THE CYCLOTOMIC NUMBERS OF ORDER SIXTEEN[1]

BY

ALBERT LEON WHITEMAN

1. **Introduction.** 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 $(i, j) = (i, j)_e$ is the number of values of y, $1 \leqq y \leqq p-2$, for which

$$y \equiv g^{es+i}, \; 1 + y \equiv g^{et+j} \qquad (\text{mod } p),$$

where the values of s and t are each selected from the integers $0, 1, \cdots, f-1$. Dickson [5] showed in the case $e=8$ that $64(i, j)$ is expressible for each i, j as a linear combination with integral coefficients of p, x, y, a and b, where

$$p = x^2 + 4y^2 = a^2 + 2b^2 \qquad (x \equiv a \equiv 1 \; (\text{mod } 4)), \tag{1.1}$$

and where the signs of y and b depend on the choice of the primitive root g. There are four sets of formulas depending on whether f is even or odd and whether 2 is a biquadratic residue or not.

Emma Lehmer [8] raised the question whether or not constants α, β, γ, δ, ϵ can be found such that

$$256(i, j)_{16} = p + \alpha x + \beta y, + \gamma a + \delta b + \epsilon, \tag{1.2}$$

at least for some (i, j). To answer this question she undertook the following experiment on the SWAC (National Bureau of Standards Western Automatic Computer). The cyclotomic constants of order sixteen were computed for eight primes p of the form $32n+1$ for which 2 is not a biquadratic residue. She found that (1.2) is not satisfied for any $(i, j)_{16}$ when the signs of y and b are taken in accordance with the results on cyclotomic constants of order eight. A similar computation for primes p of the form $32n+17$ also led to a negative result.

The SWAC experiment leaves open the question of determining if the equation (1.2) can be satisfied for any prime p for which 2 is a biquadratic residue. In the present paper this is answered in the affirmative for six of the cyclotomic constants. The following formulas involving only p, a and x are derived. Let $p=16f+1$ be a prime. If the integer m is defined by the congruence $g^m \equiv 2$ (mod p), then

Presented to the Society August 30, 1955; received by the editors July 24, 1956.

(1) This research was supported by the Office of Naval Research under Contract NR 043-182.

The author wishes to express his thanks to the referee for a number of valuable suggestions.

$$(1.3)\qquad 256(0,0)_{16} = p - 47 - 18x \qquad (f \text{ even}, m \equiv 4 \pmod 8)),$$

$$(1.4)\qquad 256(8,0)_{16} = p - 15 - 18x - 32a \qquad (f \text{ even}, m \equiv 4 \pmod 8)),$$

$$(1.5)\qquad 256(4,8)_{16} = p + 1 - 2x \qquad (f \text{ even}, m \equiv 0 \pmod 8)),$$

$$(1.6)\qquad 256(0,0)_{16} = p - 31 - 18x - 16a \qquad (f \text{ odd}, m \equiv 0 \pmod 8)),$$

$$(1.7)\qquad 256(0,8)_{16} = p + 1 - 18x - 48a \qquad (f \text{ odd}, m \equiv 0 \pmod 8)),$$

$$(1.8)\qquad 256(4,0)_{16} = p - 15 - 2x + 16a \qquad (f \text{ odd}, m \equiv 4 \pmod 8)),$$

where the signs of a and x are selected so that $a \equiv x \equiv 1 \pmod 4$. In other cases it is shown that the cyclotomic constants $(i, j)_{16}$ are such that $256(i, j)_{16}$ is expressible as a linear combination with integer coefficients of p, a, b, x, y and certain other integers $c_0, c_1, c_2, c_3, d_0, d_1, \cdots, d_7$ defined in §3.

The results in §3 provide a useful tool for investigating the existence of difference sets composed of sixteenth power residues modulo p. By a difference set of order k and multiplicity λ is meant a set of k elements $a_1, a_2, \cdots, a_k \pmod v$ such that the congruence $a_i - a_j \equiv d \pmod v$ has exactly λ solutions for $d \not\equiv 0 \pmod v$. Residue difference sets are difference sets composed of eth power residues modulo a prime. It is well known that the $(p-1)/2 = k$ quadratic residues modulo a prime $p \equiv 3 \pmod 4$ form a difference set of multiplicity $\lambda = (p-3)/4$. Chowla [2] proved that the $(p-1)/4 = k$ biquadratic residues modulo p form a difference set of multiplicity $\lambda = (p-5)/16$ if $(p-1)/4$ is an odd square. Emma Lehmer [7] proved that the set of octic residues modulo p forms a difference set if and only if the number of terms $k = (p-1)/8$ and the multiplicity $\lambda = (p-9)/64$ are both odd squares. It is proved in §4 that the set of sixteenth power residues modulo p cannot form a difference set if 2 is an octic residue of p. Whether such difference sets exist when 2 is not an octic residue of p remains an unsolved problem.

It is a known result [7] that the number 2 is an eth power residue of p if and only if $(0, 0)_e$ is odd. In §5 the expressions for $(0, 0)_{16}$ are employed to deduce a new proof of the Cunningham-Aigner criterion [3; 1] for the sixteenth power residue character of 2.

2. **Cyclotomy.** The following basic properties of the cyclotomic numbers are established in the paper of Dickson [5].

$$(2.1)\qquad (i, j) = (e - i, j - i),$$

$$(2.2)\qquad (i, j) = \begin{cases} (j, i) & (f \text{ even}), \\ (j + e/2, i + e/2) & (f \text{ odd}); \end{cases}$$

$$(2.3)\qquad \sum_{i=0}^{e-1} (i, j) = \begin{cases} f - 1 & (j = 0), \\ f & (1 \leqq j \leqq e - 1). \end{cases}$$

When e is even we put $e = 2E$ and define

$$(2.4)\qquad s(i, j) = (i, j) - (i, j + E), \quad t(i, j) = (i, j) - (i + E, j).$$

The notation $s(i, j)$ should, of course, not be confused with s times (i, j). By (2.2) we have

$$(2.5)\qquad t(i, j) = \begin{cases} s(j, i) & (f \text{ even}), \\ s(j + E, i + E) & (f \text{ odd}). \end{cases}$$

We also have the easily proved formula

$$(2.6)\qquad (i, j)_E = (i, j) + (i + E, j) + (i, j + E) + (i + E, j + E).$$

The last result is a consequence of the fact that a number of the form $g^{Es+i} \pmod p$ is either of the form g^{et+i} or $g^{et+i+E} \pmod p$.

Let m, n denote integers and put $\beta = \exp(2\pi i/e)$. Then we define the Jacobi sum [6]

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

where $\beta^{\text{ind}(0)} = 0$. Two important properties of the Jacobi sum are

$$(2.7)\qquad \psi(\beta^m, \beta^n) = \psi(\beta^n, \beta^m) = (-1)^{nf}\psi(\beta^{-m-n}, \beta^n),$$

and

$$(2.8)\qquad \psi(\beta^m, \beta^n)\psi(\beta^{-m}, \beta^{-n}) = p,$$

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

The finite Fourier series expansion of $\psi(\beta^{vn}, \beta^n)$ is given by

$$(2.9)\qquad \psi(\beta^{vn}, \beta^n) = (-1)^{vnf} \sum_{i=0}^{e-1} B(i, v)\beta^{ni},$$

where the coefficient

$$(2.10)\qquad B(i, v) = \sum_{h=0}^{e-1} (h, i - vh)$$

is a Dickson-Hurwitz sum [10]. By (2.3) $B(i, 0)$ equals $f-1$ or f according as i is divisible by e or not. We have also the identity

$$(2.11)\qquad B(i, v) = B(i, e - v - 1).$$

We next let α denote a root of the equation $\alpha^{p-1} = 1$ and put $\zeta = \exp(2\pi i/p)$. The Lagrange sum

$$\tau(\alpha) = \sum_{a=0}^{p-1} \alpha^{\text{ind } a}\zeta^a$$

is related to the Jacobi sum by means of the formula

$$\psi(\beta^m, \beta^n) = \tau(\beta^m)\tau(\beta^n)/\tau(\beta^{m+n}), \tag{2.12}$$

provided $m+n$ is not divisible by e. Another important property of the Lagrange sum is given in the formula [6]

$$\tau(-1)\tau(\alpha^2) = \alpha^{2m}\tau(\alpha)\tau(-\alpha) \qquad (g^m \equiv 2 \pmod{p}). \tag{2.13}$$

We now prove two lemmas of which the second is a generalization of a lemma given by the author in an earlier paper [10].

LEMMA 1. *If e is even and $E=e/2$, then*

$$4(i, j)_e = (i, j)_E + s(i, j) + s(i + E, j) + 2t(i, j), \tag{2.14}$$

where $s(i, j)$ and $t(i, j)$ are defined in (2.4).

This lemma follows from (2.4) and (2.6).

LEMMA 2. *Let $e=2^k$, $E=2^{k-1}$, $k\geqq 1$ and let $B(i, v)$ be defined by* (2.10). *Then for any integer j we have*

$$\sum_{v=0}^{e-1} (B(i + jv, v) - B(i + E + jv, v)) = es(j, i). \tag{2.15}$$

To prove Lemma 2 we first deduce from (2.10) the relation

$$\sum_{v=0}^{e-1} B(i + jv, v) = e(j, i) + \sum_{v=0}^{e-1}\sum_{h=1}^{e-1} (h + j, i - vh). \tag{2.16}$$

Now replace i by $i+E$. For a fixed value of h, $1\leqq h\leqq e-1$, put

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

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

$$\begin{aligned} \sum_{v=0}^{e-1}\sum_{h=1}^{e-1} (h + j, i + E - vh) &= \sum_{h=1}^{e-1}\sum_{v=0}^{e-1}(h + j, i + 2^a(2^{k-1-a} - vb)) \\ &= \sum_{h=1}^{e-1}\sum_{v=0}^{e-1} (h + j, i + 2^a(-vb)) \\ &= \sum_{v=0}^{e-1}\sum_{h=1}^{e-1} (h + j, i - vh). \end{aligned} \tag{2.17}$$

Subtracting the left member of (2.17) from the left member of (2.16) we obtain (2.15). This completes the proof of the lemma.

3. **Determination of the cyclotomic constants of order sixteen.** When e is a power of 2 Lemmas 1 and 2 provide a technique for calculating the value of $(i, j)_e$ given the value of $(i, j)_E$. For this purpose we require the values of the successive terms of the sum in (2.15). In this section we take $e=16$, $E=8$ and derive formulas for the values of $B(k, v)-B(k+8, v)$, $k=i+jv$, $v=0, 1, \cdots, 15$. The following lemma will be used frequently.

LEMMA 3. *If $e=2^k$, $k\geqq 1$ and q is an odd integer, then*

$$B(i, \bar{q}) = B(qi, q), \tag{3.1}$$

where $\bar{q}$ is any solution of the congruence $q\bar{q} \equiv 1 \pmod{e}$.

In (2.10) replace i by qi, v by q and h by $i-qh$. As h runs over a complete residue system (mod e) so does $i-qh$. Therefore by (2.2)

$$B(qi, q) = \sum_{h=0}^{e-1}\left(q^2h + \frac{1}{2}ef, i - qh + \frac{1}{2}ef\right). \tag{3.2}$$

Now replace h by $\bar{q}^2h$ and use (2.2) again. Then the right member of (3.2) reduces after simplification to the sum for $B(i, \bar{q})$. This completes the proof of the lemma.

Put $p=16f+1$ and $\beta=\exp(2\pi i/16)$. We now make five applications of (2.13) with $\alpha=\beta, \beta^2, \beta^3, \beta^6, \beta^7$ respectively. Using (2.7) and (2.12) we get with a little manipulation

$$\psi(\beta^6, \beta^2) = \psi(\beta^8, \beta^2) = (-1)^f\beta^{2m}\psi(\beta^6, \beta), \tag{3.3a}$$

$$\psi(\beta^4, \beta^4) = \psi(\beta^8, \beta^4) = \beta^{4m}\psi(\beta^4, \beta^2), \tag{3.3b}$$

$$\psi(\beta^6, \beta^2) = \psi(\beta^8, \beta^6) = \beta^{6m}\psi(\beta^{11}, \beta^3), \tag{3.3c}$$

$$\psi(\beta^6, \beta^2) = \beta^{4m}\psi(\beta^{12}, \beta^2), \tag{3.3d}$$

$$\psi(\beta^7, \beta) = \beta^{2m}\psi(\beta^{14}, \beta) = (-1)^f\beta^{2m}\psi(\beta, \beta), \tag{3.3e}$$

where the integer m is defined by the congruence $g^m\equiv 2 \pmod{p}$.

By (2.8) and (2.9) it is clear that $\psi(\beta^{-4}, \beta^{-4})$ is the complex conjugate of $\psi(\beta^4, \beta^4)$. Employing the notation used by Dickson [5] and making use of (2.9) we may write

$$\psi(\beta^4, \beta^4) = -x + 2yi, \qquad p = x^2 + 4y^2. \tag{3.4}$$

The finite Fourier series expansion of $\psi(\beta^4, \beta^2)$ is given by (2.9) with $v=2$, $n=2$. Introducing this expansion into (3.3b) and equating coefficients of like powers of β we get the formulas

$$\begin{aligned} B(0, 2) - B(4, 2) + B(8, 2) - B(12, 2) &= (-1)^{(m+2)/2}x, \\ B(2, 2) - B(6, 2) + B(10, 2) - B(14, 2) &= (-1)^{m/2}2y. \end{aligned} \tag{3.5}$$

Again by (2.8) and (2.9) we see that $\psi(\beta^{-6}, \beta^{-2})$ is the complex conjugate of $\psi(\beta^6, \beta^2)$. By (2.9) we have (compare [10])

$$\psi(\beta^6, \beta^2) = -a + b(\beta^2 + \beta^6), \qquad p = a^2 + 2b^2. \tag{3.6}$$

In the sequel it will be convenient to distinguish the following four cases:

First case; $m \equiv 0 \pmod 8$, f even or $m \equiv 4 \pmod 8$, f odd.

Second case; $m \equiv 0 \pmod 8$, f odd or $m \equiv 4 \pmod 8$, f even.

Third case; $m \equiv 2 \pmod 8$, f even or $m \equiv 6 \pmod 8$, f odd.

Fourth case; $m \equiv 2 \pmod 8$, f odd or $m \equiv 6 \pmod 8$, f even.

The finite Fourier series expansion of $\psi(\beta^6, \beta)$ is given by (2.9) with $v=6$, $n=1$. Comparing coefficients in (3.3a) and (3.6) we obtain in the first case

$$\begin{aligned} -a &= B(0, 6) - B(8, 6), \\ b &= B(2, 6) - B(10, 6) = B(6, 6) - B(14, 6), \\ 0 &= B(4, 6) - B(12, 6). \end{aligned} \tag{3.7}$$

Equations (3.7) are valid in the second case when $-a$ is replaced by a and b is replaced by $-b$. For the third case we have the formulas

$$\begin{aligned} a &= B(4, 6) - B(12, 6), \\ b &= -\left[B(6, 6) - B(14, 6)\right] = B(2, 6) - B(10, 6), \\ 0 &= B(0, 6) - B(8, 6). \end{aligned} \tag{3.8}$$

Equations (3.8) are valid in the fourth case when a is replaced by $-a$ and b is replaced by $-b$.

Formulas (3.7) and (3.8) yield values for $B(i, 6) - B(i+8, 6)$ when i is even. When i is odd we put $e=16$, $q=9$ in (3.1) and deduce readily with the aid of (2.11) that

$$B(i, 6) - B(i + 8, 6) = 0 \qquad (i \text{ odd}). \tag{3.9}$$

We next put $v=7$, $n=1$ in (2.9). Then we may write

$$\psi(\beta^7, \beta) = (-1)^f \sum_{i=0}^{7} c_i\beta^i, \qquad c_i = B(i, 7) - B(i + 8, 7). \tag{3.10}$$

By (3.1) with $q=7$ we have $B(i, 7) = B(7i, 7)$. This yields the formulas

$$c_1 = c_7, \qquad c_2 = -c_6, \qquad c_3 = c_5, \qquad c_4 = 0. \tag{3.11}$$

The following formulas now follow from (2.9) and (3.3e).

$$\begin{aligned} c_i &= B(i, 1) - B(i + 8, 1) && \text{(First case)}, \\ c_i &= B(i - 4, 1) - B(i + 4, 1) && \text{(Third case)}. \end{aligned} \tag{3.12}$$

When c_i is replaced by $-c_i$ the first and third cases of (3.12) are transformed into the second and fourth cases, respectively.

Finally we put $v=2$, $n=1$ in (2.9). Then we may write

$$\psi(\beta^2, \beta) = \sum_{i=0}^{7} d_i\beta^i, \qquad d_i = B(i, 2) - B(i+8, 2). \tag{3.13}$$

Comparing (3.3c) and (3.3d) we get $\psi(\beta^{12}, \beta^2) = \beta^{2m}\psi(\beta^{11}, \beta^3)$. We next multiply both members of the last equation by $\tau(\beta)\tau(\beta^{14})/\tau(\beta^3)\tau(\beta^{12})$ and make use of (2.7) and (2.12) to obtain

$$\psi(\beta^2, \beta) = (-1)^f\beta^{2m}\psi(\beta^4, \beta). \tag{3.14}$$

Therefore by (3.13), (3.14) and (2.9) with $v=4$, $n=1$, we get after equating coefficients

$$\begin{aligned} d_i &= B(i, 4) - B(i+8, 4) && \text{(First case)},\\ d_i &= B(i-4, 4) - B(i+4, 4) && \text{(Third case)}. \end{aligned} \tag{3.15}$$

The first and third cases of (3.15) are transformed into the second and fourth cases when d_i is replaced by $-d_i$.

By (2.11) and (3.1) with $q=3$ and 5 we have $B(i, 4) = B(3i, 3)$ and $B(i, 2) = B(5i, 5)$. These results lead to the formulas

$$B(i, 4) - B(i+8, 4) = B(3i, 3) - B(3i+8, 3), \tag{3.16}$$

and

$$d_i = B(5i, 5) - B(5i+8, 5), \tag{3.17}$$

which are, of course, valid in all four cases.

By means of formulas (3.7), $\cdots$, (3.17) in conjunction with formulas (2.3) and (2.11) the sum in Lemma 2 can be expressed as a linear combination of a, b, c_i and d_i. In [9] Emma Lehmer has tabulated the values of the 64 constants $(i, j)_8$. These values are expressible in terms of p, x, y, a and b, where the signs of x and a are such that $x \equiv a \equiv 1 \pmod 4$. Employing the method indicated by Lemmas 1 and 2 the present author has, in turn, calculated the values of each of the 256 constants $(i, j)_{16}$. There are eight sets of formulas depending on the parity of f and the eighth power residue character of 2. Of the 408 essentially different formulas there are only six which, fortunately, do not involve the c's and d's. These are the especially simple formulas (1.3), $\cdots$, (1.8) cited in the introduction.

It should be noted that in some instances the result in Lemma 1 may be simplified. Thus it follows from (2.2) and (2.4) that $t(i, j) = 0$ when f is even and $j=8$ or when f is odd and $j=0$. The application of Lemma 2 may also be simplified by making use of the result

$$\text{(3.18)}\quad \sum_{v=0}^{(e-2)/2} (B(i+2jv,2v) - B(i+E+2jv,2v)) = E(s(j,i) + s(j+E,i)).$$

To establish (3.18) we replace j by $j+E$ in Lemma 2. Then the vth term in the sum of (2.15) is multiplied by $(-1)^v$ and (3.18) follows easily.

To illustrate the technique of calculating a value of $(i, j)_{16}$ we now give the details of the computation of the formula

$$\text{(3.19)}\quad \begin{aligned} 256(0,2)_{16} = p &- 15 + 6x + 16b + 16y + 8c_0 + 32c_2 \\ &- 16d_0 + 16d_2 + 16d_4 + 16d_6, \end{aligned}$$

which is valid when f is even, $m\equiv 0 \pmod 8$. From the table in [9] we have when 2 is a biquadratic residue of a prime $p\equiv 1 \pmod{16}$, $64(0,2)_8 = p-7+6x+16y$. Using the classification of cases given immediately after formula (3.6), we find that in the first case the 8 consecutive terms of the sum (3.18) for $i=2, j=0$ are given by $0, d_2, d_2, b, c_2, -d_2, d_6, c_2$. Therefore $8(s(0,2)+s(8,2)) = b+2c_2+d_2+d_6$. We find also that the 16 consecutive terms of the sum (2.15) for $i=0, j=2$ are given by $-1, c_2, d_4, d_2, -d_0, d_2, 0, c_2, c_0, b, d_4, d_6, -d_0, -d_2, 0, 0$. Therefore $16t(0,2) = 16s(2,0) = -1+b+c_0+2c_2-2d_0+d_2+2d_4+d_6$. Formula (3.19) now follows at once from the identity $256(0,2)_{16} = 64(0,2)_8 + 64s(0,2) + 64s(8,2) + 128t(0,2)$.

In checking a numerical instance of a formula such as (3.19) the following remark should be kept in mind. Dickson [5] has shown in the case $e=8$ that the formulas for the cyclotomic numbers $64(i,j)_8$ are such that $x\equiv a\equiv 1 \pmod 4$. Formula (3.5) not only provides a check on the value of x but renders y unambiguous. Similarly, formulas (3.7) and (3.8) determines a and b without ambiguity.

4. **Application to residue difference sets.** The following theorem is due to Emma Lehmer [7]: If e is even and $f=(p-1)/e$ is odd, then a necessary and sufficient condition for the set of eth power residues modulo p to form a difference set is that $(i,0) = (f-1)/e$, $i=0, 1, \cdots, e/2-1$, where $(f-1)/e = \lambda$ is the multiplicity of the difference set. We shall now give an application of this result in the case $e=16$, f odd, $m\equiv 0 \pmod 8$. The values of the cyclotomic constants $(i,0)_{16}$ are tabulated in Table IV of the appendix. Making use of these results we may verify the relation $128((1,0)+(5,0)-(3,0)-(7,0))+256((2,0)-(6,0)) = 64y$. The condition $(i,0) = (p-17)/256$, $i=0, 1, \cdots, 7$ now implies the absurd conclusion $y=0$. Thus we have proved the following theorem.

THEOREM 1. *If 2 is an octic residue of p, then the set of 16th power residues modulo p cannot form a difference set.*

It is not necessary to give a separate proof of this theorem for the case f even. For it is known [7] that there exists no residue difference set for e odd, or for e even and f even.

Whether the set of 16th power residues can form a difference set when 2 is not an octic residue of p is not known. However, when f is odd and $m \equiv 4 \pmod 8$, formula (1.8) together with the equation $256(4, 0) = p - 17$ leads to the necessary condition $8a = x - 1$, where $a \equiv x \equiv 1 \pmod 4$. An examination of Cunningham's table [4] of quadratic partitions of primes p less than 100,000 has revealed only one instance in which the three conditions f odd, $m \equiv 4 \pmod 8$ and $8a = x - 1$ are simultaneously satisfied. The single example is $p = 98{,}321$ with $x = -311$ and $a = -39$. There are therefore no difference sets with $m \equiv 4 \pmod 8$ below this limit.

When f is odd and $m \equiv 2 \pmod 8$ we employ the formulas for $(i, 0)$ given in Table V of the appendix. We may thus establish

$$128((1,0) - (3, 0) + (5,0) - (7, 0)) - 256((0, 0) - (4, 0)) = -16x + 16.$$

The condition that the numbers $(i, 0)$ be equal therefore implies that $x = 1$. The condition $256(2, 0) = p - 17$ now yields $y = 2d_4$. Finally the relation

$$256((0, 0) - (2,0) + (4, 0) - (6, 0)) = -16 - 64d_4 + 16a$$

leads to $a = 1 + 2y$. This equation together with $x = 1$ implies that $p = 1 + b^4$. We conclude that when 2 is not a biquadratic residue of p a necessary condition for the set of sixteenth powers to form a difference set is that $p = 1 + b^4$. By the table in [8] the first example of $p = 1297$ does not give a residue difference set. The next example is $p = 1336337$ so that there are no difference sets of the prescribed type below this limit. It should also be noted that when f is odd and $m \equiv 6 \pmod 8$ the equations $x = 1$, $a = 1 - 2y$ again lead to $p = 1 + b^4$.

A modified residue difference set is one in which zero is counted as a residue. It is known [7] that such difference sets cannot exist for e odd, or for e even and f even. Emma Lehmer [7] has proved that if e is even and $f = (p-1)/e$ is odd, then a necessary and sufficient condition for the set of eth power residues and zero to be a difference set is that $1 + (0, 0) = (i, 0) = (f+1)/e$, $i = 1, 2, \cdots, e/2 - 1$, where $(f+1)/e = \lambda$ is the multiplicity of the set. Proceeding exactly as in the proof of Theorem 1 we obtain

THEOREM 1′. *If 2 is an octic residue of p, then the set of 16th power residues and zero modulo p cannot form a difference set.*

Suppose now that f is odd and $m \equiv 4 \pmod 8$. Then by (1.8) the condition $256(4, 0) = p + 15$ is equivalent to the condition $8a = x + 15$. Hence in order for the set of 16th power residues and zero to be a difference set it is necessary that $8a = x + 15$, where $x \equiv a \equiv 1 \pmod 4$. There is not a single example in Cunningham's table in which this relation is satisfied.

Finally suppose that f is odd and 2 is not a biquadratic residue of p. The method used in the case of ordinary residue difference sets may be applied again. This time we deduce that a necessary condition for the set of sixteenth powers and zero to form a difference set is that $x=-15$, $a=-15\pm 2y$, where the sign is plus or minus according as $m\equiv\pm 2 \pmod 8$. It follows that $b^2=\pm 30y$. Since a and b cannot both be multiples of 5 there is no difference set in this case.

5. **The sixteenth power residue character of 2.** An integer n is said to belong to the residue class i with respect to a primitive root g if $n\equiv g^{es+i} \pmod p$. We shall make use of the easily proved lemma [7]: the cyclotomic numbers $(0, i)$ are odd or even according as 2 belongs to the residue class i or not. Employing this lemma we may now verify the criterion of Cunningham [3] and Aigner [1] for the sixteenth power residue character of 2 (compare the proof in [10]).

Suppose to begin with that 2 is a biquadratic residue of a prime p of the form $16f+1$. From the first of the two formulas [9]

$$64(2, 4)_8 = p + 1 - 2x, \qquad 64(2, 5)_8 = p + 1 + 2x - 4a,$$

we deduce that $x\equiv 1$ or $9 \pmod{16}$ according as f is even or odd. From the second formula we see that $a\equiv 1 \pmod 8$. The congruence $a^2+2b^2\equiv 1 \pmod{16}$ now implies that $b\equiv 0 \pmod 4$.

We next assume that 2 is also an octic residue of p. Then, by Reuschle's criterion [10] for octic residuacity, we have $y\equiv 0 \pmod 8$. Returning to (1.1) we may now derive the two congruences

$$p \equiv x^2 + 32y \pmod{512}, \qquad a \equiv x - 4b \pmod{32}. \tag{5.1}$$

The lemma asserts that $256(0, 0)\equiv 256$ or $0 \pmod{512}$ according as 2 belongs to the residue class 0 or 8. It is convenient to consider separately two cases. We examine the easier case first.

(i) f odd, $m\equiv 0 \pmod 8$. We make use of (5.1) and the fact that $x\equiv 9 \pmod{16}$. Converting (1.6) into a congruence modulo 512 we get

$$256(0, 0) \equiv 32y + 64b + 256 \pmod{512}. \tag{5.2}$$

(ii) f even, $m\equiv 0 \pmod 8$. In addition to the values of $256(0, 0)$ and $256(4, 0)$ listed in Table I of the appendix we have also the formulas

$$\begin{aligned} 256(1, 8) &= p + 1 + 2x + 4a + 16y + 8b + 8c_0 - 8c_2 - 16d_2 - 16d_4, \\ 256(2, 8) &= p + 1 + 6x + 16y - 8c_0 - 16d_0 - 16d_4, \\ 256(5, 8) &= p + 1 + 2x + 4a + 16y - 8b + 8c_0 + 8c_2 + 16d_2 - 16d_4. \end{aligned}$$

From these equations we obtain the result

$$\begin{aligned} &256[(0, 0) - 6((1, 8) + (2, 8) + (5, 8)) - 9(4, 0)] \\ &\qquad = -26p + 70 - 60x - 240a - 288y. \end{aligned}$$

Since 2 belongs to the residue class 0 or 8 it follows from the lemma that (4, 0) is even. Therefore

$$(5.3)\qquad 256(0,0) \equiv -26p + 70 - 60x - 240a - 288y \pmod{512}.$$

Just as in the derivation of (5.2) we may now use (5.1) and the fact that $x \equiv 1 \pmod{16}$ to verify that the right member of (5.3) is congruent to $32y+64b+256 \pmod{512}$.

In either event we conclude that 2 is a 16th power residue modulo p or not according as $32y+64b\equiv 0$ or $256 \pmod{512}$. We have therefore proved the following theorem.

THEOREM 2. *Let $p=x^2+4y^2=a^2+2b^2$ be a prime of the form $16f+1$. If 2 is an octic residue of p, then $2^{(p-1)/16}\equiv(-1)^{(y/8)+(b/4)} \pmod{p}$.*

APPENDIX: Cyclotomic constants $(i, 0)$ of order 16.

The 256 constants $(i, j)_{16}$ have at most 51 different values for a given p. These values are expressible in terms of p, x, y, a and b in (1.1) and the numbers $c_0, c_1, c_2, c_3, d_0, d_1, \cdots, d_7$ defined in §3. There are eight cases depending on the parity of f and the eighth power residue character of 2. Because of the application to residue difference sets the values of the 16 special constants $(i, 0)$, $i=0, \cdots, 15$ are of particular interest. These values are given by the relations contained in the following tables. It should be noted that when f is odd the value of $(i, 0)$, $i=8, \cdots, 15$ may be calculated from the relation $(i, 0)=(i+8, 0)$. When $m\equiv 6 \pmod 8$ a table of values for $(i, 0)$ may be deduced from the table corresponding to $m\equiv 2 \pmod 8$. For this purpose make the following transformations: replace $(i, 0)$ by $(-i, 0)$ and replace the letters $x, y, a, b, d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7, c_0, c_1, c_2, c_3$ by $x, -y, a, -b, d_0, -d_7, -d_6, -d_5, -d_4, -d_3, -d_2, -d_1, c_0, -c_1, c_2, -c_3$, respectively.

TABLE I. f even, $m\equiv 0 \pmod 8$.

$256(0,0)=p-47-18x-48a+96d_0+48c_0$
$256(1,0)=p-15+2x+16y+4a+24b+32d_1+16d_2-16d_3+16d_4-16d_5-8c_0+32c_1+8c_2$
$256(2,0)=p-15+6x+16y+16b-16d_0+16d_2+16d_4+16d_6+8c_0+32c_2$
$256(3,0)=p-15+2x-16y+4a+24b+16d_1+32d_3-16d_4+16d_6+16d_7-8c_0-8c_2+32c_3$
$256(4,0)=p-15-2x+16a+32d_4$
$256(5,0)=p-15+2x+16y+4a-24b+16d_1-16d_2+16d_4+32d_5+16d_7-8c_0-8c_2+32c_3$
$256(6,0)=p-15+6x-16y+16b-16d_0+16d_2-16d_4+16d_6+8c_0-32c_2$
$256(7,0)=p-15+2x-16y+4a-24b-16d_3-16d_4-16d_5-16d_6+32d_7-8c_0+32c_1+8c_2$
$256(8,0)=p-15-18x-16a-32d_0-16c_0$
$256(9,0)=p-15+2x+16y+4a+24b-32d_1+16d_2+16d_3+16d_4+16d_5-8c_0-32c_1+8c_2$
$256(10,0)=p-15+6x+16y-16b-16d_0-16d_2+16d_4-16d_6+8c_0-32c_2$
$256(11,0)=p-15+2x-16y+4a+24b-16d_1-32d_3-16d_4+16d_6-16d_7-8c_0-8c_2-32c_3$
$256(12,0)=p-15-2x+16a-32d_4$
$256(13,0)=p-15+2x+16y+4a-24b-16d_1-16d_2+16d_4-32d_5-16d_7-8c_0-8c_2-32c_3$
$256(14,0)=p-15+6x-16y-16b-16d_0-16d_2-16d_4-16d_6+8c_0+32c_2$
$256(15,0)=p-15+2x-16y+4a-24b+16d_3-16d_4+16d_5-16d_6-32d_7-8c_0-32c_1+8c_2$

TABLE II. f even, $m\equiv 2 \pmod 8$.

$$256(0,0)=p-47+6x+48d_0+48d_4+24c_0$$
$$256(1,0)=p-15+2x+4a-8b-16d_0+16d_1+16d_2-16d_7-8c_0+16c_1+8c_2+16c_3$$
$$256(2,0)=p-15-2x-16y-16a+16b-16d_2+16d_6+16c_0$$
$$256(3,0)=p-15+2x+4a+8b+16d_0+16d_3+16d_5+16d_6+32d_7-8c_0+16c_1+8c_2+16c_3$$
$$256(4,0)=p-15-10x+16a-16d_0+48d_4-8c_0$$
$$256(5,0)=p-15+2x+4a+8b-16d_0-16d_2-16d_3+16d_5-8c_0-16c_1-8c_2+16c_3$$
$$256(6,0)=p-15-2x+16y-16b-16d_2-32d_4+16d_6-32c_2$$
$$256(7,0)=p-15+2x+4a-8b+16d_0+16d_1-32d_3-16d_6+16d_7-8c_0+16c_1-8c_2-16c_3$$
$$256(8,0)=p-15+6x-16d_0-16d_4-8c_0$$
$$256(9,0)=p-15+2x+4a-8b-16d_0-16d_1+16d_2+16d_7-8c_0-16c_1+8c_2-16c_3$$
$$256(10,0)=p-15-2x-16y-16a-16b+16d_2-16d_6+16c_0$$
$$256(11,0)=p-15+2x+4a+8b+16d_0-16d_3-16d_5+16d_6-32d_7-8c_0-16c_1+8c_2-16c_3$$
$$256(12,0)=p-15-10x-16a-16d_0-16d_4+24c_0$$
$$256(13,0)=p-15+2x+4a+8b-16d_0-16d_2+16d_3-16d_5-8c_0+16c_1-8c_2-16c_3$$
$$256(14,0)=p-15-2x+16y+16b+16d_2-32d_4-16d_6+32c_2$$
$$256(15,0)=p-15+2x+4a-8b+16d_0-16d_1+32d_3-16d_6-16d_7-8c_0-16c_1-8c_2+16c_3$$

TABLE III. f even, $m\equiv 4 \pmod 8$.

$$256(0,0)=p-47-18x$$
$$256(1,0)=p-15+2x+16y+4a+8b+16d_2+16d_3-16d_4-16d_5-8c_0-8c_2$$
$$256(2,0)=p-15+6x+16y-16b+16d_0-16d_2+16d_4-16d_6+8c_0$$
$$256(3,0)=p-15+2x-16y+4a+8b-16d_1+16d_4+16d_6+16d_7-8c_0+8c_2$$
$$256(4,0)=p-15-2x-32d_0+32d_4+16c_0$$
$$256(5,0)=p-15+2x+16y+4a-8b+16d_1-16d_2-16d_4-16d_7-8c_0+8c_2$$
$$256(6,0)=p-15+6x-16y-16b+16d_0-16d_2-16d_4-16d_6+8c_0$$
$$256(7,0)=p-15+2x-16y+4a-8b-16d_3+16d_4+16d_5-16d_6-8c_0-8c_2$$
$$256(8,0)=p-15-18x-32a$$
$$256(9,0)=p-15+2x+16y+4a+8b+16d_2-16d_3-16d_4+16d_5-8c_0-8c_2$$
$$256(10,0)=p-15+6x+16y+16b+16d_0+16d_2+16d_4+16d_6+8c_0$$
$$256(11,0)=p-15+2x-16y+4a+8b+16d_1+16d_4+16d_6-16d_7-8c_0+8c_2$$
$$256(12,0)=p-15-2x-32d_0-32d_4+16c_0$$
$$256(13,0)=p-15+2x+16y+4a-8b-16d_1-16d_2-16d_4+16d_7-8c_0+8c_2$$
$$256(14,0)=p-15+6x-16y+16b+16d_0+16d_2-16d_4+16d_6+8c_0$$
$$256(15,0)=p-15+2x-16y+4a-8b+16d_3+16d_4-16d_5-16d_6-8c_0-8c_2$$

TABLE IV. f odd, $m\equiv 0 \pmod 8$.

$$256(0,0)=p-31-18x-16a$$
$$256(1,0)=p-15+2x+16y+4a+8b+16d_2-16d_4-8c_0-8c_2$$
$$256(2,0)=p-15+6x+16y+16d_0+16d_4+8c_0$$
$$256(3,0)=p-15+2x-16y+4a+8b+16d_4+16d_6-8c_0+8c_2$$
$$256(4,0)=p-15-2x-32d_0+16c_0$$
$$256(5,0)=p-15+2x+16y+4a-8b-16d_2-16d_4-8c_0+8c_2$$
$$256(6,0)=p-15+6x-16y+16d_0-16d_4+8c_0$$
$$256(7,0)=p-15+2x-16y+4a-8b+16d_4-16d_6-8c_0-8c_2$$

TABLE V. f odd, $m \equiv 2 \pmod 8$.

$$256(0, 0) = p-31+6x+16d_0-16d_4+8c_0$$
$$256(1, 0) = p-15+2x+4a+8b+16d_0+16d_2-8c_0-8c_2$$
$$256(2, 0) = p-15-2x-16y+32d_4$$
$$256(3, 0) = p-15+2x+4a-8b-16d_0+16d_6-8c_0-8c_2$$
$$256(4, 0) = p-15-10x-16d_0-16d_4+8c_0$$
$$256(5, 0) = p-15+2x+4a-8b+16d_0-16d_2-8c_0+8c_2$$
$$256(6, 0) = p-15-2x+16y-16a+16c_0$$
$$256(7, 0) = p-15+2x+4a+8b-16d_0-16d_6-8c_0+8c_2$$

TABLE VI. f odd, $m \equiv 4 \pmod 8$.

$$256(0, 0) = p-31-18x-32a+32d_0+16c_0$$
$$256(1, 0) = p-15+2x+16y+4a+24b+16d_2+16d_4-8c_0+8c_2$$
$$256(2, 0) = p-15+6x+16y-16d_0+16d_4+8c_0$$
$$256(3, 0) = p-15+2x-16y+4a+24b-16d_4+16d_6-8c_0-8c_2$$
$$256(4, 0) = p-15-2x+16a$$
$$256(5, 0) = p-15+2x+16y+4a-24b-16d_2+16d_4-8c_0-8c_2$$
$$256(6, 0) = p-15+6x-16y-16d_0-16d_4+8c_0$$
$$256(7, 0) = p-15+2x-16y+4a-24b-16d_4-16d_6-8c_0+8c_2$$

References

1. A. Aigner, *Kriterion zum* 8. *und* 16. *Potenzcharacter der Reste* 2 *und* −2, Deutsche Math. vol. 4 (1939) pp. 44–52.

2. S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India Sect. A vol. 14 (1944) pp. 45–46.

3. A. Cunningham, *On* 2 *as a* 16-*ic residue*, Proc. London Math. Soc. (1) vol. 27 (1895) pp. 85–122.

4. ———, *Quadratic partitions*, London, 1904.

5. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. vol. 57 (1935) pp. 391–424.

6. H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin-Göttingen-Heidelberg, 1950.

7. E. Lehmer, *On residue difference sets*, Canadian J. Math. vol. 5 (1953) pp. 425–432.

8. ———, *On the cyclotomic numbers of order sixteen*, Canadian J. Math. vol. 6 (1954) pp. 449–454.

9. ———, *On the number of solutions of* $u^k+D\equiv w^2 \pmod p$, Pacific J. Math. vol. 5(1955) pp. 103–118.

10. A. L. Whiteman, *The sixteenth power residue character of* 2, Canadian J. Math. vol. 6 (1954) pp. 364–373.

University of Southern California,
Los Angeles, Calif.