ARKIV FÖR MATEMATIK Band 1 nr 33

Communiqué le 24 janvier 1951

Sur un théorème d'Axel Thue

Par Trygve Nagell

§ 1.

On doit à Axel Thue le théorème remarquable que voici:[1]

Théorème 1. *Soit p un nombre premier. Si a est un nombre entier non divisible par p, on peut trouver deux nombres entiers positifs x et $y < \sqrt{p}$ et tels qu'on ait*

$$a \equiv \pm \frac{x}{y} \pmod{p} \tag{1}$$

pour l'un ou l'autre des deux signes.

Démonstration. Considérons la totalité des nombres de la forme $ay + x$, où x et y sont des nombres dans la suite $0, 1, 2, \ldots, [\sqrt{p}]$. (Comme d'ordinaire $[c]$ signifie le plus grand nombre entier $\leqq c$.) Le nombre de ces nombres étant égal à $([\sqrt{p}] + 1)^2 > p$, il y en a au moins deux qui sont congrus modulo p. Si nous supposons

$$a y_1 + x_1 \equiv a y_2 + x_2 \pmod{p},$$

nous aurons

$$a (y_1 - y_2) \equiv x_2 - x_1 \pmod{p}. \tag{2}$$

Ici on a évidemment

$$0 < |y_1 - y_2| \leqq [\sqrt{p}], \quad 0 < |x_1 - x_2| \leqq [\sqrt{p}].$$

En effet, si l'une des différences $x_1 - x_2$ et $y_1 - y_2$ était égale à zéro, l'autre le serait aussi. Si nous posons dans (2) $|x_1 - x_2| = x$ et $|y_1 - y_2| = y$, nous aurons la congruence

$$ay \equiv \pm x \pmod{p}$$

et le théorème 1 se trouve démontré.

[1] *Voir* Axel Thue, *Et par antydninger til en talteoretisk methode,* Vidensk. selsk. Forhandl., Christiania 1902, No 7.

§ 2.

Quand nous parlerons de la représentation (1) du nombre a nous supposerons toujours que $(x, y) = 1$. Il suffit de considérer les valeurs $a = 1, 2, 3, \ldots, p-1$.

Pour $p = 3$ nous avons les représentations suivantes

$$1 \equiv \frac{1}{1}, \quad 2 \equiv -\frac{1}{1} \pmod{3}.$$

Pour $p = 5$ toutes les représentations du type (1) sont données par

$$1 \equiv \frac{1}{1}, \quad 2 \equiv \frac{2}{1} \equiv -\frac{1}{2}, \quad 3 \equiv \frac{1}{2} \equiv -\frac{2}{1}, \quad 4 \equiv -\frac{1}{1} \pmod{5}.$$

Pour $p = 7$ nous avons les représentations

$$1 \equiv \frac{1}{1}, \quad 2 \equiv \frac{2}{1}, \quad 3 \equiv -\frac{1}{2}, \quad 4 \equiv \frac{1}{2}, \quad 5 \equiv -\frac{2}{1}, \quad 6 \equiv -\frac{1}{1} \pmod{7}.$$

Pour $p = 11$ on aura les représentations

$$1 \equiv \frac{1}{1}, \quad 2 \equiv \frac{2}{1}, \quad 3 \equiv \frac{3}{1} \equiv -\frac{2}{3}, \quad 4 \equiv \frac{1}{3} \equiv -\frac{3}{2}, \quad 5 \equiv -\frac{1}{2},$$

$$6 \equiv \frac{1}{2}, \quad 7 \equiv -\frac{1}{3} \equiv \frac{3}{2}, \quad 8 \equiv -\frac{3}{1} \equiv \frac{2}{3}, \quad 9 \equiv -\frac{2}{1}, \quad 10 \equiv -\frac{1}{1},$$

où le module est $= 11$.

On voit que dans les cas de $p = 3$ et $p = 7$ il n'y a qu'une seule représentation de chaque nombre a. Dans les cas de $p = 5$ et $p = 11$ il y a deux représentations de certains nombres a.

S'il existe au moins un nombre a ayant deux représentations du type (1) avec $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$ et $(x, y) = 1$, nous dirons que le nombre premier p est de la *première catégorie*. Si pour tout nombre a il n'y a qu'une seule représentation, nous dirons que le nombre premier p est de la *seconde catégorie*.

Ainsi les nombres premiers 5 et 11 sont de la première catégorie, tandis que les nombres premiers 3 et 7 sont de la seconde catégorie.

Tous les nombres premiers $p \equiv 1 \pmod{4}$ sont de la première catégorie. En effet, on a $p = x^2 + y^2$, où x et y sont des entiers positifs $< \sqrt{p}$; donc

$$\frac{x}{y} \equiv -\frac{y}{x} \pmod{p}.$$

Théorème 2. *Le nombre des représentations du type* (1) *d'un nombre donné a est au plus égal à 2. S'il y a deux représentations, on a le signe supérieur dans l'une d'eux et le signe inférieur dans l'autre.*

Démonstration. Supposons qu'on ait les deux représentations différentes du type (1):

$$a \equiv \frac{u}{v} \pmod{p}, \qquad a \equiv \frac{u_1}{v_1} \pmod{p},$$

où u, v, u_1, v_1 sont des entiers (différents de zéro), dont les valeurs absolues sont $\leqq [\sqrt{p}]$. La différence $u v_1 - u_1 v$ est divisible par p; elle est différente de zéro, puisque $(u, v) = (u_1, v_1) = 1$. Nous aurons donc

$$p \leqq |u v_1 - u_1 v| < 2 (\sqrt{p})^2 = 2p$$

et par suite

$$|u v_1 - u_1 v| = p.$$

Si $\frac{u}{v}$ et $\frac{u_1}{v_1}$ ont le même signe, on a

$$|u v_1 - u_1 v| < (\sqrt{p})^2 - 1 = p - 1.$$

Il faut donc que $\frac{u}{v}$ et $\frac{u_1}{v_1}$ soient de signes opposés. Il en résulte qu'il ne peut pas exister trois représentations différentes du même nombre a, et le théorème 2 est démontré.

Pour qu'il y ait deux représentations du nombre positif a, il faut que $a \geqq [\sqrt{p}]$. En effet, supposons que $a \equiv -\frac{x}{y} \pmod{p}$, $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$, $(x, y) = 1$ et que $a \leqq [\sqrt{p}] - 1$. Si nous posons $a y + x = p h$, où h est un entier positif, nous avons

$$p h = a y + x < [\sqrt{p}]^2 + [\sqrt{p}] < 2p,$$

d'où $h = 1$. Donc

$$a = \frac{p - x}{y} \geqq \frac{p - [\sqrt{p}]}{[\sqrt{p}]} > [\sqrt{p}] - 1$$

contre l'hypothèse.

§ 3.

Quand $\varphi(m)$ signifie la fonction d'Euler, nous posons

$$\Phi(n) = \sum_{k=1}^{n} \varphi(k). \tag{3}$$

On en déduit sans peine l'identité

$$\Phi(n) = \tfrac{1}{2}\sum_{k=1}^{n}\mu(k)\left(\left[\frac{n}{k}\right]^2 + \left[\frac{n}{k}\right]\right). \tag{4}$$

A l'aide de ce résultat on établit facilement la formule approximative

$$\Phi(n) = \frac{3}{\pi^2}n^2 + O(n\log n). \tag{5}$$

Pour la démonstration de ces résultats je renvoie à HARDY and WRIGHT, *An introduction to the theory of numbers,* Oxford 1945, Theorem 330.

Si nous désignons par $A(p)$ le nombre des nombres de la forme $\pm\frac{x}{y}$, où x et y sont des nombres entiers positifs $\leqq [\sqrt{p}]$, tels que $(x, y) = 1$, il est évident que

$$A(p) = 4\,\Phi([\sqrt{p}]) - 2. \tag{6}$$

Théorème 3. *Les nombres premiers* 3, 7, 23 *et* 47 *sont de la seconde catégorie.*

En effet, pour que le nombre premier p soit de la seconde catégorie, il faut et il suffit que

$$p - 1 = A(p) = 4\,\Phi([\sqrt{p}]) - 2.$$

Pour $p = 23$ on a $[\sqrt{p}] = 4$ et

$$\Phi(4) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) = 6,$$

donc

$$4\,\Phi(4) - 2 = 22 = p - 1.$$

Pour $p = 47$ on a $[\sqrt{p}] = 6$ et

$$\Phi(6) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) + \varphi(6) = 12,$$

donc

$$4\,\Phi(6) - 2 = 46 = p - 1.$$

Nous savons déjà que 3 et 7 sont de la seconde catégorie.

En vertu de la formule (5) on aura

$$A(p) - (p-1) = 4\,\Phi([\sqrt{p}]) - p - 1 = \left(\frac{12}{\pi^2} - 1\right)p + 0(\sqrt{p}\log p).$$

On en conclut que la différence $A(p) - (p-1)$ est positive pour tous les p suffisamment grands. Il en résulte

Théorème 4. *Il n'y a qu'un nombre fini de nombres premiers de la seconde catégorie.*

Pour déterminer tous les nombres premiers de la seconde catégorie il suffit de préciser la formule (5) et la remplacer par une inégalité. On peut p. ex. vérifier que

$$\Phi(x) > \frac{3}{\pi^2}x^2 - \tfrac{1}{2}x\log x + 1$$

pour tous les $x \geqq 2$. Cependant, cette méthode entraînerait des calculs numériques très pénibles. Par cette raison nous allons nous servir d'une autre méthode pour déterminer tous les nombres premiers de la seconde catégorie.

§ 4.

Pour tout nombre premier $p > 3$ on a l'inégalité

$$p \leqq [\sqrt{p}]^2 + 2[\sqrt{p}] - 1. \tag{7}$$

En effet, si nous posons $[\sqrt{p}] = \sqrt{p} - \varepsilon$, où $0 < \varepsilon < 1$, nous aurons

$$p - [\sqrt{p}]^2 - 2[\sqrt{p}] = p - (\sqrt{p} - \varepsilon)^2 - 2\sqrt{p} + 2\varepsilon =$$
$$= (2\varepsilon - 2)\sqrt{p} + 2\varepsilon - \varepsilon^2 = (2\varepsilon - 2)\sqrt{p} - (1-\varepsilon)^2 + 1 < 1.$$

p étant un nombre premier > 3 on ne peut pas avoir

$$p = [\sqrt{p}]^2 + 2[\sqrt{p}].$$

Ainsi l'inégalité (7) est établie.

Théorème 5. *Tout nombre premier p satisfaisant à l'inégalité*

$$p - [\sqrt{p}]^2 < \sqrt{p} \tag{8}$$

est de la première catégorie.

Car dans ce cas le nombre $[\sqrt{p}]$ a les deux représentations

$$[\sqrt{p}] \equiv \frac{[\sqrt{p}]}{1} \pmod{p}$$

et

$$[\sqrt{p}] \equiv -\frac{p - [\sqrt{p}]^2}{[\sqrt{p}]} \pmod{p}.$$

Théorème 6. *Tout nombre premier $p > 3$ satisfaisant aux inégalités*

$$p - [\sqrt{p}]^2 > \sqrt{p} \tag{9}$$

et

$$p \neq [\sqrt{p}]^2 + 2[\sqrt{p}] - 1 \tag{10}$$

est de la première catégorie.

Démonstration. Nous avons

$$[\sqrt{p}] + 2 \equiv \frac{[\sqrt{p}]^2 + 2[\sqrt{p}] - p}{[\sqrt{p}]} \pmod{p} \tag{11}$$

et

$$[\sqrt{p}] + 2 \equiv -\frac{p - [\sqrt{p}]^2 - [\sqrt{p}] + 2}{[\sqrt{p}] - 1} \pmod{p}. \tag{12}$$

Il en résulte que le nombre $[\sqrt{p}] + 2$ a deux représentations. Car, en vertu des inégalités (7), (9) et (10) nous avons

$$1 < [\sqrt{p}]^2 + 2[\sqrt{p}] - p < [\sqrt{p}]$$

et

$$2 < p - [\sqrt{p}]^2 - [\sqrt{p}] + 2 < [\sqrt{p}] + 1.$$

Théorème 7. *Tout nombre premier $p > 47$ tel que*

$$p = [\sqrt{p}]^2 + 2[\sqrt{p}] - 1 \tag{13}$$

est de la première catégorie.

En effet, dans ce cas le nombre $[\sqrt{p}] + 4$ a les deux représentations

$$[\sqrt{p}] + 4 \equiv \frac{[\sqrt{p}] - 3}{[\sqrt{p}] - 1} \pmod{p}$$

et

$$[\sqrt{p}] + 4 \equiv -\frac{7}{[\sqrt{p}] - 2} \pmod{p}.$$

Car, p étant > 47, on a $[\sqrt{p}] > 7$.

On voit aisément que les nombres 7, 23 et 47 sont les seuls nombres premiers $\leqq 47$ ayant la forme (13).

Il résulte de tout ce qui précède dans ce numéro:

Théorème 8. *Tous les nombres premiers sont de la première catégorie sauf les nombres* 3, 7, 23 *et* 47.

§ 5.

Si p est un nombre premier impair, nous désignons par ψ_p le plus petit nombre premier impair, qui est un non-reste quadratique modulo p.

Dans un travail antérieur nous avons établi les résultats suivants:[1]

1) Si $p \equiv 1 \pmod{8}$, on a $\psi_p \leqq [\sqrt{p}]$.

2) Si $p \equiv 5 \pmod{8}$, on a $\psi_p \leqq [\sqrt{2p}]$.

3) Si $p \equiv 7 \pmod{8}$ et $p > 7$, on a $\psi_p \leqq [\sqrt{2p}] - 1$.

4) Si $p \equiv 3 \pmod{8}$ et $p > 3$, on a $\psi_p \leqq [2\sqrt{p}] + 1$.

Au troisième de ces résultats nous allons apporter la précision suivante:

Théorème 9. *Si p est un nombre premier* $\equiv 7$ (*mod.* 8), *on a*

$$\psi_p \leqq [\sqrt{p}] \tag{14}$$

sauf pour $p = 7$ *et* $p = 23$.

Démonstration. Le théorème n'est pas vrai pour $p = 7$, vu que $[\sqrt{7}] = 2$. Il n'est pas vrai non plus pour $p = 23$, puisque $[\sqrt{23}] = 4$, et que 3 est un reste quadratique de 23. Le théorème est vrai pour $p = 47$, puisque $[\sqrt{47}] = 6$, et que 5 est un non-reste quadratique de 47.

Soit ensuite p un nombre premier $\equiv 7 \pmod{8}$ qui est de la première catégorie. Alors, d'après le théorème 8 il existe un nombre entier a qui possède deux représentations

$$a \equiv \frac{x}{y} \pmod{p}, \tag{15}$$

$$a \equiv -\frac{x_1}{y_1} \pmod{p}, \tag{16}$$

où les entiers x, y, x_1, y_1 sont positifs et $< \sqrt{p}$.

---

[1] *Voir* T. Nagell, *Sur les restes et les non-restes quadratiques suivant un module premier*, Arkiv f. Matematik, Bd 1, Nr 16, Stockholm 1950. Errata à ce travail: Page 186, ligne 18, remplacer $K(\sqrt{p})$ par $K(\sqrt{-p})$. Page 187, ligne 4, comptant en remontant, remplacer p^2 par p. Page 190, ligne 20, remplacer q par a.

Si a est un non-reste quadratique, il résulte de (15) que ou x ou y est un non-reste quadratique. Puisque 2 est un reste quadratique, on en conclut que

$$\psi_p \leqq [\sqrt{p}].$$

Si a est un reste quadratique, il résulte de (16) que ou x_1 ou y_1 est un non-reste quadratique, vu que -1 est un non-reste quadratique. Puisque 2 est un reste quadratique, il en résulte que

$$\psi_p \leqq [\sqrt{p}].$$

Tryckt den 20 april 1951

Uppsala 1951. Almqvist & Wiksells Boktryckeri AB