Communiqué le 23 Novembre 1949

Sur les restes et les non-restes quadratiques suivant un module premier

Par Trygve Nagell

§ 1. Démonstration de quelques lemmes

Si a est un nombre entier $\equiv 1 \pmod{8}$ et si h est un nombre entier $\geqq 3$, il est bien connu que la congruence

$$u^2 \equiv a \pmod{2^h} \tag{1}$$

admet exactement quatre racines incongrues modulo 2^h. Si u_0 est une racine de cette congruence, les trois nombres

$$2^{h-1} - u_0, \quad 2^{h-1} + u_0, \quad 2^h - u_0$$

satisfont aussi à la congruence. De plus, on voit sans peine que les quatre nombres

$$u_0, \quad 2^{h-1} - u_0, \quad 2^{h-1} + u_0, \quad 2^h - u_0 \tag{2}$$

sont incongrus entre eux deux à deux modulo 2^h. Il en résulte

Lemme 1. *Si u_0 est la plus petite racine positive de la congruence (1), les quatre nombres (2) représentent les solutions incongrues modulo 2^h, et ils satisfont aux inégalités*

$$0 < u_0 < 2^{h-1} - u_0 < 2^{h-1} + u_0 < 2^h - u_0 . \tag{3}$$

*

On doit à Thue le théorème suivant [1]:[1]

Lemme 2. *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*

---

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