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

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