

RAOUL BRICARD

**Sur le caractère quadratique du
nombre 3 par rapport à un nombre
premier quelconque**

Nouvelles annales de mathématiques 3^e série, tome 16
(1897), p. 546-549

http://www.numdam.org/item?id=NAM_1897_3_16__546_1

© Nouvelles annales de mathématiques, 1897, 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/>

[14]

**SUR LE CARACTÈRE QUADRATIQUE DU NOMBRE 5
PAR RAPPORT A UN NOMBRE PREMIER QUELCONQUE ;**

PAR M. RAOUL BRICARD.

Euler, Legendre et plus récemment Stieltjes ⁽¹⁾ ont donné des démonstrations simples des théorèmes relatifs aux caractères quadratiques des nombres -1 et 2 par rapport à un module premier. Je me propose d'indiquer dans cette Note comment on peut, par une méthode élémentaire, déterminer les nombres premiers dont le nombre 3 est ou n'est pas résidu quadratique.

⁽¹⁾ Voir l'*Introduction à l'Étude de la Théorie des Nombres et de l'Algèbre supérieure*, de MM. E. Borel et J. Dieck

Soit p un nombre premier et m_1 un nombre quelconque de la suite $2, 3, \dots, p-1$. On peut déterminer un nombre entier m_2 , inférieur à p et tel que l'on ait

$$m_1 m_2 \equiv m_1 - 1 \pmod{p}.$$

Il est évident que l'on n'a ni

$$m_2 \equiv 0 \pmod{p},$$

ni

$$m_2 \equiv 1 \pmod{p};$$

m_2 appartient donc à la même suite que m_1 .

Le nombre m_2 ainsi obtenu permet de déterminer un nombre m_3 , appartenant à la suite $2, 3, \dots, p-1$, tel que l'on ait

$$m_2 m_3 \equiv m_2 - 1 \pmod{p},$$

et ainsi de suite.

La suite de nombres ainsi obtenue, $m_1, m_2, m_3, \dots$ donne lieu aux remarques suivantes :

1° Si m_2 est différent de m_1 , il en est de même de m_3 . En effet, on aurait, dans le cas contraire,

$$m_2 m_1 \equiv m_2 - 1 \equiv m_1 - 1 \pmod{p},$$

d'où

$$m_2 = m_1.$$

ce qui serait contraire à l'hypothèse.

2° On a toujours, au contraire,

$$m_4 = m_1.$$

Écrivons, en effet, de la manière suivante, les congruences qui déterminent successivement les nombres m_2, m_3, m_4 :

$$m_1(m_2 - 1) \equiv -1 \pmod{p},$$

$$m_2 m_3 \equiv m_2 - 1 \pmod{p},$$

$$m_2(m_3 - 1) \equiv -1 \pmod{p},$$

$$m_3 m_4 \equiv m_3 - 1 \pmod{p}.$$

La seconde congruence est écrite de deux manières différentes.

Multiplions membre à membre la première et la deuxième congruence. Opérons de même sur la troisième et la quatrième. Il vient, après divisions par des facteurs incongrus à zéro,

$$m_1 m_2 m_3 \equiv -1 \pmod{p},$$

$$m_2 m_3 m_4 \equiv -1 \pmod{p},$$

d'où l'on tire

$$(m_1 - m_4) m_2 m_3 \equiv 0 \pmod{p},$$

et, par suite,

$$m_1 = m_4.$$

3° Enfin il peut arriver que l'on ait $m_2 = m_4$. Alors tous les termes de la suite $m_1, m_2, \dots$ seront identiques. m_1 est dans ce cas une racine de la congruence

$$x^2 - x + 1 \equiv 0 \pmod{p},$$

qui admet aussi la racine $p + 1 - m$, et celle-là seulement, comme on le voit immédiatement. Cette nouvelle racine est nécessairement distincte de la première, si l'on suppose $p \neq 3$. En effet, on aurait, dans le cas contraire,

$$m_1 = p + 1 - m, \quad \text{d'où} \quad m_1 = \frac{p+1}{2},$$

et, par suite,

$$\left(\frac{p+1}{2}\right)^2 - \left(\frac{p+1}{2}\right) + 1 \equiv 0 \pmod{p},$$

ou

$$p^2 + 3 \equiv 0 \pmod{p},$$

congruence impossible.

On peut résumer ainsi ce qui précède : si la congruence

$$x^2 - x + 1 \equiv 0 \pmod{p}$$

est impossible, les nombres de la suite $2, 3, \dots, p-1$ se répartissent en un certain nombre de groupes de trois

termes, et l'on a nécessairement

$$p - 2 \equiv 0 \pmod{3},$$

et le nombre p est de la forme $3q + 2$.

Si au contraire cette congruence est possible, la même suite comprend deux nombres satisfaisant à cette congruence, plus un certain nombre de groupes de trois termes.

On a alors

$$p - 2 - 2 \equiv 0 \pmod{3}.$$

Le nombre p est de la forme $3q + 1$.

Les réciproques sont évidemment vraies.

Remarquons maintenant que la congruence

$$x^2 - x + 1 \equiv 0 \pmod{p}$$

peut s'écrire

$$(2x - 1)^2 + 3 \equiv 0 \pmod{p}.$$

Elle est donc possible ou impossible, suivant que l'on a

$$\left(\frac{-3}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{-3}{p}\right) = -1.$$

et l'on en déduit le théorème suivant :

Le nombre -3 est résidu quadratique des nombres premiers de la forme $3q + 1$, et non résidu des nombres premiers de la forme $3q + 2$.

En combinant ce théorème avec les théorèmes relatifs au caractère quadratique du nombre -1 , on obtient facilement la valeur du symbole $\left(\frac{3}{p}\right)$ pour toutes les valeurs du nombre premier p . Je n'insiste pas sur le résultat bien connu que l'on obtient ainsi : mon but était simplement de montrer comment on peut y parvenir par les procédés les plus élémentaires.