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.