ARKIV FÖR MATEMATIK Band 1 nr 38

Communiqué le 6 juin 1951

Sur le plus petit non-reste quadratique impair

Par TRYGVE NAGELL

§ 1.

Soit p un nombre premier >2. Désignons par ψ le plus petit nombre impair positif qui est un non-reste quadratique modulo p. C'est évident que ψ est toujours un nombre premier.

Dans une note [1] publiée en 1923 j'ai proposé le problème de déterminer une borne supérieure de ψ en fonction de p, et par des raisonnements très simples j'y ai démontré que

$$\psi < 2\sqrt{p} + 1 \tag{1}$$

pour tous les nombres premiers $p > 3$.

Ensuite, par des moyens analytiques, J. M. VINOGRADOV a établi le résultat plus précis que voici [2]:

Si p est un nombre premier suffisamment grand tel que $p \equiv \pm 1 \pmod 8$, on a

$$\psi < p^{\nu} (\log p)^2, \tag{2}$$

où $\nu = \dfrac{1}{2\sqrt{e}} = 0.303\ldots$

Enfin, par une méthode élémentaire, A. BRAUER a obtenu le résultat suivant [3]:

Pour tous les nombres premiers $p \equiv \pm 3 \pmod 8$ on a

$$\psi < 2(4p)^{\frac{2}{5}} + 2(4p)^{\frac{1}{5}} + 1. \tag{3}$$

Pour tous les nombres premiers $p \equiv -1 \pmod 8$ on a

$$\psi < (2p)^{\frac{2}{5}} + 3(2p)^{\frac{1}{5}} + 1. \tag{4}$$

J'ai montré récemment comment on peut employer un théorème d'AXEL THUE pour trouver une borne supérieure de ψ. Il s'agit du théorème suivant [4]:

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

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

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