	3
157	3	2	14	4
163	2	5	25	1
181	2	5	7	5
193	2	3	23	3
199	2	5	11	5

Remarque. Les théorèmes 9 et 10 sont aussi vrais pour les restes et les non-restes biquadratiques. J'en publierai bientôt les démonstrations. Probablement on pourrait aussi étendre ces résultats aux restes et non-restes $n^{\text{ièmes}}$ quand $n \geqq 5$.

INDEX BIBLIOGRAPHIQUE

1. T. NAGELL, Zahlentheoretische Notizen. Videnskr. selsk. Skrifter, Matem.-naturv. Kl., Oslo 1913, No 13, IV.
2. ——, Sur les restes et les non-restes quadratiques suivant un module premier. Arkiv f. Matematik, Bd 1, Nr 16, Stockholm 1950.
3. ——, Sur le plus petit non-reste quadratique impair. Arkiv f. Matematik, Bd 2, Nr 2, Stockholm 1951.
4. ——, Sur les restes et les non-restes cubiques, Arkiv f. Matematik, Bd 1, Nr 39, Stockholm 1951.
5. E. LANDAU, Über die Verteilung der Primediale in den Idealklassen eines algebraischen Zahlkörpers. Mathem. Annalen Bd. 63, 1907.
6. P. BACHMANN, Die Lehre von der Kreistheilung. Leipzig 1872.

Tryckt den 20 april 1955

Uppsala 1955. Almqvist & Wiksells Boktryckeri AB