

H. ROCHETTE

Solution de la question 343

Nouvelles annales de mathématiques 1^{re} série, tome 16 (1857), p. 159-160

http://www.numdam.org/item?id=NAM_1857_1_16__159_1

© Nouvelles annales de mathématiques, 1857, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

SOLUTION DE LA QUESTION 343

(voir t. XV, p. 353);

PAR LE P. H. ROCHETTE, S. J.

Si p et $4p + 1$ sont des nombres premiers absolus, 2

est racine primitive relativement au nombre $4p + 1$.

(ТШЕВИЧЕФ.)

Pour que 2 soit racine primitive de $4p + 1$, il faut, comme l'indique la marche que l'on suit pour obtenir ces racines, que ce nombre ne se trouve ni parmi les résidus quadratiques, ni parmi les résidus de puissance p des $4p$ premiers nombres naturels. Or on sait que si 2 était résidu quadratique par rapport à l'un de ces nombres, x par exemple, c'est-à-dire si l'on avait

$$x^2 \equiv 2 \pmod{(4p + 1)},$$

on aurait aussi (Serret, *Algèbre supérieure*, p. 332)

$$(1) \quad 2^{2p} \equiv 1 \pmod{(4p + 1)},$$

et s'il était résidu de puissances p , on aurait de même

$$(2) \quad 2^p \equiv 1 \pmod{(4p + 1)}.$$

La première de ces deux congruences est impossible, car n représentant un nombre premier, on a constamment (*Nouvelles Annales*, t. V, p. 657)

$$2^{\frac{n-1}{4}} \equiv (-1)^{\frac{n-1}{4}} \pmod{(n)},$$

expression qui se réduit dans le cas actuel à

$$(3) \quad 2^{2p} \equiv (-1)^p \pmod{(4p + 1)},$$

et comme p est premier et par conséquent impair, la forme (3) entraîne l'impossibilité de la forme (1).

Quant à la congruence (2), elle ne pourrait évidemment avoir lieu que dans le cas de $p = 1$, et dans ce cas on n'a plus à considérer les résidus de puissances p . Ainsi 2, ne se trouvant pas parmi les résidus des puissances marquées par les facteurs premiers de $4p$, sera racine primitive relativement à $4p + 1$.