

# ON QUADRATIC RESIDUES\*

BY

J. McDONNELL

1. Let  $m$  be any integer,  $n$  a positive odd integer, and  $s$  a primitive  $n$ th root of unity. We shall prove that the product

$$A = \prod_{k=1}^{\frac{1}{2}(n-1)} \frac{s^{km} - s^{-km}}{s^k - s^{-k}}$$

is identical with Jacobi's symbol  $(m/n)$  and obtain a proof of the quadratic reciprocity theorem. If  $m$  and  $n$  have a common factor  $g$ , then  $A = 0$ , since the numerator of  $A$  has the factor  $s^{qm} - s^{-qm} = 0$ , where  $q = n/g$ .

2. We shall show that, when  $m$  and  $n$  are relatively prime,  $A$  is independent of the particular primitive root  $s$  employed. First, let  $m$  be positive and odd, and let  $r$  be a primitive  $m$ th root of unity. Since  $m$  is odd, the  $m$ th roots of unity are  $1, r^2, r^4, \dots, r^{2(m-1)}$ . Hence

$$x^m - y^m \equiv (x - y)(xr - yr^{-1})(xr^2 - yr^{-2}) \dots (xr^{m-1} - yr^{-(m-1)}),$$

identically. Take  $x = s^a, y = s^{-a}$ . We see that

$$A = \prod_{p=1}^{m-1} \prod_{q=1}^{\frac{1}{2}(n-1)} (r^p s^a - r^{-p} s^{-a}).$$

Similarly,

$$B = \prod_{k=1}^{\frac{1}{2}(m-1)} \frac{r^{kn} - r^{-kn}}{r^k - r^{-k}} = \prod_{p'=1}^{\frac{1}{2}(m-1)} \prod_{q'=1}^{n-1} (r^{p'} s^{a'} - r^{-p'} s^{-a'}).$$

To any factor  $F = r^p s^a - r^{-p} s^{-a}$  in  $A$  there corresponds a factor

$$F' = r^{p'} s^{a'} - r^{-p'} s^{-a'}$$

in  $B$  such that one of the alternatives

- (i)  $p = p', \quad q = q', \quad p \leq \frac{1}{2}(m-1), \quad q' \leq \frac{1}{2}(n-1),$
  - (ii)  $p + p' = m, \quad q + q' = n, \quad p > \frac{1}{2}(m-1), \quad q' > \frac{1}{2}(n-1),$
- holds. In the first case,  $F = F'$ ; in the second,  $F = -F'$ . Hence

$$A = (-1)^{\frac{(m-1)(n-1)}{4}} B.$$

As  $B$  is independent of  $s$ ,  $A$  is also.

\* Presented to the Society (Chicago), March 21, 1913.

Next, let  $m$  be negative or even. Choose  $t$  so that  $\mu = m + tn$  is positive and odd. The expression in § 1 for  $A$  remains unaltered if we replace  $s^m$  by  $s^\mu$ . By the preceding proof,  $A$  is independent of  $s$ .

Accordingly we can in all cases represent the function  $A$  by the symbol  $f(m, n)$ , since it depends upon  $m$  and  $n$  only.

3. We shall now show how to evaluate  $f(m, n)$  by a process of reduction based upon the following three properties:\*

- (1)  $f(m, n) = f(p, n)$  if  $p \equiv m \pmod{n}$ ,
- (2)  $f(p, n) = (-1)^{\frac{n-1}{2}} f(q, n)$  if  $p + q \equiv 0 \pmod{n}$ ,
- (3)  $f(m, n) = (-1)^{\frac{(m-1)(n-1)}{4}} f(n, m)$  if  $m$  and  $n$  are positive and odd.

Let  $p$  be the positive remainder  $< n$  obtained by dividing  $m$  by  $n$ . Then  $f(m, n) = f(p, n)$  by (1). If  $p$  is even, define the odd number  $q$  by  $p + q = n$  and apply (2). Thus either  $p$  itself or else  $q$  is positive and less than  $n$ . We now apply (3). After repetitions of this process, we ultimately reach unity and an odd number  $l$  such that  $f(m, n) = \pm f(1, l)$ . But  $f(1, l) = 1$  (§ 1). Thus  $f(m, n) = \pm 1$  and the sign is determined by the reduction process.

4. If  $m = pq$ , then

$$(4) \quad f(m, n) = f(p, n) \cdot f(q, n).$$

We may assume that  $m$  is relatively prime to  $n$ , since otherwise each member is zero by § 1. Then  $s_1 = s^a$  is a primitive  $n$ th root of unity and

$$\frac{s^{km} - s^{-km}}{s^k - s^{-k}} = \frac{s_1^{kp} - s_1^{-kp}}{s_1^k - s_1^{-k}} \cdot \frac{s^{ka} - s^{-ka}}{s^k - s^{-k}},$$

from which (4) follows. In particular,

$$(5) \quad f(m, n) = \{f(2, n)\}^p \cdot f(q, n), \quad \text{if } m = 2^p q \quad (q \text{ odd}).$$

By (2) and (3),

$$f(2, n) = (-1)^{\frac{n-1}{2}} f(n-2, n), \quad f(n-2, n) = f(n, n-2),$$

\* The third property was proved in § 2. The first and second follow from

$$s^{kp} = s^{km}, \quad s^{ka} - s^{-ka} = -s^{kp} + s^{-kp}.$$

since  $(n-1)(n-3) \equiv 0 \pmod{8}$ . Then, from these and (1),

$$(6) \quad f(2, n) = (-1)^{\frac{n-1}{2}} f(2, n-2).$$

If  $\omega$  is an imaginary cube root of unity,

$$f(2, 3) = \frac{\omega^2 - \omega^{-2}}{\omega - \omega^{-1}} = -1.$$

Then, by (6),  $f(2, 5) = -1$ ,  $f(2, 7) = 1$ ,  $f(2, 9) = 1$ , and, generally,

$$(7) \quad f(2, n) = (-1)^{\frac{n^2-1}{8}}.$$

5. If  $n = ab$ , as in any text on the theory of numbers,

$$\frac{n^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8}, \quad \frac{n-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}.$$

Hence by (7) and (3), with  $m$  replaced by an odd number  $q$ ,

$$f(2, n) = f(2, a) \cdot f(2, b), \quad f(q, n) = f(q, a) \cdot f(q, b).$$

The extension to the case in which  $n$  is the product  $abc \cdots$  of several factors is evident. Hence, using (5), we get

$$(8) \quad f(m, n) = f(m, a) \cdot f(m, b) \cdot f(m, c) \cdots.$$

6. Let  $x$  be the product of the factors in the numerator of  $A$  (§ 1) and  $y$  the product of those in the denominator of  $A$ . Set  $\eta = (-1)^{\frac{(n-1)(n-3)}{8}}$ . As shown by GAUSS,\*

$$\eta x = 1 + s^m + s^{2m} + \cdots + s^{m(n-1)^2}, \quad \eta y = 1 + s + s^4 + \cdots + s^{(n-1)^2}.$$

First, let  $n$  be a prime, and let  $\alpha$  range over the quadratic residues ( $< n$ ) of  $n$ , and  $\beta$  over the non-residues. Then

$$\eta y = 1 + 2\Sigma s^\alpha, \quad \eta x = 1 + 2\Sigma s^\alpha \quad \text{or} \quad 1 + 2\Sigma s^\beta,$$

according as  $m$  is a quadratic residue or non-residue. Hence

$$x = y, \quad f(m, n) = x/y = 1,$$

if  $m$  be a residue of  $n$ ; while if  $m$  be a non-residue,

$$\eta(x+y) = 2(1 + \Sigma s^\alpha + \Sigma s^\beta) = 0, \quad f(m, n) = -1.$$

Hence, if  $n$  is a prime,  $f(m, n)$  is identical with Legendre's symbol  $(m/n)$ .

Next, let  $n = abc \dots$ , where  $a, b, \dots$  are primes. Then, by (8),

$$f(m, n) = \left(\frac{m}{a}\right) \left(\frac{m}{b}\right) \left(\frac{m}{c}\right) \dots$$

Thus  $f(m, n)$  is identical with Jacobi's symbol  $(m/n)$ .

\* *Disquisitiones arithmeticae*, German translation by MASER, 1889, p. 474.