ARKIV FÖR MATEMATIK Band 1 nr 39

Communiqué le 12 septembre 1951

Sur les restes et les non-restes cubiques

Par TRYGVE NAGELL

§ 1.

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

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

où A et B sont des entiers tels que $A \equiv B \pmod 2$. Dans un travail publié en 1923 (voir [1]) j'ai établi le résultat suivant:

Théorème 1. *Dans la représentation du nombre premier p sous la forme* (1) *tout diviseur premier du produit AB est un reste cubique modulo p.*

Comme ce résultat paraît d'être resté inaperçu, j'y en reproduis la démonstration. Celle-ci repose sur la théorie du corps quadratique imaginaire $\boldsymbol{K}(\varrho)$ engendré par le nombre $\varrho = \tfrac{1}{2}(-1+\sqrt{-3})$. Les propriétés des entiers de ce corps sont supposées connues; voir [2], p. 185–195 et p. 223.

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

$$\omega = \tfrac{1}{2}(A + 3\,B\sqrt{-3}).$$

Désignons par q un nombre premier rationnel qui divise ou A ou B. Alors, pour établir le théorème 1 il faut montrer qu'on ait

$$q^{\frac{1}{3}(p-1)} \equiv 1 \pmod p,$$

ou, ce qui est la même chose,

$$q^{\frac{1}{3}(p-1)} \equiv 1 \pmod \omega.$$

Si nous introduisons le symbole d'Eisenstein pour le caractère cubique, il faut donc que

$$\left[\frac{q}{\omega}\right] = 1.$$

Nous distinguirons quatre cas.

1) Quand $q \equiv -1 \pmod 6$, nous aurons en employant la loi de réciprocité cubique

$$\left[\frac{q}{\omega}\right] = \left[\frac{\omega}{q}\right] = \left[\frac{\tfrac{1}{2}(A + 3\,B\sqrt{-3})}{q}\right].$$

Si A est divisible par q, il en résulte que

$$\left[\frac{q}{\omega}\right] = \left[\frac{12B\sqrt{-3}}{q}\right] = \left[\frac{-4B(\sqrt{-3})^3}{q}\right] = \left[\frac{-4B}{q}\right] = 1.$$

Si B est divisible par q, il vient

$$\left[\frac{q}{\omega}\right] = \left[\frac{4A}{\omega}\right] = 1.$$

En effet, si m est rationnel et premier à q, et si $q \equiv -1 \pmod 3$, on a

$$\left[\frac{m}{q}\right] \equiv m^{\frac{1}{3}(q^2-1)} \equiv \left(m^{\frac{q+1}{3}}\right)^{q-1} \equiv 1 \pmod q.$$

2) Quand $q = 2$, nous aurons à l'aide de la loi de réciprocité cubique

$$\left[\frac{2}{\omega}\right] = \left[\frac{\omega}{2}\right] = \left[\frac{\frac{1}{2}(A + 3B\sqrt{-3})}{2}\right] = \left[\frac{\frac{1}{2}(A + 3B)}{2}\right] = 1.$$

Car A et B sont tous les deux pairs; et vu que p est impair, le nombre $\frac{1}{2}(A + 3B)$ l'est aussi.

3) Soit $q \equiv 1 \pmod 6$, et soit $q = \alpha\alpha'$ la décomposition de q en nombres premiers primaires. D'après la loi de réciprocité cubique on aura alors

$$\left[\frac{q}{\omega}\right] = \left[\frac{\alpha}{\omega}\right]\left[\frac{\alpha'}{\omega}\right] = \left[\frac{\omega}{\alpha}\right]\left[\frac{\omega}{\alpha'}\right].$$

Si A est divisible par q, il en résulte que

$$\left[\frac{q}{\omega}\right] = \left[\frac{12B\sqrt{-3}}{\alpha}\right]\left[\frac{12B\sqrt{-3}}{\alpha'}\right] = \left[\frac{12B\sqrt{-3}}{\alpha}\right]\left[\frac{12B\sqrt{-3}}{\alpha}\right]^2 = 1.$$

Si B est divisible par q, il s'ensuit que

$$\left[\frac{q}{\omega}\right] = \left[\frac{4A}{\alpha}\right]\left[\frac{4A}{\alpha'}\right] = \left[\frac{4A}{\alpha}\right]\left[\frac{4A}{\alpha}\right]^2 = 1.$$

Car, pour tout m rationnel et premier à q on a évidemment

$$\left[\frac{m}{\alpha'}\right] = \left[\frac{m}{\alpha}\right]^2.$$

4) Quand $q = 3$, le nombre B est divisible par 3, et on aura

$$\left[\frac{3}{\omega}\right] = \varrho^{2B} = 1.$$

Le théorème 1 se trouve ainsi démontré.

*

Quand p est un nombre premier impair, nous désignons par $\pi(p; 3)$ le plus petit nombre premier qui est un reste cubique modulo p. Si p est $\equiv -1 \pmod 6$, tout nombre entier est un reste cubique modulo p; donc on a dans ce cas $\pi(p; 3) = 2$. Du théorème 1 il suit immédiatement:

Théorème 2. *Quand le nombre premier p est $\equiv 1 \pmod 6$, on a l'inégalité*

$$\pi(p; 3) \leqq \sqrt{4p - 27}, \tag{2}$$

sauf pour $p = 7$. Pour les p qui ne sont pas de la forme $\frac{1}{4}(A^2 + 27)$, cette inégalité peut être remplacée par la suivante:

$$\pi(p; 3) \leqq \sqrt{\tfrac{1}{27}(4p - 1)}. \tag{3}$$

On a p. ex. $\pi(13; 3) = 5$, $\pi(19; 3) = 7$, $\pi(31; 3) = 2$, $\pi(37; 3) = 11$, $\pi(43; 3) = 2$.

§ 2.

Quand p est un nombre premier impair $\equiv 1 \pmod 6$, nous désignons par $\psi(p; 3)$ le plus petit nombre positif qui est un non-reste cubique modulo p. C'est évident que $\psi(p; 3)$ est toujours un nombre premier; dans ce qui suit nous écrirons pour abréger ψ.

Supposons d'abord que $\psi > 2$. En divisant p par 2ψ nous aurons

$$p = 2\psi h \pm r, \tag{4}$$

où h est un entier positif, et où r est un entier impair positif $\leqq \psi - 2$. Il en résulte que r est un reste cubique modulo p. Vu que les nombres 2 et -1 sont des restes cubiques modulo p, il faut que h soit un non-reste cubique modulo p. Nous ne pouvons pas avoir $h = \psi$, puisque ψ^2 n'est pas un reste cubique. Vu que $\frac{1}{2}(\psi + 1)$ est $< \psi$, ce nombre est un reste cubique modulo p, et ainsi h ne peut pas être $= \psi + 1$. Par conséquent, on a $h \geqq \psi + 2$, et il suit de (4) que

$$p \geqq 2\psi(\psi + 2) - \psi + 2 = 2\psi^2 + 3\psi + 2.$$

En posant

$$p = 2\psi^2 + 3\psi + 2 + 2a, \tag{5}$$

où a est un entier $\geqq 0$, nous aurons

$$p - (2a + 7)\psi = 2(\psi - 1)(\psi - a - 1).$$

Si nous supposons que $a + 1 < \psi$, le second membre de cette égalité est un reste cubique modulo p. Il faut donc que $(2a + 7)\psi$ soit un reste cubique modulo p. Ainsi $2a + 7$ est nécessairement un non-reste cubique $\geqq \psi + 2$. Alors l suit de (5) que

$$p \geqq 2\psi^2 + 4\psi - 3,$$

d'où

$$\psi \leqq -1 + \sqrt{\tfrac{1}{2}(p + 5)}.$$

Cette inégalité est aussi valable pour $\psi = 2$, si $p \geqq 13$. Ainsi nous avons le résultat suivant:

Théorème 3. *Quand le nombre premier p est $\equiv 1$ (mod 6), nous avons l'inégalité*

$$\psi(p; 3) \leqq -1 + \sqrt{\tfrac{1}{2}(p + 5)}, \tag{6}$$

sauf pour $p = 7$.

On a p. ex. $\psi(13; 3) = 2$, $\psi(19; 3) = 2$, $\psi(31; 3) = 3$, $\psi(37; 3) = 2$, $\psi(43; 3) = 3$.

*

On voit sans peine que la même méthode de démonstration que ci-dessus nous donnera le résultat plus général suivant:

Théorème 4. *Soit p un nombre premier $\geqq 13$, et soit n un nombre entier impair $\geqq 3$, tel que le plus grand commun diviseur de n et $p - 1$ soit > 1. Alors, si $\psi(p; n)$ désigne le plus petit nombre positif qui est un non-reste $n^{ième}$ modulo p, nous avons l'inégalité*

$$\psi(p; n) \leqq -1 + \sqrt{\tfrac{1}{2}(p + 5)}.$$

Un résultat plus précis a été trouve par J. M. VINOGRADOV par des moyens analytiques; voir [3]. Voir aussi les travaux de H. J. KANOLD [4] et [5].

§ 3.

Soit p un nombre premier impair. Désignons par $\psi(p; 2)$ le plus petit nombre premier qui est un non-reste quadratique modulo p; et désignons par $\pi(p; 2)$ le plus petit nombre premier qui est un reste quadratique modulo p. Dans des travaux antérieurs j'ai déterminé des bornes supérieures de $\psi(p; 2)$ et de $\pi(p; 2)$ en fonctions de p; voir [1], [6] et [7]. Cependant, les fonctions $\psi(p; 2)$ et $\pi(p; 2)$ ne sont pas bornées. En effet, nous allons établir les résultats suivants:

Théorème 5.

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

Théorème 6.

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

Démonstration. Soit t un nombre positif quelconque, et désignons par Q le produit de tous les nombres premiers impairs $\leqq t$. Soit p un nombre premier tel que $p \equiv 1 \pmod{8\,Q}$. Alors, si q est un diviseur premier de Q, on a

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = +1.$$

Le nombre 2 est aussi un reste quadratique modulo p. Donc on a $\psi(p; 2) > t$, ce qui démontre le théorème 5.

Pour démontrer le théorème 6 nous choisissons un nombre premier p tel qu'on ait

$$p \equiv 5 \pmod 8 \text{ et } p \equiv h_q \pmod q \tag{7}$$

pour tous les diviseurs premiers q de Q; ici h_q est un non-reste quadratique modulo q. L'existence d'un nombre premier p qui satisfait au système des congruences (7) est assurée par le théorème de Dirichlet sur la progression arithmétique. Alors on a

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{h_q}{q}\right) = -1.$$

Donc tous les nombres premiers $\leqq t$ sont des non-restes quadratiques modulo p. Ainsi nous avons $\pi(p; 2) > t$, ce qui démontre le théorème 6.

Comme corollaire du théorème 5 nous avons le

Théorème 7. *Si $g(p)$ désigne la plus petite racine primitive positive du module premier p, on a*

$$\limsup_{p\to\infty} g(p) = \infty.$$

En effet, le nombre $g(p)$ est un non-reste quadratique modulo p. Donc on a $g(p) \geqq \psi(p; 2)$.

§ 4.

Pour les non-restes cubiques nous avons le résultat analogue au théorème 5:

Théorème 8.

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

Démonstration. Si t est un nombre positif quelconque, nous désignons par Q le produit de tous les nombres premiers $\leqq t$. Considérons la forme quadratique en u et v

$$u^2 + 27\,Q^2 v^2.$$

Il est bien connu que cette forme représente une infinité de nombres premiers quand u et v prennent des valeurs entières; voir [8]. Soit p un de ces nombres premiers. Alors, en vertu du théorème 1 tout diviseur premier de Q est un reste cubique modulo p. Nous avons donc $\psi(p; 3) > t$, ce qui démontre le théorème 8.

Nous finissons par démontrer le

Théorème 9.

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

Démonstration. Soit t un nombre quelconque > 3, et désignons par $3Q$ le produit de tous les nombres premiers $\leqq t$. Soient $q_1, q_2, q_3, \ldots, q_r$ tous les nombres premiers $\equiv -1 \pmod 3$ qui ne surpassent pas t. Désignons par $f_1, f_2, f_3, \ldots, f_s$ tous les nombres premiers $\equiv 1 \pmod 3$ non surpassant t. Soit $f_i = \alpha_i \alpha_i'$ la décomposition de f_i en nombres premiers primaires dans le corps $\boldsymbol{K}(\varrho)$.

Désignons par μ_i un reste cubique dans $\boldsymbol{K}(\varrho)$ modulo α_i, par ν_i un non-reste cubique dans $\boldsymbol{K}(\varrho)$ modulo α_i' et par τ_j un non-reste cubique dans $\boldsymbol{K}(\varrho)$ modulo q_j. L'existence des nombres μ_i, ν_i et τ_j se vérifie sans peine par la théorie du corps $\boldsymbol{K}(\varrho)$.

Alors c'est évident que le système des $r + 2s$ congruences simultanées

$$(8)\qquad \begin{cases} \xi \equiv \mu_i \pmod{\alpha_i}, & (i = 1, 2, \ldots, s), \\ \xi \equiv \nu_i \pmod{\alpha_i'}, & (i = 1, 2, \ldots, s), \\ \xi \equiv \tau_j \pmod{q_j}, & (j = 1, 2, \ldots, r), \end{cases}$$

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

En employant le symbole d'Eisenstein nous avons donc

$$(9)\qquad \left[\frac{\xi}{\alpha_i}\right] = 1, \quad \left[\frac{\xi}{\alpha_i'}\right] \neq 1, \quad \left[\frac{\xi}{q_j}\right] \neq 1.$$

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 $\xi + Q$ est une autre solution du système (8) 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, si b_1 n'est pas divisible par 3, la solution ξ peut être remplacée par l'une ou l'autre des deux solutions

$$\xi_1 = \xi \pm Q\sqrt{-3} = \tfrac{1}{2}(a_1 + (b_1 \pm 2Q)\sqrt{-3}).$$

Nous choisissons ici le signe de façon que $b_1 \pm 2Q$ soit divisible par 3. Si $b_1 \pm 2Q$ est divisible par 9, nous pouvons remplacer ξ_1 par la solution

$$\xi_2 = \xi_1 + 3Q\sqrt{-3} = \tfrac{1}{2}(a_1 + (b_1 \pm 2Q + 3Q)\sqrt{-3}),$$

où le nombre $b_1 \pm 2Q + 3Q$ est divisible par 3 et non par 9. Par conséquent, nous pouvons supposer que

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

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

$$\tfrac{1}{4}((au + 3Qv)^2 + 27(bu + 3Qv)^2).$$

Cette forme représente une infinité de nombres premiers, quand u et v prennent des valeurs entières; voir [8]. Soit p un de ces nombres premiers, et soit $p = \omega\omega'$ la décomposition de p en nombres premiers primaires, donc

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

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

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

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

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

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

Car, le nombre b n'est pas divisible par 3, et c'est évident que le nombre u ne l'est pas non plus.

Il résulte de tout ce qui précède que tous les nombres premiers rationnels $\leqq t$ sont des non-restes cubiques modulo p. Donc nous avons $\pi(p; 3) > t$, ce qui démontre le théorème 9.

*

C'est un fait très intéressant que les démonstrations des théorèmes 1, 2, 5, 6, 7, 8 et 9 reposent sur l'emploi des lois de réciprocité quadratique ou cubique.

INDEX BIBLIOGRAPHIQUE. [1] **T. Nagell,** Zahlentheoretische Notizen, Vidensk. selsk. Skrifter, Matem.-naturv. Kl., Oslo 1923, No 13, IV. — [2] **Paul Bachmann,** Die Lehre von der Kreistheilung, Leipzig 1872. — [3] **J. M. Vinogradov,** On the bound of the least non-residue of n-th powers, Transactions of the American Mathematical Society 29 (1927), S. 218–226. — [4] **H. J. Kanold,** Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme I, Journal für Mathematik, Bd 187 (1949). — [5]. **H. J. Kanold,** Eine Bemerkung zur Verteilung der r-ten Potenznichtreste einer ungeraden Primzahl, Journal für Mathematik, Bd 188 (1950). — [6] **T. Nagell,** Sur les restes et les non-restes quadratiques suivant un module premier, Arkiv f. Matematik, Bd 1, Nr 16, Stockholm 1950. — [7] **T. Nagell,** Sur le plus petit non-reste quadratique impair, Arkiv f. Matematik, Bd 2, Nr 2, Stockholm 1951. — [8] **H. Weber,** Beweis des Satzes; dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist, Mathematische Annalen, Bd 20 (1882).

Tryckt den 26 oktober 1951

Uppsala 1951. Almqvist & Wiksells Boktryckeri AB