THE SIXTEENTH POWER RESIDUE CHARACTER OF 2

A. L. WHITEMAN

1. Introduction. The problem of giving a criterion for the eth power residue character of 2 has long interested number theorists. This paper is primarily concerned with the cases $e = 4$, 8 and 16. Gauss **(8)** proved that 2 is a biquadratic residue of a prime p of the form $4n + 1$ if and only if p is representable as $x^2 + 64y^2$. A simple demonstration of this result is due to Dirichlet **(7)**. Reuschle **(13)** stated, but did not prove, the following criterion for the octavic character of 2: Let p be a prime of the form $8n + 1$. If n is even, then 2 is an octavic residue of p if and only if p is representable as $x^2 + 256y^2$; if n is odd, then 2 is an octavic residue of p if and only if p is representable as $x^2 + 64y^2$ but not as $x^2 + 256y^2$. The first proof of Reuschle's criterion was given by Western **(14)**.

Cunningham **(4)** examined the first 118 primes of which 2 is an octavic residue. On the basis of the evidence he conjectured a criterion for the 16th power (sextodecimic) residue character of 2 which may be stated as follows: Let z denote an odd number. The number 2 is a 16th power residue of a prime p of the form $16n + 1$ if and only if p is simultaneously representable in the forms $x^2 + 1024y^2$ and $x^2 + 128y^2$ or in the forms $x^2 + 256z^2$ and $x^2 + 32z^2$. Aigner **(1)** rediscovered Cunningham's criterion and gave the first proof. His method employs class field theory. Beeger **(3)** noted that Cunningham's criterion may be deduced from some complicated formulas about the field of eighth roots of unity stated without proof by Goldscheider **(9)**.

In the present paper the theory of cyclotomy (division of the circle) is employed to prove the criteria of Gauss, Reuschle and Cunningham. This is the method created by Gauss to derive the biquadratic character of 2, and it is surprising that it has not previously been used to derive the 8th and 16th power residue characters of 2.

It is natural to ask for a criterion giving the 32nd power residue character of 2. Such a criterion is yet to be discovered. It is hoped that the present paper constitutes a first step in this direction.

Before proceeding to the proofs, we find it useful to make some preliminary comments about the eth power residues of an odd prime p. Let g denote a fixed primitive root of p. For an integer a not divisible by p, the index of a (ind a) is defined by the congruence $a \equiv g^{\text{ind } a} \pmod{p}$. Let E denote the highest common divisor of e and $p - 1$. Then the eth power residues (mod p) are precisely those numbers whose indices are divisible by E. Consequently the number of eth power residues (mod p) is $(p - 1)/E$. If a is an eth power residue, the congruence $x^e \equiv a \pmod{p}$ has exactly E solutions. The extension of

Received March 2, 1953. This investigation was supported by the Office of Naval Research.

Euler's criterion for primes p of the form $ef + 1$ states that an integer a is an eth power residue of p if and only if $a^{(p-1)/e} \equiv 1 \pmod{p}$.

Suppose now that the conditions are known under which 2 is an eth power residue of p for $e = 2, 2^2, \ldots, 2^{k-1}$. These include the results for $e = 2^k$ except when $p \equiv 1 \pmod{2^k}$. For otherwise, since $E = (2^k, p - 1)$, we have $E = 2^l$, $l < k$, and then the results for $e = 2^k$ are included in the results for 2^l.

2. Cyclotomy. For proofs of the basic formulas in the theory of cyclotomy, the reader should consult the treatise of Bachmann **(2)** or the memoir of Dickson **(6)**.

Let p be an odd prime and e a divisor of $p - 1$. Let g be a fixed primitive root of p and write $p - 1 = ef$. The cyclotomic number (h, k) is the number of values of y, $1 \leqslant y \leqslant p - 2$, for which

$$y \equiv g^{es+h}, \quad 1 + y \equiv g^{et+k} \pmod{p}, \tag{2.1}$$

where the values of s and t are each selected from the integers $0, 1, \ldots, f - 1$. Noting that $g^{ef} \equiv 1 \pmod{p}$, we may infer immediately that the value of (h, k) is unchanged if either h or k is augmented by a multiple of e. The symbol (h, k) also has the following properties **(2**, pp. 201-203**)**:

$$(h, k) = (e - h, k - h); \tag{2.2}$$

$$(h, k) = \begin{cases} (k, h) & (f \text{ even}), \\ (k + \tfrac{1}{2}e, h + \tfrac{1}{2}e) & (f \text{ odd}); \end{cases} \tag{2.3}$$

$$\sum_{k=0}^{e-1} (h, k) = \begin{cases} f - 1 & (h = 0, f \text{ even or } h = \tfrac{1}{2}e, f \text{ odd}), \\ f & (\text{otherwise}). \end{cases} \tag{2.4}$$

Let m, n denote integers and put $\beta = \exp(2\pi i/e)$. Then we define the Jacobi sum **(2**, p. 122**)**

$$\psi(\beta^m, \beta^n) = \sum_{a=0}^{p-1} \beta^{m \operatorname{ind} a + n \operatorname{ind}(1-a)}, \tag{2.5}$$

where the convention is made that $\beta^{\operatorname{ind}(0)} = 0$. Now replace m in (2.5) by vn, where v is an integer. For $a \neq 0$, replace a by $-a$ and put $a = g^b$. Observing that $\beta^{\operatorname{ind}(-1)} = \beta^{\frac{1}{2}ef} = (-1)^f$, we find that (2.5) becomes

$$\psi(\beta^{vn}, \beta^n) = (-1)^{vnf} \sum_{b=0}^{p-2} \beta^{(vb + \operatorname{ind}'(1+g^b))n}.$$

In the last sum, we collect those exponents of β which are in the same residue class (mod e). Put

$$b = es + h, \quad 0 \leqslant h \leqslant e - 1, \quad 0 \leqslant s \leqslant f - 1.$$

For a fixed value of h, the number of solutions of the congruence

$$vh + \operatorname{ind}(1 + g^{es+h}) \equiv i \pmod{e}$$

is the same as the number of solutions of the congruence

$$1 + g^{es+h} \equiv g^{et+(i-vh)} \pmod{p}, \quad 0 \leqslant s, t \leqslant f - 1,$$

and hence is equal to the cyclotomic number $(h, i - vh)$. The finite Fourier series expansion of $\psi(\beta^{vn}, \beta^n)$ is therefore given by

$$\psi(\beta^{vn}, \beta^n) = (-1)^{vnf} \sum_{i=0}^{e-1} B(i, v)\, \beta^{ni}, \tag{2.6}$$

where

$$B(i, v) = \sum_{h=0}^{e-1} (h, i - vh). \tag{2.7}$$

The sum $B(i, v)$ has been studied by Dickson **(5)** and by Hurwitz **(11)**. From (2.3) and (2.4) it follows that

$$B(i, 0) = \sum_{h=0}^{e-1} (h, i) = \begin{cases} f - 1 & (i = 0), \\ f & (1 \leqslant i \leqslant e - 1). \end{cases} \tag{2.8}$$

We have also the identity

$$B(i, v) = B(i, e - v - 1). \tag{2.9}$$

To prove (2.9) we employ (2.2). Then we get

$$\sum_{h=0}^{e-1} (h, i - vh) = \sum_{h=0}^{e-1} (e - h, i - vh - h) = \sum_{h=0}^{e-1} (h, i - (e - v - 1)\, h).$$

We next let α denote a root of the equation $\alpha^{p-1} = 1$ and put $\zeta = \exp(2\pi i/p)$. The Jacobi sum (2.5) is closely related to the Lagrange sum **(2**, p. 83**)** defined by

$$\tau(\alpha) = \sum_{a=0}^{p-1} \alpha^{\operatorname{ind} a} \zeta^a. \tag{2.10}$$

Indeed we have the formula **(2**, p. 86**)**

$$\psi(\beta^m, \beta^n) = \tau(\beta^m)\, \tau(\beta^n)/\tau(\beta^{m+n}), \tag{2.11}$$

when $m + n$ is not divisible by e. We have also the easily proved formula **(2**, p. 87**)**

$$\tau(\beta^n)\, \tau(\beta^{-n}) = (-1)^{nf} p, \tag{2.12}$$

if n is not divisible by e. Using (2.11) and (2.12) we may deduce at once that

$$\psi(\beta^m, \beta^n) = \psi(\beta^n, \beta^m) = (-1)^{nf}\, \psi(\beta^{-m-n}, \beta^n), \tag{2.13}$$

and **(2**, p. 123**)**

$$\psi(\beta^m, \beta^n)\, \psi(\beta^{-m}, \beta^{-n}) = p, \tag{2.14}$$

provided no one of m, n, $m + n$ is divisible by e.

Jacobi **(12**, p. 167**)** stated without proof the following property of the Lagrange sum (2.10). If the integer m is defined by the congruence $g^m \equiv 2 \pmod{p}$, then

$$\tau(-1)\, \tau(\alpha^2) = \alpha^{2m}\, \tau(\alpha)\, \tau(-\alpha). \tag{2.15}$$

A proof of (2.15) attributed to H. H. Mitchell is given by Dickson **(6**, p. 407**)**. Another proof appears in the book of Hasse **(10**, p. 442**)**.

We shall require the following lemma.

LEMMA. *If* $e = 2^k$, $k \geqslant 1$ *and* $B(i, v)$ *is defined by* (2.7), *then*

$$(2.16) \qquad \sum_{v=0}^{\frac{1}{2}e-1} (B(i, v) - B(i + \tfrac{1}{2}e, v)) = \tfrac{1}{2}e((0, i) - (0, i + \tfrac{1}{2}e)).$$

In order to establish (2.16) we use (2.7) and get

$$(2.17) \qquad \sum_{v=0}^{e-1} B(i, v) = \sum_{v=0}^{e-1} \sum_{h=0}^{e-1} (h, i - vh) = e\,(0, i) + \sum_{h=1}^{e-1} \sum_{v=0}^{e-1} (h, i - vh).$$

Now replace i by $i + \frac{1}{2}e$. For a fixed value of h, $1 \leqslant h \leqslant e - 1$, put

$$h = 2^a b,\ 0 \leqslant a \leqslant k - 1,\ b \text{ odd}.$$

Since e is a power of 2 and b is odd, vb runs over a complete residue system (mod e) whenever v does. Hence we obtain

$$(2.18) \qquad \begin{aligned} -e(0, i + \tfrac{1}{2}e) + \sum_{v=0}^{e-1} B(i + \tfrac{1}{2}e, v) &= \sum_{h=1}^{e-1} \sum_{v=0}^{e-1} (h, i + 2^a(2^{k-1-a} - vb)) \\ &= \sum_{h=1}^{e-1} \sum_{v=0}^{e-1} (h, i - 2^a vb) = \sum_{h=1}^{e-1} \sum_{v=0}^{e-1} (h, i - vh). \end{aligned}$$

Subtracting (2.18) from (2.17) we derive the identity

$$\sum_{v=0}^{e-1} (B(i, v) - B(i + \tfrac{1}{2}e, v)) = e((0, i) - (0, i + \tfrac{1}{2}e)).$$

The Lemma now follows at once with the aid of (2.9).

3. The biquadratic character of 2. We consider the case $e = 4$ of §2 and divide the discussion into two parts.

(i) *f even.* The assumption f even is, of course, necessary in order that 2 be a biquadratic residue of p. In this case the relations which follow from (2.2) and (2.3) may be summarized schematically by means of the matrix

$$(3.1) \qquad \begin{vmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{vmatrix},$$

in which the letter in the hth row and kth column ($h, k = 0, 1, 2, 3$) represents the value of the cyclotomic number (h, k). Applying (2.4) for $h = 0, 1, 2$ and using (3.1), we get

$$(3.2) \qquad A + B + C + D = f - 1, \quad B + D + 2E = f, \quad C + E = \tfrac{1}{2}f.$$

Returning to (2.6) we see that in this case $\beta = \exp(2\pi i/4) = i$. Take

https://doi.org/10.4153/CJM-1954-035-8 Published online by Cambridge University Press

$v = n = 1$ and note that $\psi(i^3, i^3)$ is the complex conjugate of $\psi(i, i)$. Evidently (2.14) implies

$$\psi(i, i) = a + bi, \quad a = B(01) - B(21), \quad b = B(11) - B(31), \tag{3.3}$$

where $p = a^2 + b^2$. Also we have from (2.7) and (3.1)

$$B(01) = A + C + 2E, \quad B(11) = 2B + 2E, \quad B(21) = B + 2C + D, \quad B(31) = 2D + 2E. \tag{3.4}$$

By (3.4) and the first of (3.2) the formulas for a and b in (3.3) reduce to $a = 2A + 2E - f + 1$ and $b = 2B - 2D$. Since a is odd and b is even it follows that b is actually divisible by 4. Eliminating B, C and D from the three equations in (3.2) we get $2A = 6E - f - 2$. Also we obtain immediately $B + D = 2C$. It follows that

$$a = 8E - 2f - 1, \quad \tfrac{1}{4}b = B - C. \tag{3.5}$$

The second formula in (3.5) may be used to deduce at once the criterion of Gauss stated in the introduction. We note that the symbol (h, h) represents the number of integers y, $1 \leqslant y \leqslant p - 2$, for which

$$y \equiv g^{4s+h}, \quad 1 + y \equiv g^{4t+h} \pmod{p}, \qquad 0 \leqslant s, t \leqslant f - 1.$$

For every such y there exists a complementary y, since $p - y - 1 \equiv g^{4t+2f+h}$, $p - y \equiv g^{4s+2f+h} \pmod{p}$. These two y's will be distinct unless $y = \frac{1}{2}(p - 1)$, in which case $2 \equiv g^{-4s+2f-h} \pmod{p}$. Conversely, if $2 \equiv g^{4u-h} \pmod{p}$, then $\frac{1}{2}(p - 1) \equiv g^{-4u+2f+h} \pmod{p}$ and $\frac{1}{2}(p + 1) \equiv g^{-4u+4f+h} \pmod{p}$, and hence (h, h) will be odd. Since 2 is a quadratic residue of p it follows that $B = (33)$ is even; also $C = (22)$ is even if and only if 2 is a biquadratic residue of p. Hence $\frac{1}{4}b$ is even if and only if 2 is a biquadratic residue of p. Thus we have proved the theorem of Gauss **(8**, p. 89**)**.

THEOREM 1. *Let $p = a^2 + b^2$, a odd, b even, be a prime of the form $4n + 1$. If 2 is a quadratic residue of p, then $2^{(p-1)/4} \equiv (-1)^{b/4} \pmod{p}$.*

The result in Theorem 1 may also be formulated by stating that if 2 is a quadratic residue of p, then $\operatorname{ind} 2 \equiv \frac{1}{2}b \pmod 4$. Clearly the validity of this congruence does not depend upon the choice of the sign of b.

(ii) *f odd.* In this case 2 is a quadratic nonresidue of p and $\frac{1}{2}b \equiv \pm 1 \pmod 4$ depending upon the choice of the sign of b. Following the lines of the argument in the case f even we may readily prove again that $\operatorname{ind} 2 \equiv \frac{1}{2}b \pmod 4$. This result is, however, ambiguous. For 2 is congruent to a number of the form g^{4s+1} or $g^{4s+3} \pmod{p}$ depending upon the choice of the primitive root g.

4. The octavic character of 2. In this section we again consider the case $e = 4$, f even. Our discussion is based upon the congruence $2 \equiv g^f(1 - g^f)^2 \pmod{p}$ which, in turn, implies

$$2^{(p-1)/8} \equiv g^{f(p-1)/8}(1 - g^f)^{(p-1)/4} \pmod{p}. \tag{4.1}$$

In order to determine the biquadratic character of $1 - g^f$ we proceed as

follows. There are exactly $\frac{1}{4}(p-1)$ roots of the congruence $x^{(p-1)/4} - g^f \equiv 0 \pmod{p}$, and these roots are given by the numbers $\beta_i \equiv g^{4i+1} \pmod{p}$, $i = 1, 2, \ldots, \frac{1}{4}(p-1)$. Hence we have the factorization

$$x^{(p-1)/4} - g^f \equiv (x-\beta_1)(x-\beta_2)\ldots(x-\beta_f) \pmod{p}. \tag{4.2}$$

Putting $x = -1$ in (4.2) we get

$$1 - g^f \equiv (1+\beta_1)(1+\beta_2)\ldots(1+\beta_f) \pmod{p}. \tag{4.3}$$

From (3.1) and the definition of the cyclotomic number (h, k) in (2.1) it is clear that (4.3) implies

$$\text{ind}\,(1-g^f) \equiv (11) + 2(12) + 3(13) \equiv D + E \pmod{4}. \tag{4.4}$$

By (3.2) and the second of (3.5) we have $D + E = (C + E) - (B - C) = f/2 - b/4$. Hence by (4.4), $\text{ind}\,(1-g^f) \equiv \frac{1}{2}f - \frac{1}{4}b \pmod{4}$. Congruence (4.1) may now be written in the form

$$2^{(p-1)/8} \equiv g^{f(f-b/4)} \pmod{p}. \tag{4.5}$$

At this point we assume that 2 is a biquadratic residue of p. By Theorem 1 $b \equiv 0 \pmod{8}$. We consider two cases: Case 1, $f \equiv 0 \pmod{4}$, $b \equiv 0 \pmod{16}$ or $f \equiv 2 \pmod{4}$, $b \equiv 8 \pmod{16}$; Case 2, $f \equiv 0 \pmod{4}$, $b \equiv 8 \pmod{16}$ or $f \equiv 2 \pmod{4}$, $b \equiv 0 \pmod{16}$. Then we find that (4.5) becomes

$$2^{(p-1)/8} \equiv \begin{cases} 1 \pmod{p} & \text{(Case 1)}, \\ -1 \pmod{p} & \text{(Case 2)}. \end{cases} \tag{4.6}$$

The result in (4.6) implies the criterion of Reuschle **(13**, p. 14**)** stated in the introduction. This criterion is also expressed in

THEOREM 2. *Let 2 be a biquadratic residue of a prime $p = a^2 + b^2$, a odd, b even, of the form $8n + 1$. If n is even, then $2^{(p-1)/8} \equiv (-1)^{b/8} \pmod{p}$; if n is odd, then $2^{(p-1)/8} \equiv (-1)^{b/8+1} \pmod{p}$.*

5. The sextodecimic character of 2. We now consider the case $e = 8$, f even of §2. A summary of the relations which may be derived from (2.2) and (2.3) is given in the matrix

$$\begin{vmatrix} A & B & C & D & E & F & G & H \\ B & H & I & J & K & L & M & I \\ C & I & G & M & N & O & N & J \\ D & J & M & F & L & O & O & K \\ E & K & N & L & E & K & N & L \\ F & L & O & O & K & D & J & M \\ G & M & N & O & N & J & C & I \\ H & I & J & K & L & M & I & B \end{vmatrix}, \tag{5.1}$$

where the element in the hth and kth column $(h, k = 0, 1, \ldots, 7)$ denotes the cyclotomic number (h, k). Of course, the letters in the matrix (5.1) represent different cyclotomic numbers than the letters in the matrix (3.1). In order to

avoid confusion we shall not refer explicitly to letters of matrix (3.1) again. Applying (2.4) for $h = 0, 1, 2, 3$ and 4, we now get

$$A+B+C+D+E+F+G+H = f-1, \quad B+H+2I = D+F+2O,$$
$$C+G+I+J+M+2N+O = f, \quad E+K+L+N = \tfrac{1}{2}f. \tag{5.2}$$

We next return to the sum $B(i, v)$ defined in (2.7). For future reference we give a list of formulas which may be derived with the aid of (5.1). To save space the plus signs between the consecutive terms in the right members of these formulas have been omitted.

$$\begin{aligned}
&B(01)=AINOEONI, \quad B(11)=BBJOKKOJ, \quad B(41)=EJGJEMCM,\\
&B(51)=FKMMKFII, \qquad\quad B(13)=B(33)=BMMDKOIL,\\
&B(23)=B(63)=CINJNOGM, \quad B(53)=B(73)=FIJLKJOH,\\
&B(02)=AMNMEJNJ, \qquad\quad B(12)=B(52)=BIOFKMJK\\
&B(32)=B(72)=DHJOLLIM, \quad B(42)=EICOEOGI.
\end{aligned} \tag{5.3}$$

Since $e = 8$ in this case we have $\beta = \exp(2\pi i/8)$. In (2.6) put $v = 2$, $n = 1$ and $v = 3$, $n = 1$. Note that $\psi(\beta^6, \beta^7)$ is the conjugate of $\psi(\beta^2, \beta)$, and that $\psi(\beta^5, \beta^7)$ is the conjugate of $\psi(\beta^3, \beta)$. If we now make use of the appropriate formulas in (5.3), we may readily verify that (2.14) implies

$$\psi(\beta^2, \beta) = a + bi, \quad a = B(02) - B(42), \quad b = B(22) - B(62), \tag{5.4}$$

and

$$\psi(\beta^3, \beta) = c + d(\beta + \beta^3), \tag{5.5}$$
$$c = B(03) - B(43), \quad d = B(13) - B(53) = B(33) - B(73),$$

where $p = a^2 + b^2 = c^2 + 2d^2$.

In the Jacobi formula (2.15) replace α by β and by β^3. We thus get

$$\tau(\beta^4)\,\tau(\beta^2)/\tau(\beta^6) = \beta^{2m}\,\tau(\beta^5)\,\tau(\beta)/\tau(\beta^6),$$
$$\tau(\beta^6)\,\tau(\beta)/\tau(\beta^7) = \beta^{6m}\,\tau(\beta^3)\,\tau(\beta)/\tau(\beta^4).$$

By (2.13) we have

$$\psi(\beta^4, \beta^2) = \psi(\beta^2, \beta^2), \quad \psi(\beta^5, \beta) = (-1)^f\psi(\beta^2, \beta), \quad \psi(\beta^6, \beta) = (-1)^f\psi(\beta, \beta).$$

Hence (2.11) implies

$$\psi(\beta, \beta) = (-1)^f\beta^{6m}\psi(\beta^3, \beta), \quad \psi(\beta^2, \beta^2) = (-1)^f\beta^{2m}\psi(\beta^2, \beta), \tag{5.6}$$
$$(g^m \equiv 2 \pmod p).$$

Later we shall assume that 2 is an octavic residue of p. At this point it suffices to assume merely that $m \equiv 0 \pmod 4$. Since f is even we derive from (5.5) and the first equation in (5.6) the relations

$$c = B(01) - B(41), \quad 0 = B(21) - B(61), \tag{5.7}$$
$$d = B(11) - B(51) = B(31) - B(71),$$

where c and d are defined in (5.5).

We are now in the position to apply the lemma of §2. The results thus far obtained provide us with explicit values for each term of the sum in the left member of (2.16). Consider first the case $i = 0$. By (2.8)

https://doi.org/10.4153/CJM-1954-035-8 Published online by Cambridge University Press

$$-1 = B(00) - B(40);$$

by (5.5) and (5.7)

$$c = B(01) - B(41) = B(03) - B(43);$$

by (5.4)

$$a = B(02) - B(42).$$

Again in the case $i = 1$ we have by (2.8)

$$0 = B(10) - B(50);$$

by (5.5) and (5.7)

$$d = B(11) - B(51) = B(13) - B(53);$$

by (5.3)

$$0 = B(12) - B(52).$$

Proceeding in a similar fashion for $i = 2$ and 3 and using (5.1), we find that (2.16) yields

(5.8) $\quad a + 2c - 1 = 4A - 4E, \quad \frac{1}{2}d = B - F = D - H, \quad \frac{1}{4}b = C - G.$

The first equation in (5.8) will not be needed in the sequel. We remark, however, that it may be used to construct another proof of Theorem 2. From the second equation in (5.8) we get at once $B + H = D + F$. Comparing this result with the second equation in (5.2) we conclude that $I = 0$. By (5.5) and (5.7) we have

$$B(11) + B(53) = B(13) + B(51).$$

Substituting from the appropriate formulas of (5.3) we may verify that this equation reduces to the identity $J = M$. We have thus established the two simple relations

(5.9) $$I = 0, \quad J = M,$$

under the assumption that $m \equiv 0 \pmod 4$. We remark that it may also be proved that $I = 0$ when $m \equiv 2 \pmod 4$.

Since $\psi(\beta^2, \beta^2) = \psi(i, i)$ we see from the second equation in (5.6) that the number a defined in (3.3) has the same sign as the number a defined in (5.4). Replacing the f which appears in (3.5) by $2f$ we get

$$a = 8(12)_4 - 4f - 1,$$

where the meaning of the subscript is clear. Since the new f is even the sign of a is determined by means of the congruence $a \equiv -1 \pmod 8$. Let us now observe that a number which is of the form $g^{4s+h} \pmod p$ is of the form either g^{8t+h} or $g^{8t+h+4} \pmod p$. From the definition of the cyclotomic number (h, k) in (2.1) it follows that

$$(12)_4 = (12)_8 + (16)_8 + (52)_8 + (56)_8 = I + M + O + J.$$

Hence we get $a = 8I + 8J + 8M + 8O - 4f - 1$. In view of (5.9) this reduces to

(5.10) $$a = 16I + 16J - 4f - 1.$$

From (5.4) and (5.7) we get $a - c = B(02) + B(41) - B(01) - B(42)$.

Using the appropriate formulas of (5.3) together with (5.9) we find that this reduces to $a - c = 8J - 8I$. Consequently $a \equiv c \pmod 8$. Combining the last equation with (5.10) we obtain

$$64I = p + 1 - 2a + 4c, \tag{5.11}$$

where the signs of a and c are determined by means of the congruence $a \equiv c \equiv -1 \pmod 8$. Again we point out that (5.10) and (5.11) have been derived under the assumption that m is divisible by 4.

To obtain a criterion for the 16th power residue character of 2 we make use of the congruence

$$2^{(p-1)/16} \equiv g^{f(p-1)/8}(1 - g^{2f})^{(p-1)/8} \pmod p, \tag{5.12}$$

which corresponds to (4.1). We must next determine the octavic character of $1 - g^{2f}$. The $\frac{1}{8}(p-1)$ roots of the congruence $x^{(p-1)/8} - g^{2f} \equiv 0 \pmod p$ are given by the numbers $\gamma_i \equiv g^{8i+2} \pmod p$, $i = 1, 2, \ldots, \frac{1}{8}(p-1)$. We therefore have the factorization

$$x^{(p-1)/8} - g^{2f} \equiv (x - \gamma_1)(x - \gamma_2) \ldots (x - \gamma_f) \pmod p. \tag{5.13}$$

For $x = -1$ (5.13) becomes

$$1 - g^{2f} \equiv (1 + \gamma_1)(1 + \gamma_2) \ldots (1 + \gamma_f) \pmod p. \tag{5.14}$$

Then, as in §4, we get making use of (5.1), (5.9) and (5.14)

$$\begin{aligned} \operatorname{ind}(1 - g^{2f}) &\equiv 1(21) + 2(22) + 3(23) + 4(24) + 5(25) + 6(26) + 7(27) \\ &\equiv -2I + 2G + 2J + 2N \pmod 8. \end{aligned} \tag{5.15}$$

Applying (5.9) to the third equation of (5.2) we have also $2J + 2N = f - C - G - 2I$. Using this result in conjunction with the formula for $\frac{1}{4}b$ in (5.8) we find that (5.15) simplifies to

$$\operatorname{ind}(1 - g^{2f}) \equiv f + 4I - b/4 \pmod 8.$$

The congruence (5.12) may now be put into the form

$$2^{(p-1)/16} \equiv g^{f(2f+4I-b/4)} \pmod p. \tag{5.16}$$

Now we assume that the integer m defined in (5.6) is actually divisible by 8. This is equivalent to the assumption that 2 is an octavic residue of p. Returning to the equation

$$p = a^2 + b^2 = c^2 + 2d^2, \qquad a \equiv c \equiv -1 \pmod 8,$$

we note that the congruence $c^2 + 2d^2 \equiv 1 \pmod{16}$ implies that $d \equiv 0 \pmod 4$. Furthermore it is easy to verify that $2f \equiv 0$ or $4 \pmod 8$ according as $a \equiv -1$ or $-9 \pmod{16}$. By Theorem 2, $b \equiv 0 \pmod{16}$. Hence $p \equiv a^2 \pmod{256}$. We consider separately two cases:

(i) $d \equiv 0 \pmod 8$. In this case we get $c^2 \equiv a^2 \pmod{128}$, whence $c \equiv a \pmod{64}$. Converting (5.11) into a congruence (mod 256), we find that $64I \equiv (a+1)^2 \pmod{256}$. If $a \equiv -1 \pmod{16}$, then $4I \equiv 0 \pmod{16}$. If

$a \equiv -9 \pmod{16}$, then $4I \equiv 4 \pmod{16}$. In either event, it is clear that $2f + 4I \equiv 0 \pmod{8}$.

(ii) $d \equiv 4 \pmod{8}$. In this case we get $c^2 \equiv a^2 - 32 \pmod{128}$, whence $c \equiv a + 16 \pmod{64}$. The equation (5.11) reduces to the congruence $64I \equiv (a+1)^2 + 64 \pmod{256}$. If $a \equiv -1 \pmod{16}$, then $4I \equiv 4 \pmod{16}$. If $a \equiv -9 \pmod{16}$, then $4I \equiv 8 \pmod{16}$. In either event we get $2f + 4I \equiv 4 \pmod{8}$.

The results derived in (i) and (ii) may be combined into the single congruence $2f + 4I \equiv d \pmod{8}$. The congruence (5.16) now becomes $2^{(p-1)/16} \equiv g^{f(d-b/4)} \equiv g^{f(d+b/4)} \pmod{p}$. We conclude that

$$2^{(p-1)/16} \equiv \begin{cases} 1, & (b/16) + (d/4) \equiv 0 \pmod{2}, \\ -1, & (b/16) + (d/4) \equiv 1 \pmod{2}. \end{cases}$$

This completes the proof of

THEOREM 3. *Let $p = a^2 + b^2 = c^2 + 2d^2$, a and c odd, be a prime of the form $16n + 1$. If $2^{(p-1)/8} \equiv 1 \pmod{p}$, then $2^{(p-1)/16} \equiv (-1)^{(b/16)+(d/4)} \pmod{p}$.*

Theorem 3 is the criterion of Cunningham **(4**, p. 88**)**.

REFERENCES

1. A. Aigner, *Kriterion zum 8. and 16. Potenzcharacter der Reste* 2 *und* $-$ 2, Deutsche Math., *4* (1939), 44–52.
2. P. Bachmann, *Die Lehre von der Kreisteilung* (Leipzig, 1872).
3. N. G. W. H. Beeger, *A problem of the theory of numbers and its history*, Nieuw Arch. Wiskunde (2), *22* (1948), 306–309.
4. A. Cunningham, *On* 2 *as a* 16*-ic residue*, Proc. London Math. Soc. (1), *27* (1895), 85–122.
5. L. E. Dickson, *On the congruence* $x^n + y^n + z^n \equiv 0 \pmod{p}$, J. Reine Angew. Math., *135* (1909), 134–142.
6. ———, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., *57* (1935), 391–424.
7. G. L. Dirichlet, *Ueber den biquadratischen Character der Zahl "Zwei,"* J. Reine Angew. Math., *57* (1860), 187–188; or *Werke*, *2* (1897), 261–262.
8. C. F. Gauss, *Werke*, *2* (1876), 67–92.
9. F. Goldscheider, *Das Reziprozitätsgesetz der 8-ten Potenzreste*, Wissensch. Beitr. z. Progr. d. Luisenstädischen Realgymn. (Berlin, 1899), 29 pp.
10. H. Hasse, *Vorlesungen über Zahlentheorie* (Berlin, Göttingen, Heidelberg, 1950).
11. A. Hurwitz, *Ueber die Kongruenz* $ax^e + by^e + cz^e \equiv 0 \pmod{p}$, J. Reine Angew. Math., *136* (1909), 272–292; or *Mathematische Werke*, *2* (1933), 430–445.
12. C. G. J. Jacobi, *Ueber die Kreisteilung und ihre Anwendung auf die Zahlentheorie*, J. Reine Angew. Math., *30* (1846), 166–182; or *Gesammelte Werke*, *6* (1891), 254–274.
13. C. G. Reuschle, *Mathematische Abhandlung, enthaltend neue Zahlentheoretische Tabellen*, Programm zum Schlusse des Schuljahrs 1855–56 am Königlichen Gymnasium zu Stuttgart (1856), 61 pp.
14. A. E. Western, *Some criteria for the residues of eighth and other powers*, Proc. London Math. Soc. (2), *9* (1911), 244–272.

The Institute for Advanced Study and
University of Southern California