

ON THE BIQUADRATIC CHARACTER OF THE NUMBER “TWO”

G. LEJEUNE DIRICHLET

(From a letter of DIRICHLET to Herrn STERN at Göttingen,
Crelle's Journal for Pure and Applied Mathematics, Vol. 57 pg.
187-188.)

Let p be a prime number of the form $4n + 1$ and

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

where a is odd. From this equation and that following from it,

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

with application of the generalized symbols of LEGENDRE, results

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

or

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

and then, according to the known theorems:

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

or, what is the same:

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

On the other hand, is obtained:

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

and, by raising to the power $\frac{1}{4}(p-1)$:

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

or, by setting

$$b \equiv af$$

and considering both the latter congruences:

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

Moreover,

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

thus,

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

or, dividing by $f^{\frac{1}{4}(p-1)}$,

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

which transforms into the result given by GAUSS in section 24 of his “*theoria residuorum biquadraticorum*”, if it is multiplied by $a^{\frac{1}{2}ab}$ and b is inserted again for a .

Göttingen, January 21, 1857
