JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

DIRICHLET

Sur le caractère biquadratique du nombre 2

Journal de mathématiques pures et appliquées 2e série, tome 4 (1859), p. 367-368.

<http://www.numdam.org/item?id=JMPA_1859_2_4__367_0>

SUR

LE CARACTÈRE BIQUADRATIQUE DU NOMBRE 2.

EXTRAIT D'UNE LETTRE DE M. DIRICHLET A M. STERN.

(TRADUCTION DE M. HOÜEL.)

Soit p un nombre premier de la forme $4n+1$, et

$$p = a^2 + b^2,$$

a étant impair. De cette équation et de la suivante

$$2p = (a+b)^2 + (a-b)^2,$$

on tire immédiatement, en faisant usage du symbole de Legendre généralisé,

$$\left(\frac{p}{a}\right) = 1, \quad \left(\frac{2p}{a+b}\right) = 1 \quad \text{ou} \quad \left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right),$$

d'où, ensuite, par des théorèmes connus,

$$\left(\frac{a}{p}\right) = 1, \quad \left(\frac{a+b}{p}\right) = (-1)^{\frac{1}{8}[(a+b)^2-1]},$$

ou, ce qui revient au même,

$$a^{\frac{1}{2}(p-1)} \equiv 1, \quad (a+b)^{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{8}[(a+b)^2-1]} \pmod{p}.$$

D'autre part, de la relation

$$(a+b)^2 = a^2 + b^2 + 2ab \equiv 2ab \pmod{p},$$

on tire, en élevant à la puissance $\frac{1}{4}(p-1)$,

$$(a+b)^{\frac{1}{2}(p-1)} \equiv 2^{\frac{1}{4}(p-1)} . a^{\frac{1}{4}(p-1)} . b^{\frac{1}{4}(p-1)} \pmod{p},$$

ou, en posant

$$b \equiv af,$$

et ayant égard aux deux dernières congruences,

$$(-1)^{\frac{1}{8}[(a+b)^2-1]} = (-1)^{\frac{1}{8}(p-1+2ab)} \equiv 2^{\frac{1}{4}(p-1)} . f^{\frac{1}{4}(p-1)} \pmod{p}.$$

Mais à cause de

$$a^2 + b^2 = p, \quad b^2 \equiv a^2 f^2,$$

on a

$$f^2 \equiv -1 \pmod{p},$$

d'où

$$(f^2)^{\frac{1}{8}(p-1+2ab)} = f^{\frac{1}{4}(p-1)} . f^{\frac{1}{2}ab} \equiv 2^{\frac{1}{4}(p-1)} . f^{\frac{1}{4}(p-1)} \pmod{p}:$$

en divisant par $f^{\frac{1}{4}(p-1)}$, on a donc enfin

$$2^{\frac{1}{4}(p-1)} \equiv f^{\frac{1}{2}ab} \pmod{p},$$

résultat qui se transforme dans celui que Gauss a donné au § 24 de sa *Theoria residuorum biquadraticorum*, lorsqu'on multiplie par $a^{\frac{1}{2}ab}$ et que l'on remplace de nouveau af par b.

Gottingue, le 21 janvier 1857.