MATHEMATICS

THE LAW OF QUADRATIC RECIPROCITY

BY

H. D. KLOOSTERMAN

(Communicated at the meeting of October 31, 1964)

L. HOLZER gives in his book "Zahlentheorie" (Teil I, p. 76; Teubner, Leipzig 1958) a remarkably simple proof of the quadratic reciprocity law. He does not seem to have observed that his proof can further be simplified. The proof then proceeds as follows.

Let F_q be the prime field with q elements (q prime $\neq 2$). Let also p be an odd prime different from q. Let $\alpha \neq 1$ be a root of the equation $x^p = 1$ in an extension field of F_q and consider the Gaussian sum

$$G = \sum_{m \bmod p}' \left(\frac{m}{p}\right) \alpha^m,$$

where the summation extends over a reduced residue system (which is denoted by the prime) mod p, and where (m/p) is the Legendre symbol. Using a classical argument we find

$$G^2 = \sum_{m,n \bmod p}' \left(\frac{mn}{p}\right) \alpha^{m+n}.$$

If m is replaced by mn (which does not alter the range of summation) we obtain

$$(1)\quad \begin{cases} G^2 = \displaystyle\sum_{m \bmod p}' \left(\frac{m}{p}\right) \sum_{n \bmod p}' \alpha^{n(m+1)} = \\ \qquad = \left(\dfrac{-1}{p}\right)(p-1) - \displaystyle\sum_{\substack{m \bmod p \\ m \not\equiv -1}}' \left(\frac{m}{p}\right) = \left(\dfrac{-1}{p}\right) p. \end{cases}$$

Therefore G belongs to the finite field with q^2 elements and G^2 belongs to F_q.

Since G is a sum in a field of characteristic q, we have

$$G^q = \sum_{m \bmod p}' \left(\frac{m}{p}\right) \alpha^{mq}.$$

Since mq runs through a reduced residue system mod p, if m does so, we obtain

$$G^q = \left(\frac{q}{p}\right) G$$

which shows that

$$\left(\frac{G^2}{q}\right) = \left(\frac{q}{p}\right)$$

or according to (1):

$$\left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{q}{p}\right)$$

which is the quadratic reciprocity law.

In order to determine the quadratic character of 2 let α be a root of the equation $x^2+1=0$ over F_q, so that α can be chosen in the finite field with q^2 elements. Now let $G=1+\alpha$. Since $\alpha^2=-1$, we have

$$G^4 = -4. \tag{2}$$

In a field of prime characteristic q we have

$$G^q = 1+\alpha^q = 1+(-1)^{(q-1)/2}\,\alpha. \tag{3}$$

Now if $q \equiv 1 \pmod 4$, it follows that

$$G^q = 1+\alpha = G, \; G^{q-1} = 1$$

and by means of (2) this can be written as

$$2^{(q-1)/2} = (-1)^{(q-1)/4} \quad (q \equiv 1 \pmod 4). \tag{4}$$

If however $q \equiv 3 \pmod 4$ it follows from (3) that

$$G^{q+1} = (1-\alpha)\,G = 1-\alpha^2 = 2$$

and by means of (2) this can be written as

$$2^{(q-1)/2} = (-1)^{(q+1)/4} \quad (q \equiv -1 \pmod 4). \tag{5}$$

The equations (4) and (5) determine the quadratic character of 2 and can be combined to

$$\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}.$$