ON THE LAW OF QUADRATIC RECIPROCITY*

BY ALBERT WHITEMAN

The following proof of the law of quadratic reciprocity, which depends upon a modified form of the Gaussian criterion, is believed to be new.

According to the usual form of this criterion, if p is any integer not divisible by the odd prime q, then p is a quadratic residue or non-residue of q according as in the series

$$p, 2p, 3p, \cdots, (q-1)p/2,$$

the number of numbers whose least positive remainders (mod q) exceed $q/2$ is even or odd. But, if $\lambda p = \mu q + r$, $q/2 < r < q$, then $2\lambda p = (2\mu+1)q + 2r - q$, and conversely. Hence we have the transformed criterion: p is a quadratic residue or non-residue of q according as the number of least positive odd remainders in the series:

$$(1) \qquad 2p, 4p, 6p, \cdots, (q-1)p \pmod{q}$$

is even or odd.†

In the following discussion p, q represent any two odd primes such that $q > p$. Let r denote any odd remainder of (1) such that $p < r < q$. Then, for a suitable λ, $(1 \leqq \lambda \leqq (q-1)/2)$,

$$(2) \qquad 2\lambda p \equiv r \pmod{q},$$

whence

$$(3) \qquad (q+1-2\lambda)p \equiv p + q - r \pmod{q},$$

where $p < p + q - r < q$.

Congruences (2) and (3) are identical only for $2\lambda = (q+1)/2$, $r = (p+q)/2$. Hence the odd remainders of (1) that are greater than p may be arranged in pairs by means of (2) and (3) except

* Presented to the Society, February 23, 1935.

† For other proofs of the reciprocity law using this transformed criterion see a paper by Lange, *Ein Elementarer Beweis des Reziprozitäts-gesetzes*, Berichte der Koeniglichen Sachsischen Gesellschaft, vol. 48 (1896), p. 629; vol. 49 (1897), p. 607; see also P. Bachmann, *Niedere Zahlentheorie*, Part 1, 1902, pp. 256–261, and pp. 266–267.

when $(q+1)/2$ is even and $(p+q)/2$ is odd, that is, when p, q are each of the form $4n+3$. In this case there is one odd remainder that does not belong to such a pair. If we denote by a the number of odd remainders greater than p, it follows that a is even if at least one of the two primes p, q is of the form $4n+1$, and odd if both are of the form $4n+3$. Consequently

$$a \equiv (p-1)(q-1)/4 \pmod{2}. \tag{4}$$

Now let b denote the number of those odd remainders in (1) that are less than p. Then $(p/q)=(-1)^{a+b}$. Also, if c denotes the number of least positive odd remainders in the series

$$2q, 4q, 6q, \cdots, (p-1)q \pmod{p}, \tag{5}$$

we have $(q/p)=(-1)^c$. Hence

$$(p/q)(q/p) = (-1)^{a+b+c}. \tag{6}$$

To complete the proof, we shall now show that the odd remainders in (1) that are less than p are identical with the odd remainders in (5), and hence that $b=c$. Let

$$2\lambda p \equiv r \pmod{q}, \tag{7}$$

where now r is an odd remainder such that $0<r<p$, and $1\leqq\lambda\leqq(q-1)/2$. Hence

$$2\lambda p = (2\mu - 1)q + r,$$

where $0<\mu<(p+1)/2$. From this we obtain

$$(p+1-2\mu)q \equiv r \pmod{p}. \tag{8}$$

Conversely, from (8), where $1\leqq\mu\leqq(p-1)/2$, we obtain (7) with $0<\lambda<(q+1)/2$.

Hence, as stated above, the odd remainders in (1) that are less than p are identical with the odd remainders in (5), so that $b=c$. The theorem then follows from (4) and (6).

THE UNIVERSITY OF PENNSYLVANIA