ACTA ARITHMETICA
XVII (1970)

The cyclotomic numbers of order twenty

by

JOSEPH B. MUSKAT (Pittsburgh, Penn.)
and ALBERT L. WHITEMAN (Princeton, N. J.)*

1. Introduction. Let $p = ef+1$ be an odd prime. Let g be a fixed primitive root of p. The *cyclotomic number of order* e

$$(h, k) = (h, k)_e$$

is defined as the number of solutions of the congruence

$$g^{es+h}+1 \equiv g^{et+k} (\mathrm{mod}\, p), \quad 0 \leqslant h, k \leqslant e-1,\ 0 \leqslant s, t \leqslant f-1.$$

A central problem in the theory of cyclotomy is to obtain formulas for the cyclotomic numbers. The derivation of these formulas has three phases.

The first step is to express the cyclotomic numbers as linear combinations of coefficients of Jacobi sums of order e and cyclotomic numbers of orders which are divisors of e. The Jacobi sums $\psi(\beta^r, \beta^s) = \psi_e(\beta^r, \beta^s)$ of order e are defined as

$$(1.1) \qquad \psi(\beta^r, \beta^s) = \sum_{j=2}^{p-1} \beta^{r\,\mathrm{ind}_g j + s\,\mathrm{ind}_g (1-j)}, \quad \text{where} \quad \beta = \exp(2\pi i/e).$$

In the second phase equations relating different Jacobi sums are determined. This permits the equating of various coefficients of Jacobi sums. At the conclusion of this phase, each cyclotomic number is represented as a linear combination of a minimal set of Jacobi coefficients and differences of Jacobi coefficients of orders e and divisors of e. The significance of this is that the relatively few numbers of the minimal set of Jacobi coefficients contain essentially enough information to generate all the cyclotomic numbers of order e for the prime p.

In the third and final step, one seeks to replace the minimal set of Jacobi coefficients by coordinates of quadratic decompositions of p. The resulting representations of the cyclotomic numbers are more useful for certain applications.

* The research of the first author was supported in part under NSF grants GP 2091 and GP 5308. The research of the second author was sponsored in part under NSF grant G 24066.

(It does not follow, however, that if one is given merely the appropriate quadratic decompositions of p, he can compute explicitly the cyclotomic numbers of order e. The labeling of the cyclotomic numbers depends upon the choice of the primitive root g. Some of the identities between Jacobi sums depend upon the indices (mod e) of the prime divisors of e. In addition, for several values of e there are sign ambiguities in the equations relating certain Jacobi sums.)

Where formulas for the cyclotomic numbers of order e in terms of quadratic decompositions of p have been obtained, we shall say that a complete solution has been found. Complete solutions for $e = 2, 3, 4, 5$, and 6 were given by L. E. Dickson [4], for $e = 8$ by Emma Lehmer [11], and for $e = 10$ and 12 by A. L. Whiteman [15], [16]. In published solutions for $e = 9$ and 18 [2], $e = 14$ [12], and $e = 16$ [14], the third phase was not carried through completely. It follows from Theorem 6 of [7], however, that the solution for $e = 16$ is indeed complete.

The principal result of this paper is a complete solution for $e = 20$. As an application, we show that if 5 is a biquadratic residue of a prime $p \equiv 1 \pmod{20}$, then the set of twentieth power residues, with or without zero, does not form a difference set. Whether such difference sets exist where 5 is not a biquadratic residue remains unsolved.

2. Cyclotomy. In this section are gathered properties of cyclotomic numbers, Jacobi sums, and the Lagrange resolvent to be used in the study of the cyclotomic numbers of order 20.

If $h \equiv h' \pmod{e}$ and $k \equiv k' \pmod{e}$, the cyclotomic numbers (h, k) and (h', k') are equal, so that there are just e^2 cyclotomic numbers to be considered. Application of the well-known identities ([1], pp. 202–203)

$$(h, k) = (-h, k-h), \tag{2.1}$$

$$(h, k) = \begin{cases} (k, h) & (f \text{ even}), \\ (k+\tfrac{1}{2}e, h+\tfrac{1}{2}e) & (f \text{ odd}), \end{cases} \tag{2.2}$$

reduces the number of distinct cyclotomic numbers to

$$[(e^2+3e+6)/6]. \tag{2.3}$$

Proof of (2.3) where f is even: By (2.1) and (2.2),

$$\begin{aligned}(h, k) = (k, h) &= (-k, h-k) = (h-k, -k) = (k-h, -h) \\ &= (-h, k-h).\end{aligned} \tag{2.4}$$

Assume first that $3 \nmid e$. There are $(e-1)(e-2)$ ordered pairs (mod e) for which

$$h, k, h-k \not\equiv 0 \pmod{e}. \tag{2.5}$$

But if (2.5) is satisfied, the six ordered pairs in (2.4) are different. This accounts for $(e-1)(e-2)/6$ distinct cyclotomic numbers. If exactly one of h, k, and $h-k$ is divisible by e, then there are three different ordered pairs in (2.4). This accounts for $e-1$ distinct cyclotomic numbers. Finally, add one for $(0, 0)$. The total is $(e^2+3e+2)/6$. (Dickson ([5], Theorem 5 and Section 12) was familiar with this result for $e = q$ or $2q$, q a prime $\geqslant 5$.)

If $3 \mid e$, one adjustment must be made — if $h = e/3$, $k = 2e/3$, then there are only two different ordered pairs in (2.4). For all other h, k satisfying (2.5), the six ordered pairs in (2.4) are different. Together these account for $1+(e^2-3e)/6$ distinct cyclotomic numbers. Thus the total is

$$1+(e^2-3e)/6+e-1+1 = (e^2+3e+6)/6.$$

A similar analysis may be performed where f is odd.

Henceforth wherever e is even, let $e = 2E$. Define the differences

$$s(h, k) = (h, k)-(h, k+E), \quad t(h, k) = (h, k)-(h+E, k).$$

Then it follows from (2.2) that

$$t(h, k) = \begin{cases} s(k, h) & (f \text{ even}), \\ s(k+E, h+E) & (f \text{ odd}). \end{cases} \tag{2.6}$$

Let $e = yz$. Dickson showed that ([6], (2))

$$(h, k)_z = \sum_{n=0}^{y-1} \sum_{r=0}^{y-1} (h+nz, k+rz)_e. \tag{2.7}$$

By rearranging this identity in the case $y = 2$, $z = E$, Whiteman ([14], Lemma 1) showed that

$$4(h, k)_e = (h, k)_E+s(h, k)+s(h+E, k)+2t(h, k). \tag{2.8}$$

Turning now to Jacobi sums, we first set $s = 0$ in (1.1):

$$\psi(\beta^r, 1) = \begin{cases} p-2 & (e \mid r), \\ -1 & (e \nmid r). \end{cases} \tag{2.9}$$

Let $r+s+t \equiv 0 \pmod{e}$. It follows easily from (1.1) (compare [5], (9)) that

$$\begin{aligned}\psi(\beta^r, \beta^s) &= \psi(\beta^s, \beta^r) = (-1)^{sf}\psi(\beta^t, \beta^s) = (-1)^{sf}\psi(\beta^s, \beta^t) \\ &= (-1)^{rf}\psi(\beta^t, \beta^r) = (-1)^{rf}\psi(\beta^r, \beta^t).\end{aligned} \tag{2.10}$$

If e is divisible by at most two distinct primes, at least two of the six expressions in (2.10) can be written in the form $\pm\psi(\beta^{vn}, \beta^n)$. (By contrast, $\psi_{30}(\beta^2, \beta^3)$ cannot be represented in this manner.) Collecting the exponents

of β which lie in the same residue class (mod e) gives the following expansion of $\psi(\beta^{vn}, \beta^n)$ in a finite Fourier series (compare [13], Theorem 3):

$$\psi(\beta^{vn}, \beta^n) = (-1)^{vnf} \sum_{j=0}^{e-1} b(j, v)\beta^{nj}. \tag{2.11}$$

The *Jacobi coefficients* $b(j, v) = b_e(j, v)$ are Dickson–Hurwitz sums ([13], (6.2)) defined by

$$b(j, v) = \sum_{h=0}^{e-1} (h, j-vh). \tag{2.12}$$

They satisfy

$$b(j, v) = b(j, e-1-v) \qquad ([12], (2.7)), \tag{2.13}$$

$$b(j, 0) = \begin{cases} f-1 & (e \mid j), \\ f & (e \nmid j), \end{cases} \qquad ([1], \text{ p. } 201). \tag{2.14}$$

If $e = yz$ it follows easily from (2.11), or alternatively from (2.12) and (2.7), that

$$b_z(j, v) = \sum_{r=0}^{y-1} b_e(j+rz, v). \tag{2.15}$$

If $e = 2E$, define the *Jacobi difference*

$$d(j, v) = d_e(j, v) = b(j, v) - b(j+E, v). \tag{2.16}$$

Note that

$$d(j+E, v) = -d(j, v). \tag{2.17}$$

If $e = 2E$ and n is odd, (2.11) can be written as

$$\psi(\beta^{vn}, \beta^n) = (-1)^{vf} \sum_{j=0}^{E-1} d(j, v)\beta^{nj}. \tag{2.18}$$

If, in addition, E is odd, (2.18) can be written as

$$\psi(\beta^{vn}, \beta^n) = (-1)^{vf} \sum_{j=0}^{E-1} d(2j, v)\beta^{2nj}. \tag{2.19}$$

In particular, if $n = E$, applying (2.10) and (2.9) to (2.19) yields ([15], (5.10))

$$\sum_{j=0}^{E-1} d(2j, v) = -1. \tag{2.20}$$

We shall have occasion to refer to the following two lemmas:

LEMMA 1. *If $e = 2E$, then* ([17], Lemma 3))

$$b(j, E) + b(j+E, E) = \begin{cases} 2f-1 & (E \mid j), \\ 2f & (E \nmid j). \end{cases}$$

LEMMA 2. *If v is relatively prime to e, then $b(j, v) = b(\bar{v}j, \bar{v})$, where $\bar{v}$ satisfies $v\bar{v} \equiv 1 \pmod{e}$* ([15], Lemma 1).

Lemma 2 implies that if $e = 2E$ and v is relatively prime to e

$$d(j, v) = d(\bar{v}j, \bar{v}). \tag{2.21}$$

There are two especially interesting cases where E is even:

$$d(j, E-1) = d\big(j(E-1), E-1\big), \tag{2.22}$$

$$d(j, E+1) = d\big(j(E+1), E+1\big) = d(j+E, E+1) = 0 \quad (j \text{ odd}), \tag{2.23}$$

by (2.17).

The resolvent of Lagrange ([1], p. 83)

$$\tau(\beta^n) = \sum_{z=1}^{p-1} \beta^{n \operatorname{ind} z} \exp(2\pi i z/p)$$

is associated with the Jacobi sums through the relationship ([1], p. 86)

$$\psi(\beta^n, \beta^r) = \tau(\beta^n)\tau(\beta^r)/\tau(\beta^{n+r}), \tag{2.24}$$

provided $n+r$ is not divisible by e. By means of (2.24) we verify that

$$\psi(\beta^n, \beta^r)\psi(\beta^{n+r}, \beta^s) = \psi(\beta^n, \beta^s)\psi(\beta^{n+s}, \beta^r). \tag{2.25}$$

An important property of the resolvent is ([1], p. 87)

$$\tau(\beta^n)\tau(\beta^{-n}) = (-1)^{nf} p, \tag{2.26}$$

provided n is not divisible by e. Hence if e does not divide n, r, or $n+r$,

$$\psi(\beta^n, \beta^r)\psi(\beta^{-n}, \beta^{-r}) = p. \tag{2.27}$$

Two cases of a remarkable identity established by Davenport and Hasse ([3], (0.9)) will be used: If $e = 2E$,

$$\tau(\beta^E)\tau(\beta^{2t}) = \beta^{2tT}\tau(\beta^t)\tau(\beta^{t+E}), \qquad g^T \equiv 2 \pmod{p}. \tag{2.28}$$

If $5 \mid e$, let θ be a primitive fifth root of unity. Then

$$\tau(\beta^t)\tau(\beta^t\theta)\tau(\beta^t\theta^2)\tau(\beta^t\theta^3)\tau(\beta^t\theta^4) = \beta^{-5tF}p^2\tau(\beta^{5t}), \qquad g^F \equiv 5 \pmod{p}. \tag{2.29}$$

Let $e = 2E$; divide (2.28) by $\tau(\beta^{2t+E})$ and also by $\tau(\beta^{t+E})\tau(\beta^{2t})/\tau(\beta^t)$. In view of (2.24),

$$\psi(\beta^{2t}, \beta^E) = \beta^{2tT}\psi(\beta^t, \beta^{t+E}) \qquad (t \not\equiv \tfrac{1}{2}E \pmod{E}), \tag{2.30}$$

$$\psi(\beta^E, \beta^t) = \beta^{2tT}\psi(\beta^t, \beta^t) \qquad (t \not\equiv 0 \pmod{E}). \tag{2.31}$$

In (2.31) replace t by $2t$ and combine with (2.30):

$$\psi(\beta^{t+E}, \beta^t) = \beta^{2tT}\psi(\beta^{2t}, \beta^{2t}) \qquad (t \not\equiv 0, \tfrac{1}{2}E \pmod{E}). \tag{2.32}$$

3. Cyclotomy where e is four times an odd prime. The primary goal of this section is to derive a general expression for $(h, k)_e$ by carrying a bit further results obtained in Sections 3 and 4 of [16].

Let $\mathscr{E}$ denote an odd integer, $E = 2\mathscr{E}$, and $e = 4\mathscr{E}$. Let $\mathscr{B}(j, v)$, $B(j, v)$, and $b(j, v)$ denote coefficients of Jacobi sums of orders $\mathscr{E}$, E, and e, respectively. Let

$$D(j, v) = B(j, v) - B(j + \mathscr{E}, v), \qquad d(j, v) = b(j, v) - b(j + E, v).$$

(This notation differs somewhat from that of earlier papers.)

We commence with a reformulation of Theorems 3 and 2 of [16].

THEOREM 1.

$$2\sum_{n=0}^{\mathscr{E}-1}[(h, k+4n) - (h+E, k+E+4n) + (h+E, k+4n) - (h, k+E+4n)]$$
$$= d\big(-h+(k-h)\mathscr{E}, \mathscr{E}\big) + d\big(-h-(k-h)\mathscr{E}, -\mathscr{E}\big).$$

Proof. It follows easily from (2.2) and (2.12) that for an odd integer v,

$$b(j, v) = \sum_{r=0}^{e-1}(j - vr, r), \tag{3.1}$$

where $r \equiv h + Ef \pmod{e}$. Take $v = \mathscr{E}$ in (3.1) and write r as $4n+z$:

$$b(j, \mathscr{E}) = \sum_{n=0}^{\mathscr{E}-1}\sum_{z=0}^{3}(j - z\mathscr{E}, 4n+z).$$

Similarly, for $v = -\mathscr{E}$,

$$b(j, -\mathscr{E}) = \sum_{n=0}^{\mathscr{E}-1}\sum_{z=0}^{3}(j + z\mathscr{E}, 4n+z).$$

Thus

$$d\big(-h+(k-h)\mathscr{E}, \mathscr{E}\big) + d\big(-h-(k-h), -\mathscr{E}\big)$$
$$= \sum_{n=0}^{\mathscr{E}-1}\sum_{z=0}^{3}\big[\big(-h+(k-h-z)\mathscr{E}, z+4n\big) - \big(-h+(k-h-z)\mathscr{E}+E, z+4n\big) +$$
$$+\big(-h-(k-h-z)\mathscr{E}, z+4n\big) - \big(-h-(k-h-z)\mathscr{E}+E, z+4n\big)\big].$$

Whenever $k-h-z$ is odd, the first and the fourth terms in the brackets cancel, and the second and the third terms also cancel. Thus z can be assumed to take on just the two values $k-h$ and $k-h+E \pmod 4$.

Then the first and the third terms are the same, and the second and the fourth terms are the same. Hence

$$d\big(-h+(k-h)\mathscr{E}, \mathscr{E}\big) + d\big(-h-(k-h)\mathscr{E}, -\mathscr{E}\big) \tag{3.2}$$
$$= 2\sum_{n=0}^{\mathscr{E}-1}[(-h, k-h+4n) - (-h+E, k-h+4n) +$$
$$+(-h+E, k-h+E+4n) - (-h, k-h+E+4n)]$$
$$= 2\sum_{n=0}^{\mathscr{E}-1}[(h, k+4n) - (h+E, k+E+4n) + (h+E, k+4n) -$$
$$-(h, k+E+4n)],$$

by (2.1), q. e. d.

Replace $-h$ by h and $k-h$ by k in (3.2):

$$d(h+k\mathscr{E}, \mathscr{E}) + d(h-k\mathscr{E}, -\mathscr{E})$$
$$= 2\sum_{n=0}^{\mathscr{E}-1}[(h, k+4n) - (h+E, k+4n) + (h+E, k+E+4n) - (h, k+E+4n)].$$

Combining this with Theorem 1 yields

THEOREM 2.

$$4\sum_{n=0}^{\mathscr{E}-1}[(h, k+4n) - (h, k+E+4n)]$$
$$= d(h+k\mathscr{E}, \mathscr{E}) + d(h-k\mathscr{E}, -\mathscr{E}) + d\big(-h+(k-h)\mathscr{E}, \mathscr{E}\big) +$$
$$+ d\big(-h-(k-h)\mathscr{E}, -\mathscr{E}\big).$$

Define

$$q(n, r) = \begin{cases} 1, & r \mid n, \\ 0, & r \nmid n. \end{cases}$$

We now state the principal result of this section.

THEOREM 3. *Let $\mathscr{E}$ be an odd prime, $E = 2\mathscr{E}$, $e = 2E$. Then*

$$4e(h, k)_e = \sum_{v=1}^{\mathscr{E}-2}\mathscr{B}(k+hv, v) - 4f(\mathscr{E}-3) + 1 + (-1)^k + (-1)^h + (-1)^{h-k} +$$
$$+\sum_{v=1}^{\mathscr{E}-1}[D(k+2hv, 2v) + D(h+2kv, 2v) + D(h-k-2kv, 2v)] +$$
$$+2\sum_{v=1}^{E-1}[d(k+2hv, 2v) + (-1)^v d(h+2kv, 2v) +$$
$$+d(h-k-2kv, 2v)] + 4[(h, k)_2 - 4(h, k)_4] - 4q(k, e) -$$
$$-4q(h-k, e) - 2[1+(-1)^{f+h/2}]q(h, E) +$$
$$+(-1)^{h-k}[D(-h, \mathscr{E}) + D(-k, \mathscr{E})] + (-1)^h D(k, \mathscr{E}) +$$
$$+2d(k+h\mathscr{E}, \mathscr{E}) + 2d(k-h\mathscr{E}, -\mathscr{E}) +$$
$$+2d\big(-h+(k-h)\mathscr{E}, \mathscr{E}\big) + 2d\big(-h-(k-h)\mathscr{E}, -\mathscr{E}\big) +$$
$$+(-1)^v 2\big[d\big(-k+(h-k)\mathscr{E}, \mathscr{E}\big) + d\big(-k-(h-k)\mathscr{E}, -\mathscr{E}\big)\big].$$

Proof. From ([16], (3.7)), Theorem 1, and (2.7),

$$(3.3)\quad e[s(h,k)+s(h+E,k)] = 2d\big(-h+(k-h)\mathscr{E},\mathscr{E}\big)+ +2d\big(-h-(k-h)\mathscr{E},-\mathscr{E}\big)+4[(h,k+E)_4-(h,k)_4+ +(h+E,k+E)_4-(h+E,k)_4]+2\sum_{v=0}^{E-1} d(k+2hv,2v).$$

From (2.6), ([16], Theorem 1), Theorem 2, and (2.7),

$$(3.4)\quad \begin{aligned} et(h,k) &= d(k+h\mathscr{E},\mathscr{E})+d(k-h\mathscr{E},-\mathscr{E})+d\big(-k+(h-k)\mathscr{E},\mathscr{E}\big)+ \\ &\quad +d\big(-k-(h-k)\mathscr{E},-\mathscr{E}\big)+4[(k,h+E)_4-(k,h)_4]+ \\ &\quad +\sum_{v=0}^{e-1} d(h+kv,v) \qquad (f \text{ even}), \\ &= d\big(k+E+(h+E)\mathscr{E},\mathscr{E}\big)+d\big(k+E-(h+E)\mathscr{E},-\mathscr{E}\big)+ \\ &\quad +d\big(-k+E+(h-k)\mathscr{E},\mathscr{E}\big)+ \\ &\quad +d\big(-k+E-(h-k)\mathscr{E},-\mathscr{E}\big)+ \\ &\quad +4[(k+E,h)_4-(k+E,h+E)_4]+ \\ &\quad +\sum_{v=0}^{e-1} d\big(h+E+(k+E)v,v\big) \qquad (f \text{ odd}). \end{aligned}$$

Separate each sum in (3.4) into two sums, one containing the terms for which v is even, and the other having the terms for which v is odd. Apply (2.13) to the sums in which v is odd. Apply (2.2) to the cyclotomic numbers of order 4 in (3.4). The result is a single expression for $et(h,k)$ which holds whether f is odd or even:

$$(3.5)\quad \begin{aligned} et(h,k) &= d(k+h\mathscr{E},\mathscr{E})+d(k-h\mathscr{E},-\mathscr{E})+4[(h+E,k)_4-(h,k)_4]+ \\ &\quad +(-1)^f\big[d\big(-k+(h-k)\mathscr{E},\mathscr{E}\big)+ \\ &\quad +d\big(-k-(h-k)\mathscr{E},-\mathscr{E}\big)\big]+\sum_{v=0}^{E-1}[d(h-k-2kv,2v)+ \\ &\quad +(-1)^f d(h+2kv,2v)]. \end{aligned}$$

Thus from (2.8), (3.3), and (3.5),

$$(3.6)\quad \begin{aligned} 4e(h,k)_c &= e(h,k)_E+2d\big(-h+(k-h)\mathscr{E},\mathscr{E}\big)+ \\ &\quad +2d\big(-h-(k-h)\mathscr{E},-\mathscr{E}\big)+2d(k+h\mathscr{E},\mathscr{E})+ \\ &\quad +2d(k-h\mathscr{E},-\mathscr{E})+(-1)^f 2\big[d\big(-k+(h-k)\mathscr{E},\mathscr{E}\big)+ \\ &\quad +d\big(-k-(h-k)\mathscr{E},-\mathscr{E}\big)\big]+4[(h,k+E)_4+ \\ &\quad +(h+E,k)_4+(h+E,k+E)_4-3(h,k)_4]+ \\ &\quad +2\sum_{v=0}^{E-1}[d(k+2hv,2v)+(-1)^f d(h+2kv,2v)+ \\ &\quad +d(h-k-2kv,2v)]. \end{aligned}$$

If (2.14) is applied to the summation in (3.6), it becomes

$$(3.7)\quad \begin{aligned} &2\sum_{v=1}^{E-1}[d(k+2hv,2v)+(-1)^f d(h+2kv,2v)+d(h-k-2kv,2v)]- \\ &-2[(-1)^{k/2}q(k,E)+(-1)^{f+h/2}q(h,E)+(-1)^{(h-k)/2}q(h-k,E)]. \end{aligned}$$

$e(h,k)_E$ has been evaluated in Theorem 2 of [12]. (Note that the f of that paper is taken to be even here.)

$$(3.8)\quad \begin{aligned} e(h,k)_E &= \sum_{v=1}^{\mathscr{E}-2}\mathscr{B}(k+hv,v)-4f(\mathscr{E}-3)+1+(-1)^k+(-1)^h+ \\ &\quad +(-1)^{h-k}+(-1)^{h-k}[D(-h,\mathscr{E})+D(-k,\mathscr{E})]+ \\ &\quad +(-1)^h D(k,\mathscr{E})+\sum_{v=1}^{\mathscr{E}-1}[D(k+2hv,2v)+ \\ &\quad +D(h+2kv,2v)+D(h-k-2kv,2v)]- \\ &\quad -2[q(k,E)+q(h,E)+q(h-k,E)]. \end{aligned}$$

Combining the q terms in (3.7) and (3.8) gives

$$(3.9)\quad -4q(k,e)-4q(h-k,e)-2[1+(-1)^{f+h/2}q(h,E)].$$

$$(3.10)\quad 4[(h,k+E)_4+(h+E,k)_4+(h+E,k+E)_4-3(h,k)_4] = 4[(h,k)_2-4(h,k)_4].$$

Substituting (3.7) and (3.8), as modified by (3.9), and (3.10) into (3.6) gives the theorem, q. e. d.

Formulas for the cyclotomic numbers of order 4 are tabulated in ([8], pp. 156–157). They are expressed in terms of a and b in the quadratic decomposition

$$(3.11)\quad p = a^2+b^2, \qquad a \equiv 1 \pmod 4.$$

By means of these formulas one verifies easily

THEOREM 4. *Let* $C(h,k) = 4[(h,k)_2-4(h,k)_4]$. *If* f *is even,*

$$\begin{aligned} &C(0,0) = 6+6x, \\ &C(0,1) = C(1,0) = C(3,3) = 2-2x-8y, \\ &C(0,2) = C(2,0) = C(2,2) = -2-2x, \\ &C(0,3) = C(3,0) = C(1,1) = 2-2x+8y, \\ &C(1,2) = C(2,1) = C(1,3) = C(3,1) = C(2,3) \\ &\qquad = C(3,1) = -2-2x. \end{aligned}$$

If f *is odd,*

$$\begin{aligned} &C(0,0) = C(2,0) = C(2,2) = 2-2x, \\ &C(0,1) = C(1,3) = C(3,2) = -2-2x+8y, \\ &C(0,2) = -6+6x, \\ &C(0,3) = C(1,2) = C(3,1) = -2-2x-8y, \\ &C(1,0) = C(1,1) = C(2,1) = C(2,3) = C(3,0) \\ &\qquad = C(3,3) = 2+2x. \end{aligned}$$

Note that Theorems 4 and 5 of [16] hold for every e which is a multiple of 4.

In (2.15), set $z = 4$, $y = \mathscr{E}$, y odd. If $v = 4t+3$,

$$\sum_{s=0}^{\mathscr{E}-1} b_e(i+4s, 4t+3) = b_1(i, 3) = b_4(i, 0) = \begin{cases} \frac{1}{4}(p-5) & (4 \mid i), \\ \frac{1}{4}(p-1) & (4 \nmid i), \end{cases}$$

by (2.15), (2.13), and (2.14). Hence

$$\begin{aligned} &\sum_{s=0}^{\mathscr{E}-1} d_e(4s, 4t+3) = d_4(0, 3) = -1, \\ &\sum_{s=0}^{\mathscr{E}-1} d_e(1+4s, 4t+3) = d_4(1, 3) = 0. \end{aligned} \tag{3.12}$$

If $v = 4t+1$,

$$\sum_{s=0}^{\mathscr{E}-1} b_e(i+4s, 4t+1) = b_4(i, 1).$$

According to Dickson ([4], (50)) $R_4(1, 1) = (-1)^f[d_4(0, 1)+d_4(1, 1)\beta^{\mathscr{E}}] = -a+b\beta^{\mathscr{E}}$, where a and b satisfy (3.11). Hence

$$\begin{aligned} &\sum_{s=0}^{\mathscr{E}-1} d_e(4s, 4t+1) = d_4(0, 1) = (-1)^{f+1} a, \\ &\sum_{s=0}^{\mathscr{E}-1} d_e(1+4s, 4t+1) = d_4(1, 1) = (-1)^f b. \end{aligned} \tag{3.13}$$

4. Cyclotomy for $e = 20$. Throughout this section $e = 20$, $E = 10$, $\mathscr{E} = 5$. β is a primitive twentieth root of unity.

Theorem 3 expresses $(h, k)_{20}$ as a linear combination of p, a constant, Jacobi coefficients of orders 5, 10, and 20, and cyclotomic numbers of orders 2 and 4. The contribution of these cyclotomic numbers is given in Theorem 4. The Jacobi coefficients of orders 5 and 10 are expressed in [15] in terms of x, u, v, w, where

$$16p = x^2+50u^2+50v^2+125w^2, \quad x \equiv 1 (\mathrm{mod}\, 5), \quad xw = v^2-u^2-4uv. \tag{4.1}$$

The relationships are summarized as

THEOREM 5.

$$\begin{aligned}
20\mathscr{B}(0, 1) &= 4p-8+4x, \\
20\mathscr{B}(1, 1) &= 4p-8-x+10u+20v+25w, && ([15], (4.7)) \\
20\mathscr{B}(2, 1) &= 4p-8-x+20u-10v-25w, \\
20\mathscr{B}(3, 1) &= 4p-8-x-20u+10v-25w, \\
20\mathscr{B}(4, 1) &= 4p-8-x-10u-20v+25w, \\
\mathscr{B}(j, 2) &= \mathscr{B}(3j, 1), \quad \mathscr{B}(j, 3) = \mathscr{B}(j, 1) && (\text{Lemma 2, (2.13)}), \\
D(2j, 4) &= \mathscr{B}(3j+3T, 1)-4f && ([15], (6.12)), \\
D(j, 2) &= D(j+4T, 4) && ([15], (6.7)), \\
D(j, 6) &= D(7j+4T, 4) && ([15], (6.8)), \\
D(j, 8) &= D(j+2T, 4) && ([15], (6.6)).
\end{aligned}$$

By virtue of (2.13), it suffices to determine $d(j, v)$, $1 \leqslant v \leqslant 17$, v odd. As we determine a minimal set of Jacobi differences for these $d(j, v)$, we shall express $d(j, 1)$, $d(j, 3)$ and $d(j, 7)$ in terms of $d(j, 9)$; $d(j, 13)$ and $d(j, 17)$ in terms of $d(j, 11)$; and $d(j, 15)$ in terms of $d(j, 5)$. We note that either a or b, defined in (3.11) and (3.13), will appear in the expression of $d(j, v_1)$ in terms of $d(j, v_2)$ if $v_1 \not\equiv v_2 (\mathrm{mod}\, 4)$. Furthermore, $d(2j, 11)$ can be expressed in terms of a Jacobi coefficient of order 5. We begin by examining $d(j, 11)$ and $d(j, 9)$.

THEOREM 6.

$$d(2j+1, 11) = 0, \quad d(4j, 11) = D(2j+4T, 1).$$

Proof. The first statement is a special case of (2.23). Now set $t = 1$ in (2.32):

$$\psi(\beta^{11}, \beta) = \beta^{2T}\psi(\beta^2, \beta^2). \tag{4.2}$$

Expand the left side of the equation by (2.18) and the right side by (2.11):

$$(-1)^f \sum_{j=0}^{9} d(j, 11)\beta^j = \beta^{2T} \sum_{j=0}^{19} b(j, 1)\beta^{2j}.$$

Since 2 is a quadratic residue of $p \equiv 1 (\mathrm{mod}\, 20)$ if and only if f is even,

$$(-1)^f = \beta^{10T}. \tag{4.3}$$

Thus

$$\sum_{j=0}^{9} d(j, 11)\beta^j = \beta^{12T} \sum_{j=0}^{9} [b(j, 1)+b(j+10, 1)]\beta^{2j}.$$

$$\begin{aligned}
\sum_{j=0}^{4} d(2j, 11)\beta^{2j} &= \beta^{12T} \sum_{j=0}^{9} B(j, 1)\beta^{2j} = \beta^{12T} \sum_{j=0}^{4} D(j, 1)\beta^{2j} \\
&= \beta^{12T} \sum_{j=0}^{4} D(j+4T, 1)\beta^{2j+8T}
\end{aligned}$$

by the first statement of the theorem, (2.15) and (2.16). Hence

$$\sum_{i=0}^{4} d(4i, 11)\beta^{4i} = \sum_{j=0}^{4} D(j+4T, 1)\beta^{2j} = \sum_{i=0}^{4} D(2i+4T, 1)\beta^{4i},$$

$$\sum_{i=1}^{4} [d(4i, 11)-d(0, 11)]\beta^{4i} = \sum_{i=1}^{4} [D(2i+4T, 1)-D(4T, 1)]\beta^{4i}.$$

These sums both lie in the cyclotomic field of degree four over the rationals formed by adjoining β^4. A basis for this field is $\beta^4, \beta^8, \beta^{12}, \beta^{16}$. Thus it is permissible to equate coefficients of like powers of β:

$$d(4i, 11)-d(0, 11) = D(2i+4T, 1)-D(4T, 1), \quad i = 0, 1, 2, 3, 4.$$

Sum this equation over $i = 0, 1, 2, 3, 4$:

$$\sum_{i=0}^{4} d(4i, 11) - 5d(0, 11) = \sum_{i=0}^{4} D(2i+4T, 1) - 5D(4T, 1).$$

Both sums equal -1, by (3.12) and (2.20), respectively. Hence $d(0, 11) = D(4T, 1)$, so that $d(4i, 11) = D(2i+4T, 1)$, $i = 0, 1, 2, 3, 4$.

By combining Theorems 5 and 6, we obtain

$$(4.4)\quad d(4j, 11) = D(2j+4T, 1) = D(2j+4T, 8) = D(2j+6T, 4) = \mathscr{D}(3j+2T, 1) - 4f.$$

The study of $d(j, 9)$ is a modification of that in [17], which was based on work of Cauchy. By (2.26),

$$(4.5)\qquad \tau(\beta^3)\tau(\beta^{17}) = (-1)^f p = \tau(\beta^7)\tau(\beta^{13}).$$

In (2.29) put $\theta = \beta^4$ and $t = 1$, then apply (4.5):

$$\tau(\beta)\tau(\beta^5)\tau(\beta^9)\tau(\beta^{13})\tau(\beta^{17}) = \beta^{-5F}\tau(\beta^5)\tau(\beta^3)\tau(\beta^{17})\tau(\beta^7)\tau(\beta^{13}),$$

$$\tau(\beta)\tau(\beta^9) = \beta^{-5F}\tau(\beta^3)\tau(\beta^7).$$

$$(4.6)\qquad \psi(\beta^9, \beta) = \beta^{-5F}\psi(\beta^7, \beta^3),$$

in view of (2.24).

In (2.18) with $v = 9$, set $n = 1$, then 3:

$$\psi(\beta, \beta^9) = (-1)^f \sum_{j=0}^{9} d(j, 9)\beta^j, \qquad \psi(\beta^3, \beta^7) = (-1)^f \sum_{j=0}^{9} d(j, 9)\beta^{3j}.$$

By (2.22),

$$(4.7)\qquad \begin{aligned} d(1, 9) &= d(9, 9), \quad d(3, 9) = d(7, 9), \\ d(2, 9) &= -d(8, 9), \quad d(4, 9) = -d(6, 9). \end{aligned}$$

Hence

$$(4.8)\qquad (-1)^f\psi(\beta, \beta^9) = A + BI + (C+DI)(\theta - \theta^2 - \theta^3 + \theta^4),$$

where $\theta = \beta^4$, $I = \beta^5$,

$$(4.9)\qquad \begin{aligned} 2A &= 2d(0, 9) + d(2, 9) - d(4, 9), \\ 2B &= 2d(5, 9) + d(3, 9) - d(1, 9), \\ 2C &= d(2, 9) + d(4, 9), \\ 2D &= d(3, 9) + d(1, 9). \end{aligned}$$

Similarly,

$$(4.10)\qquad (-1)^f\psi(\beta^3, \beta^7) = A - BI + (-C+DI)(\theta - \theta^2 - \theta^3 + \theta^4).$$

By the law of quadratic reciprocity, $(5/p) = (p/5) = 1$. Hence F is even. If $F \equiv 0 \pmod 4$, equating (4.8) and (4.10) by virtue of (4.6) shows that

$$2BI + 2C(\theta - \theta^2 - \theta^3 + \theta^4) = 0.$$

Since I is purely imaginary and $\theta - \theta^2 - \theta^3 + \theta^4$ is real, $B = C = 0$. By (2.27)

$$(4.11)\qquad p = |(-1)^f\psi(\beta^9, \beta)|^2 = |A + DI(\theta - \theta^2 - \theta^3 + \theta^4)|^2 = A^2 + 5D^2.$$

Similarly, if $F \equiv 2 \pmod 4$, $\psi(\beta^9, \beta) = -\psi(\beta^7, \beta^3)$, so $A = D = 0$.

$$(4.12)\qquad p = |BI + C(\theta - \theta^2 - \theta^3 + \theta^4)|^2 = B^2 + 5C^2.$$

Set $t = 2$ in (3.13) and apply (4.7):

$$(4.13)\qquad \begin{aligned} (-1)^{f+1}a &= d(0, 9) + 2d(4, 9) + 2d(8, 9), \\ (-1)^f b &= d(5, 9) + 2d(1, 9) + 2d(13, 9). \end{aligned}$$

Let the quadratic decomposition of p given by (4.11) and (4.12) be written as

$$(4.14)\qquad p = c^2 + 5d^2.$$

If $F \equiv 0 \pmod 4$, let $c = A, d = D$. $B = C = 0$. If $F \equiv 2 \pmod 4$, let $c = B$, $d = C$. $A = D = 0$. Then the six equations in (4.9) and (4.13) can be solved for the six quantities $d(0, 9)$, $d(4, 9)$, $d(8, 9)$, $d(1, 9)$, $d(5, 9)$ and $d(13, 9)$ in terms of a, b, c and d, yielding:

THEOREM 7. *If 5 is a biquadratic residue of p,*

$$\begin{aligned} 5d(0, 9) &= (-1)^{f+1}a + 4c, \\ 5d(4t, 9) &= (-1)^{f+1}a - c \quad (5 \nmid t), \\ 5d(5, 9) &= (-1)^f b, \\ 5d(1, 9) &= 5d(9, 9) = (-1)^f b + 5d, \\ 5d(13, 9) &= 5d(17, 9) = (-1)^f b - 5d. \end{aligned}$$

If 5 is a biquadratic nonresidue of p

$$\begin{aligned} 5d(5, 9) &= (-1)^f b + 4c, \\ 5d(5+4t, 9) &= (-1)^f b - c \quad (5 \nmid t), \\ 5d(0, 9) &= (-1)^{f+1}a, \\ 5d(4, 9) &= 5d(16, 9) = (-1)^{f+1}a + 5d, \\ 5d(8, 9) &= 5d(12, 9) = (-1)^{f+1}a - 5d. \end{aligned}$$

COROLLARY. *If 5 is a biquadratic residue of p, $5|b$ and d is even. Otherwise $5|a$ and c is even.*

Proof. By (2.13) and (2.16), $d(j,9) = d(j,10)$. But (2.16) and Lemma 1 imply that $d(j,10)$ is odd if and only if $10|j$. Thus if $F \equiv 0 \pmod 4$, the formula for $5d(1,9)$ shows that $5|b$ and, since b is even, d must be even. If $F \equiv 2 \pmod 4$, look at the formulas for $5d(0,9)$ and $5d(1,9)$.

Part of this corollary is not new. See, e. g., ([9], p. 69).

THEOREM 8.

$$d(j,1) = d(j+12T, 9).$$

Proof. In (2.31) set $t = 1$ and apply (2.10), then (4.3):

$$\beta^{2T}\psi(\beta,\beta) = \psi(\beta^{10},\beta) = (-1)^f\psi(\beta^9,\beta),$$

$$\psi(\beta,\beta) = \beta^{8T}\psi(\beta^9,\beta). \tag{4.15}$$

Expand (4.15) by means of (2.18):

$$\sum_{j=0}^{9} d(j,1)\beta^j = \beta^{8T}\sum_{j=0}^{9} d(j,9)\beta^j = \beta^{8T}\sum_{j=0}^{9} d(j+12T,9)\beta^{j+12T}.$$

By (2.17)

$$\sum_{i=0}^{4} d(4i,1)\beta^{4i} + d(4i+1,1)\beta^{4i+1} = \sum_{i=0}^{4} d(4i+12T,9)\beta^{4i} + d(4i+1+12T,9)\beta^{4i+1}.$$

$$\sum_{i=0}^{4} [d(4i,1)-d(8,1)]\beta^{4i} + [d(4i+1,1)-d(9,1)]\beta^{4i+1} = \sum_{i=0}^{4} [d(4i+12T,9)-d(8+12T,9)]\beta^{4i} + [d(4i+1+12T,9)-d(9+12T,9)]\beta^{4i+1}. \tag{4.16}$$

Since the coefficients of β^8 and β^9 in (4.16) are zero, and since the set $1, \beta, \beta^4, \beta^5, \beta^{12}, \beta^{13}, \beta^{16}, \beta^{17}$ forms a basis for the cyclotomic field formed by adjoining β to the rationals, we may equate coefficients of corresponding powers of β in (4.16):

$$d(4i,1)-d(8,1) = d(4i+12T,9)-d(8+12T,9), \tag{4.17}$$

$$d(4i+1,1)-d(9,1) = d(4i+1+12T,9)-d(9+12T,9). \tag{4.18}$$

Sum (4.17) over $i = 0, 1, 2, 3, 4$ and apply the first statement of (3.13) to obtain $d(8,1) = d(8+12T,1)$, so that $d(4i,1) = d(4i+12T,9)$. Similar use of the second statement of (3.13) after summing (4.18) yields $d(4i+1,1) = d(4i+1+12T,9)$.

LEMMA 3. *Let*

$$\mu\psi(\beta,\beta) = \psi(\beta^3,\beta). \tag{4.19}$$

Then $\mu^2 = \beta^{5F}$.

Proof. Set $t = 2$ in (2.32), apply (2.10), then use (2.24):

$$\beta^{4T}\psi(\beta^4,\beta^4) = \psi(\beta^{12},\beta^2) = \psi(\beta^6,\beta^2),$$

$$\beta^{4T}\tau(\beta^4)^2 = \tau(\beta^6)\tau(\beta^2),$$

$$\tau(\beta)\tau(\beta)/\tau(\beta^2)\cdot\tau(\beta^3)\tau(\beta^3)/\tau(\beta^6) = \beta^{-4T}[\tau(\beta)\tau(\beta^3)/\tau(\beta^4)]^2,$$

$$\psi(\beta,\beta)\psi(\beta^3,\beta^3) = \beta^{-4T}\psi(\beta^3,\beta)^2 = \mu^2\beta^{-4T}\psi(\beta,\beta)^2,$$

by (4.19). But

$$\psi(\beta^3,\beta^3) = \beta^{4T}\psi(\beta^7,\beta^3) = \beta^{4T+5F}\psi(\beta^9,\beta) = \beta^{-4T+5F}\psi(\beta,\beta),$$

by (4.15) with β replaced by β^3, (4.6), and (4.15) as it is written. Hence $\mu^2 = \beta^{5F}$.

Since F is even, μ is a fourth root of unity. In order to facilitate working with equations containing μ, we introduce the following notation: Let

$$\mu = \beta^m, \quad M = (-1)^{\frac{1}{4}m(m+1)}, \quad M' = (-1)^{\frac{1}{4}m(m-1)}. \tag{4.20}$$

One may assume that m takes on the four values 0, 5, 10 and 15.

THEOREM 9.

$$d(4j,3) = d(4j-m,1)-[1+d_4(-m,1)]/5,$$

$$d(4j+1,3) = d(4j+1-m,1)-d_4(1-m,1)/5.$$

Proof. We proceed as in the proof of Theorem 8. Expand (4.19) by (2.18) and use (4.20):

$$\sum_{j=0}^{9} d(j,3)\beta^j = \beta^m\sum_{j=0}^{9} d(j,1)\beta^j = \beta^m\sum_{j=0}^{9} d(j-m,1)\beta^{j-m} = \sum_{j=0}^{9} d(j-m,1)\beta^j.$$

$$d(4i,3)-d(8,3) = d(4i-m,1)-d(8-m,1), \tag{4.21}$$

$$d(4i+1,3)-d(9,3) = d(4i+1-m,1)-d(9-m,1). \tag{4.22}$$

Sum (4.21) over $i = 0, 1, 2, 3, 4$:

$$\sum_{i=0}^{4} d(4i,3)-5d(8,3) = \sum_{i=0}^{4} d(4i-m,1)-5d(8-m,1).$$

The two sums can be evaluated by (3.12) and (3.13), respectively. Then substituting the value of $d(8,3)$ back into (4.21) yields the first statement of the theorem. The second part is obtained by summing (4.22), evaluating the sums, and substituting back into (4.22).

By combining Theorems 8 and 9, we obtain

$$\begin{aligned} d(4j-12T,3) &= d(4j-m,9)-[1+d_4(-m,1)]/5,\\ d(4j+1-12T,3) &= d(4j+1-m,9)-d_4(1-m,1)/5. \end{aligned} \tag{4.23}$$

We now evaluate (4.23) by means of Theorem 7, and express the results compactly with the aid of the notation defined in (4.20) to obtain

THEOREM 10.

$$\begin{aligned} d(8T,3) &= (4Mc-1)/5,\\ d(4j+8T,3) &= (-Mc-1)/5 \quad (5\nmid j),\\ d(4j+5+8T,3) &= \left(\frac{j}{5}\right)M'd. \end{aligned} \tag{4.24}$$

Notice that a and b do not appear in Theorem 10.

From Theorem 9 and (4.24) we deduce that $1+d_4(-m,1)$, $d_4(1-m,1)$ and $Mc+1$ are divisible by 5. Combining this with the Corollary to Theorem 7, we obtain the following determination of μ:

LEMMA 4.

$$\begin{aligned} &\mu=1, \quad m=0, \quad M=1, \quad M'=1: \quad a\equiv(-1)^f \pmod 5, \quad c\equiv 9 \pmod{10}.\\ &\mu=-1, \quad m=10, \quad M=-1, \quad M'=-1: \quad a\equiv-(-1)^f \pmod 5, \quad c\equiv 1 \pmod{10}.\\ &\mu=\beta^5, \quad m=5, \quad M=-1, \quad M'=1: \quad b\equiv(-1)^f \pmod 5, \quad c\equiv 6 \pmod{10}.\\ &\mu=\beta^{15}, \quad m=15, \quad M=1, \quad M'=-1: \quad b\equiv-(-1)^f \pmod 5, \quad c\equiv 4 \pmod{10}. \end{aligned}$$

This determination is definitive only if $F\equiv 0 \pmod 4$, for in this case we use the fact that $a\equiv 1 \pmod 4$ to ascertain whether $\mu=1$ or -1. Since the sign of b depends upon the choice of the primitive root g, if $F\equiv 2 \pmod 4$ whether $\mu=\beta^5$ or β^{15} depends upon g.

Although by (2.21), $d(j,7)=d(3j,3)$, we prefer to evaluate $d(j,7)$ by means of

$$\beta^{4T}\psi(\beta^7,\beta)=\mu\psi(\beta^9,\beta). \tag{4.25}$$

Proof of (4.25). By (4.19) with β^7 replacing β,

$$\begin{aligned} \psi(\beta^7,\beta) &= \psi(\beta^7,\beta^{21}) = \mu^7\psi(\beta^7,\beta^7)\\ &= \mu^7\beta^{16T}\psi(\beta^3,\beta^7) = \mu^7\beta^{16T+5F}\psi(\beta^9,\beta) = \mu\beta^{16T}\psi(\beta^9,\beta), \end{aligned}$$

by (4.15) with β^7 replacing β, (4.6), and Lemma 3.

Expand (4.25) by means of (2.18):

$$\beta^{4T}\sum_{j=0}^{9}d(j,7)\beta^j=\beta^m\sum_{j=0}^{9}d(j,9)\beta^j,$$

$$\beta^{4T}\sum_{j=0}^{9}d(j-4T,7)\beta^{j-4T}=\beta^m\sum_{j=0}^{9}d(j-m,9)\beta^{j-m}.$$

Proceeding as in the proof of Theorem 9, we establish

$$\begin{aligned} d(4j-4T,7) &= d(4j-m,9)-[1+d_4(-m,1)]/5,\\ d(4j+1-4T,7) &= d(4j+1-m,9)-d_4(1-m,1)/5. \end{aligned}$$

Comparison with (4.23) shows that $d(j-4T,7)=d(j-12T,3)$. Hence from Theorem 10 we obtain

THEOREM 11.

$$\begin{aligned} d(-4T,7) &= (4Mc-1)/5,\\ d(4j-4T,7) &= (-Mc-1)/5 \quad (5\nmid j),\\ d(4j+5-4T,7) &= \left(\frac{j}{5}\right)M'd. \end{aligned}$$

We turn now to the evaluation of $d(i,13)$ and $d(i,17)$. By (2.21),

$$d(j,13)=d(17j,17). \tag{4.26}$$

THEOREM 12. *If* $F\equiv 0 \pmod 4$,

$$\begin{aligned} d(4j,17) &= Md(4j+12T,11)+[(-1)^{f+1}a+M]/5,\\ d(4j+5,17) &= (-1)^f b/5. \end{aligned}$$

If $F\equiv 2 \pmod 4$,

$$\begin{aligned} d(4j,17) &= (-1)^{f+1}a/5,\\ d(4j+5,17) &= Md(4j+12T,11)+[(-1)^f b+M]/5. \end{aligned}$$

Proof. In (2.25), take $n=1$, $r=2$, $s=1$, then divide by (4.19):

$$\mu\psi(\beta,\beta^2)=\psi(\beta^2,\beta^2)=\beta^{-2T}\psi(\beta^{11},\beta),$$

by (4.2). Apply (2.10) and (4.3):

$$\mu\psi(\beta^{17},\beta)=\beta^{-12T}\psi(\beta^{11},\beta).$$

Expand by means of (2.18):

$$\begin{aligned} \beta^m\sum_{j=0}^{9}d(j-m,17)\beta^{j-m} &= \beta^{-12T}\sum_{j=0}^{9}d(j+12T,11)\beta^{j+12T}\\ &= \sum_{i=0}^{4}d(2i+12T,11)\beta^{2i}, \end{aligned}$$

by Theorem 6. Hence

$$d(4j-m,17)-d(8-m,17) = d(4j+12T,11)-d(8+12T,11),$$
$$d(4j+1-m,17)-d(9-m,17) = 0.$$

Sum over $j = 0, 1, 2, 3, 4$, apply (2.15) and (3.12), and substitute to obtain

$$d(4j-m,17) = d(4j+12T,11)+[1+d_4(-m,1)]/5,$$
$$d(4j+1-m,17) = d_4(1-m,1)/5.$$

To complete the proof, set $m = 0$ and 10, then 5 and 15, and apply (3.13).

THEOREM 13. *If* $F \equiv 0 \pmod 4$,

$$Md(4j,15) = d(8j,5)+[(-1)^f a-M]/5,$$
$$-Md(4j+5,15) = d(8j+5,5)-(-1)^f b/5.$$

If $F \equiv 2 \pmod 4$,

$$Md(4j,15) = d(8j+5,5)-[(-1)^f b-M]/5,$$
$$Md(4j+5,15) = d(8j,5)+(-1)^f a/5.$$

Proof. In (2.25), set $n = 1$, $r = 3$, $s = 1$, then divide by (4.19):

$$\mu\psi(\beta^4,\beta) = \psi(\beta^2,\beta^3).$$
$$\mu\psi(\beta^{15},\beta) = \psi(\beta^{15},\beta^3),$$

by (2.10). Expand by means of (2.18):

$$\beta^m \sum_{j=0}^{9} d(j-m,15)\beta^{j-m} = \sum_{j=0}^{9} d(j,5)\beta^{3j} = \sum_{j=0}^{9} d(7j,5)\beta^j.$$

Thus if we take as a basis $\beta, \beta^4, \beta^8, \beta^9, \beta^{12}, \beta^{13}, \beta^{16}, \beta^{17}$,

$$d(4j-m,15)-d(-m,15) = d(8j,5)-d(0,5),$$
$$d(4j+5-m,15)-d(5-m,15) = d(8j+15,5)-d(15,5).$$

Sum over $j = 0, 1, 2, 3, 4$ and apply (2.15) and (3.13):

$$d(4j-m,15) = d(8j,5)+[d_4(-m,3)+(-1)^f a]/5,$$
$$d(4j+5-m,15) = d(8j+15,5)+[d_4(1-m,3)+(-1)^f b]/5.$$

To complete the proof, set $m = 0$ and 10, then 5 and 15, and apply (3.12).

Some of the relationships between Jacobi sums developed in this section were previously stated by Dickson ([6], Section 15).

5. Evaluating the cyclotomic numbers of order twenty. To produce a formula for any cyclotomic number of order 20, substitute into Theorem 3 values of the appropriate cyclotomic numbers of orders two and four and Jacobi sums of orders 5, 10, and 20 which can be obtained from Theorems 4 through 13 and (4.26). It is necessary to specify only two parameters, T and μ. These determine the parity of f, and F (mod4), by (4.3) and Lemma 3, respectively.

The formula could be expressed as a linear combination of twenty variables: p, the constant 1, a, b (see (3.11)), c, d (see (4.14)), x, u, v, w (see (4.1)), and $d(j,5)$, $0 \leqslant j \leqslant 9$. According to Theorem 6 of [7],

$$\sum_{j=0}^{9} d(j,5)^2 = p,$$

so the solution of the cyclotomic number problem for $e = 20$ is complete according to the definition given in the introduction.

Not all of the variables are linearly independent, however. According to (3.13),

$$d(0,5)-d(2,5)+d(4,5)-d(6,5)+d(8,5) = (-1)^{f+1}a,$$
$$d(1,5)-d(3,5)+d(5,5)-d(7,5)+d(9,5) = (-1)^f b.$$

Two of these variables must be dropped to form a minimal set. In the interests of symmetry, a and b were dropped, instead of two of the $d(j,5)$.

Producing a list of all the formulas for the cyclotomic numbers, however, is a formidable task. There are ten choices for T (mod10) and four possibilities for μ, so that there are forty *classes* to be considered. For each class 77 formulas must be computed, according to (2.3). We turned to the computer for assistance in deriving the 3080 formulas. An assembly language program was written for the IBM7070 to generate the formulas.

Computers were quite useful in earlier phases of the study as well. First the cyclotomic numbers of order twenty were computed for over 600 primes. From these, values of Jacobi coefficients were computed; examination of these values helped formulate some of the theorems proved in Section 4.

When the cyclotomic numbers were computed for the prime p, g was chosen to be the smallest positive primitive root. Unless $5 \mid T$ and $4 \mid F$, the choice of g determined in part which one of the forty classes of formulas would be applicable to p. Where the cyclotomic numbers had been computed for at least eighteen primes in a class, the formulas for that class were determined empirically. Specifically, we found the coefficient x_{jhk} of the jth variable in the formula for $1600(h,k)$.

For eighteen primes p_i, $1 \leqslant i \leqslant 18$, in a class, the values of the eighteen variables were computed. This gave rise to a set of eighteen linear equations

$$\sum_{j=1}^{18} a_{ij}x_{jhk} = 1600(h,k)_i, \tag{5.1}$$

where a_{ij} denotes the value of the jth variable for the ith prime, and $(h,k)_i$ is the value of (h,k) for the ith prime. The scaling factor of 1600 was used to insure rational integral values for the x_{jhk}.

The set of equations (5.1) was solved by computer. The computed

values of the coefficients were rounded to the nearest integer. It was then verified that these integers formed the exact solution. These coefficients, computed for nine classes, were very helpful in the detection (and elimination) of errors in the program which generated all the formulas for the cyclotomic numbers.

It is not appropriate to include all 3080 formulas. Table 1 consists of the formulas for the class $T \equiv 1 \pmod{10}$, f odd, $\mu = \beta^5$, $F \equiv 2 \pmod 4$. For each of eighteen primes in this class, the values of sixteen of the

TABLE 1. Cyclotomic number formulas
f odd, $\operatorname{ind} 2 \equiv 1 \pmod{10}$,

$(h,\ k)\quad p$	1	c	d	x	u	v	w
1600 (0, 0) = 4	−156	16	−40	−5	−110	−20	25
1600 (0, 1) = 4	4	−48	−80	−18	120	−60	350
1600 (0, 2) = 4	4	−48	40	23	30	−40	−175
1600 (0, 3) = 4	4	16	120	−24	50	−50	−150
1600 (0, 4) = 4	4	16	120	19	30	−90	0
1600 (0, 5) = 4	4	32	−40	27	−70	−140	−175
1600 (0, 6) = 4	4	32	0	−2	80	60	−220
1600 (0, 7) = 4	4	16	−200	31	30	−40	55
1600 (0, 8) = 4	4	16	−120	−20	−230	100	−250
1600 (0, 9) = 4	4	−48	40	2	−10	30	0
1600 (0, 10) = 4	4	−48	120	3	−270	60	225
1600 (0, 11) = 4	4	16	80	6	−40	20	150
1600 (0, 12) = 4	4	16	40	15	110	120	25
1600 (0, 13) = 4	4	112	−40	−8	50	−50	250
1600 (0, 14) = 4	4	−48	−200	−22	30	−90	0
1600 (0, 15) = 4	4	−64	−40	11	90	180	225
1600 (0, 16) = 4	4	−64	0	−10	0	−100	−50
1600 (0, 17) = 4	4	−48	120	7	110	120	−175
1600 (0, 18) = 4	4	112	40	−12	−70	110	−50
1600 (0, 19) = 4	4	16	40	−14	70	−210	0
1600 (1, 0) = 4	−76	16	0	−10	−40	20	150
1600 (1, 1) = 4	−76	16	−40	−10	70	−10	100
1600 (1, 2) = 4	4	16	−200	−4	−10	130	50
1600 (1, 3) = 4	4	−48	−160	−8	−100	−100	−100
1600 (1, 4) = 4	4	−64	−40	0	30	10	150
1600 (1, 5) = 4	4	−104	40	10	20	40	150
1600 (1, 6) = 4	4	−24	80	−14	50	−150	−100
1600 (1, 7) = 4	4	−48	40	12	170	−10	−50
1600 (1, 8) = 4	4	16	0	0	−100	−100	100
1600 (1, 12) = 4	4	16	120	0	70	90	−250
1600 (1, 13) = 4	4	16	0	0	20	−60	−100
1600 (1, 14) = 4	4	16	200	−4	−130	−110	50
1600 (1, 15) = 4	4	72	40	−18	60	120	50
1600 (1, 16) = 4	4	56	−80	10	−110	−70	100
1600 (1, 17) = 4	4	16	−120	0	−30	−10	−150
1600 (1, 18) = 4	4	16	−160	16	−20	60	100
1600 (1, 19) = 4	4	32	40	12	30	10	−150
1600 (2, 0) = 4	−76	16	−40	15	30	−40	25
1600 (2, 1) = 4	4	−64	40	0	110	−30	−50
1600 (2, 2) = 4	−76	−64	40	0	−150	150	−150
1600 (2, 3) = 4	4	16	160	0	−140	20	300
1600 (2, 4) = 4	4	16	80	10	160	20	50
1600 (2, 5) = 4	4	56	80	−15	90	80	−25
1600 (2, 6) = 4	4	16	−120	0	−70	−90	−150

variables a_{ij} in equation (5.1) are given in Table 2 and the values of the 77 cyclotomic numbers are listed in Table 3. Some formulas for $(h, 0)$, $0 \leqslant h \leqslant 9$, in five other classes are included as Table 4; they are used in the next section. In column headings $d(i, 5)$ appears as d_j.

It was pointed out in [12] that for several values of e, there are fewer distinct cyclotomic number formulas than the upper bound given by (2.3). This phenomenon has been observed for $e = 6, 8, 10, 12, 14$ and 18. For $e = 20$, the 77 formulas are all different for only some of the classes.

for the class $\operatorname{ind} 2 \equiv 1 \pmod{10}$, $\mu = \beta^5$
$\operatorname{ind} 5 \equiv 2 \pmod 4$, $e \equiv 6 \pmod{10}$

d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_2	d_3	d_{13}	d_{17}
72	−8	−8	−8	−8	16	−64	16	16	16
72	72	−8	−88	−8	48	48	−32	48	−32
−56	24	−56	−56	24	32	32	32	−48	−48
−88	−8	−8	72	72	0	−80	80	−80	0
72	72	−8	−8	−88	16	−64	16	−64	96
72	−8	−8	−8	−8	−32	208	−32	−32	−32
−56	−56	24	24	−56	−48	32	−48	32	32
−88	72	72	−8	−8	80	−80	0	0	−80
72	−8	72	−88	−8	−64	−64	96	16	16
72	−8	−88	−8	72	−32	48	48	−32	48
−216	24	24	24	24	−48	192	−48	−48	−48
−88	72	−8	72	−8	−80	−80	0	80	0
72	−8	−88	72	−8	96	−64	−64	16	16
72	−8	−8	72	−88	−32	48	48	48	−32
−56	−56	24	24	−56	−48	32	−48	32	32
72	−8	−8	−8	−8	0	−80	0	0	0
72	−88	−8	−8	72	16	−64	16	96	−64
72	−88	72	−8	−8	48	48	−32	−32	48
−56	24	−56	−56	24	32	32	32	−48	−48
−88	−8	72	−8	72	0	−80	−80	0	80
8	−72	8	8	8	16	16	16	−64	16
8	8	8	8	−72	16	16	16	16	−64
−8	−8	32	32	−8	−40	0	−40	0	0
−8	−8	−8	−8	72	8	−32	8	8	88
8	8	8	−72	8	−24	16	56	−24	−24
−72	8	8	48	−32	56	16	−64	16	−24
72	32	−48	−8	−8	−80	0	−40	40	0
−8	−8	−8	72	−8	8	−32	88	8	8
8	−72	8	−72	88	56	16	−24	−24	−24
8	8	48	−32	−72	56	16	−24	−64	16
8	−72	8	8	8	−24	16	−24	56	−24
−8	72	−8	−8	−8	−40	0	−40	40	−40
−8	−8	−8	32	32	8	48	48	−32	8
8	−32	−32	8	8	96	−64	−24	−24	16
8	8	88	−72	−72	−24	16	−24	56	−24
−8	−8	−8	72	−8	−40	0	40	−40	−40
−8	72	−48	−48	72	8	−32	8	48	48
−8	−8	72	−8	−8	−64	16	16	16	16
8	−72	−32	48	8	−24	16	56	16	−64
−8	−8	−8	72	−8	16	16	−64	16	16
8	8	8	8	−72	−24	16	−24	−24	56
−8	−48	72	−8	32	−64	16	16	56	−24
8	−32	8	−32	8	16	−64	−24	96	−24
−8	−8	−48	32	72	56	16	−24	16	−64

Table 1 (continued)

(h, k) p	1	c	d	x	u	v	w	d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
1600 (2, 7) = 4	4	−24	0	0	−10	−70	−50	8	8	−32	8	−32	−24	−64	16	−24	96
1600 (2,14) = 4	4	16	−80	10	40	−20	250	−8	32	−8	−8	32	16	16	16	−24	−24
1600 (2,15) = 4	4	−24	−80	−35	50	0	75	−72	48	8	−32	8	16	16	−24	−64	56
1600 (2,16) = 4	4	−64	−40	0	50	−50	50	−8	72	32	−48	−8	−24	16	56	−64	16
1600 (2,17) = 4	4	−24	80	0	−170	10	−50	−72	8	−32	8	48	−24	16	16	56	−64
1600 (2,18) = 4	4	16	−80	−10	120	−60	150	−8	32	−8	72	−48	16	16	−64	−24	56
1600 (2,19) = 4	4	16	0	20	−20	−140	−200	8	88	−72	8	−72	−24	16	56	−24	−24
1600 (3, 0) = 4	−76	−64	−40	0	50	−50	50	8	8	8	−72	8	16	16	−64	16	16
1600 (3, 1) = 4	4	16	160	−4	100	−100	−200	−8	−8	72	−8	−8	40	0	−40	−40	−40
1600 (3, 2) = 4	4	−48	0	−8	−140	20	100	−8	72	−8	−8	−8	8	−32	8	88	8
1600 (3, 3) = 4	−76	16	40	15	30	−40	25	8	8	−72	8	8	−64	16	16	16	16
1600 (3, 4) = 4	4	16	40	0	50	150	−150	8	8	−72	8	8	56	16	−24	−24	−24
1600 (3, 5) = 4	4	−24	−80	−4	−90	−30	−150	72	−8	32	−8	−48	40	0	0	−40	−80
1600 (3, 6) = 4	4	−48	80	2	−120	60	50	−8	−48	72	72	−48	48	−32	48	8	8
1600 (3,16) = 4	4	16	80	10	0	100	50	8	−32	8	−72	48	−64	16	16	−24	56
1600 (3,17) = 4	4	16	−80	6	40	180	150	−8	32	−8	−8	32	0	0	0	−40	−40
1600 (3,18) = 4	4	−8	−80	−23	90	80	−225	−8	32	−8	32	−8	−32	48	8	48	8
1600 (3,19) = 4	4	16	−120	0	−90	−30	−50	8	−72	−72	88	8	−24	16	−24	−24	56
1600 (4, 0) = 4	−76	16	40	−10	70	−10	100	−8	−8	−8	−8	72	16	16	16	16	−64
1600 (4, 1) = 4	4	32	−40	12	−10	−70	−150	−8	−8	72	−8	−8	88	−32	8	8	8
1600 (4, 2) = 4	4	−48	80	−2	80	60	150	24	−16	−56	−56	−16	32	−48	32	−8	−8
1600 (4, 3) = 4	4	16	40	−4	10	70	−50	−8	−8	−8	−8	72	−40	0	−40	−40	40
1600 (4, 4) = 4	−76	16	0	−10	−40	20	−250	−8	72	−8	−8	−8	16	16	16	−64	16
1600 (4, 5) = 4	4	−8	80	2	−150	50	100	−8	32	32	−8	−8	48	48	8	8	−32
1600 (4,18) = 4	4	32	−40	8	−70	−90	50	24	−56	−16	−16	−56	−8	−48	−8	32	32
1600 (4,19) = 4	4	−24	−40	26	−20	160	−50	72	−8	−8	−48	32	−40	0	−80	0	40
1600 (5, 0) = 4	−76	16	40	15	90	−20	−75	−72	8	8	8	8	16	−64	16	16	16
1600 (5, 1) = 4	4	56	−40	−10	−60	80	50	8	8	8	−32	−32	−24	−64	96	16	−24
1600 (5, 2) = 4	4	−24	80	−19	−30	−160	75	72	−48	−8	32	−8	0	0	40	−80	−40
1600 (5, 3) = 4	4	72	0	12	70	−110	250	−8	−8	32	−8	32	8	48	−32	8	48
1600 (5, 4) = 4	4	−24	−80	10	10	−30	−100	−72	−32	48	8	8	−64	16	56	−24	16
1600 (6, 2) = 4	4	16	200	0	−110	30	50	−8	−8	32	32	−8	−24	16	−24	16	16
1600 (6, 3) = 4	4	16	−80	−10	80	60	−50	8	48	−72	8	−32	16	16	−64	56	−24

TABLE 2. Values of 16 of the variables

for 18 primes in the class ind $2 \equiv 1 \pmod{10}$, $\mu = \beta^5$

p	c	d	x	u	v	w	d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
421	−4	−9	−19	8	1	5	−11	1	4	−2	−7	−13	2	−7	2	2
701	−24	−5	−79	4	9	1	13	3	8	−2	−17	7	6	1	4	8
821	−24	−7	31	4	15	−1	9	10	−1	11	−4	12	−10	−16	1	−1
1301	36	−1	121	0	−11	1	−3	5	2	8	13	25	−14	3	−2	14
1901	36	−11	−29	8	15	11	1	−16	−19	−3	2	10	−14	18	23	−11
2221	−4	21	131	16	7	−5	25	22	5	−11	4	2	2	−22	17	−13
3701	−24	25	−29	12	11	19	−23	−8	−13	−33	22	24	22	−4	−17	1
7901	−84	13	71	−48	11	−1	65	−14	5	−3	32	2	−30	34	1	19
8861	−84	−19	−49	0	35	−25	1	8	1	−15	10	−58	42	−2	−53	−23
9221	96	1	−369	12	−9	−1	−39	38	−29	−25	−40	16	14	−52	5	3
10141	−4	45	191	−48	3	−9	1	26	61	21	−24	−22	34	−54	1	−13
10861	−104	−3	−149	52	−5	11	13	2	23	11	−4	40	−26	4	−83	−29
11261	−84	29	−149	−24	−41	19	25	18	25	−79	16	6	34	38	5	23
13901	−84	−37	121	−32	−27	−31	25	−59	−70	−8	−3	−23	50	−21	−14	34
14461	−104	−27	−149	20	59	11	−11	10	−1	−29	−44	−104	22	4	−11	−5
15461	−84	41	−149	24	55	19	37	44	37	21	−74	46	−6	38	35	−7
15901	76	45	71	20	55	−25	−27	−22	23	3	28	0	10	−4	5	115
16301	−84	−43	171	48	15	−29	41	70	−39	49	4	6	−38	−26	49	35

TABLE 3. Values of 77 cyclotomic numbers for the 18 primes in Table 2

p	421	701	821	1301	1901	2221	3701	7901
(0, 0)	0	2	2	4	6	4	6	26
(0, 1)	3	5	3	1	7	7	15	17
(0, 2)	0	0	2	4	2	8	12	20
(0, 3)	0	0	0	4	4	2	10	18
(0, 4)	0	2	2	6	2	8	8	22
(0, 5)	0	0	0	4	0	8	6	18
(0, 6)	2	2	2	2	4	6	6	12
(0, 7)	2	0	4	8	6	6	6	14
(0, 8)	0	4	2	0	6	2	2	32
(0, 9)	0	2	2	2	4	6	12	28
(0,10)	2	0	0	0	0	2	18	18
(0,11)	2	0	2	4	6	6	8	18
(0,12)	0	2	6	6	8	10	10	20
(0,13)	2	2	0	4	10	4	6	12
(0,14)	4	4	2	0	4	0	6	14
(0,15)	2	4	6	2	8	8	12	26
(0,16)	0	2	2	2	6	6	8	28
(0,17)	0	4	4	2	2	10	12	24
(0,18)	0	0	0	4	8	4	12	14
(0,19)	2	0	0	6	2	4	10	14
(1, 0)	1	2	1	3	6	2	12	21
(1, 1)	2	3	2	2	7	5	9	14
(1, 2)	3	3	4	2	7	3	6	17
(1, 3)	1	2	2	4	3	1	6	26
(1, 4)	2	3	2	1	5	5	13	23
(1, 5)	2	3	5	2	3	7	14	20
(1, 6)	1	2	1	1	2	8	7	20
(1, 7)	1	2	3	4	5	7	9	20
(1, 8)	0	0	0	5	5	4	13	23
(1,12)	0	3	3	3	2	9	10	17
(1,13)	1	1	1	3	5	6	7	18
(1,14)	0	0	0	3	2	8	10	21
(1,15)	1	2	1	3	8	4	12	15
(1,16)	0	0	2	8	7	3	8	21
(1,17)	2	3	2	2	4	6	4	17
(1,18)	2	1	3	4	7	3	6	19
(1,19)	0	0	2	6	5	9	9	20
(2, 0)	2	1	1	4	4	6	7	18
(2, 1)	1	2	2	1	5	6	10	21
(2, 2)	0	3	5	1	2	6	8	27
(2, 3)	1	2	1	3	4	5	13	23
(2, 4)	2	1	1	3	6	9	11	16
(2, 5)	1	2	2	3	9	8	10	16
(2, 6)	0	0	2	5	5	4	6	19
(2, 7)	1	2	2	4	3	4	7	23
(2,14)	2	1	2	5	7	5	12	17
(2,15)	3	4	2	1	4	1	13	14
(2,16)	2	3	2	2	2	5	11	21
(2,17)	0	0	1	2	4	5	10	24
(2,18)	3	3	3	4	5	4	9	11
(2,19)	0	0	1	5	2	7	4	18
(3, 0)	2	3	3	2	3	7	12	20
(3, 1)	0	1	1	4	1	9	10	15
(3, 2)	1	3	3	2	5	5	9	26
(3, 3)	1	0	1	4	5	7	9	19
(3, 4)	0	2	4	3	6	8	11	18
(3, 5)	0	3	3	2	3	5	5	24
(3, 6)	0	3	3	3	4	4	9	28
(3,16)	1	1	1	3	5	7	13	23

numbers for the 18 primes in Table 2

8861	9221	10141	10861	11261	13901	14461	15461	15901	16301
18	22	24	24	30	36	32	38	36	40
19	29	17	37	41	29	43	49	24	43
28	18	26	30	30	42	34	34	38	44
22	20	20	34	26	28	30	36	46	36
16	24	28	30	32	32	30	44	44	44
28	20	36	18	30	52	30	24	36	38
26	28	28	22	18	38	40	36	52	44
18	20	24	30	20	28	30	34	30	48
32	20	26	18	30	38	46	40	44	38
28	16	22	28	34	44	40	38	42	44
30	24	44	20	36	36	44	36	38	18
16	24	30	20	24	24	38	42	41	42
16	22	22	30	16	32	30	46	46	54
12	30	22	22	24	26	34	42	34	34
26	28	20	30	28	44	46	34	32	44
24	14	20	36	26	30	48	52	38	50
20	16	20	30	34	40	32	38	30	44
28	16	30	34	28	38	38	48	54	44
22	34	24	20	24	28	32	34	46	28
14	30	24	30	32	30	26	28	44	38
21	23	23	30	30	34	36	38	40	30
20	28	22	31	27	29	39	45	32	39
27	24	23	26	19	35	46	37	39	45
24	20	20	26	33	47	34	28	37	47
27	18	21	34	37	35	46	43	32	39
23	19	30	35	29	34	41	49	35	45
23	27	26	27	34	40	37	37	35	46
22	15	20	35	25	33	37	46	42	51
18	22	25	26	36	38	26	28	35	28
26	27	31	31	25	32	35	46	52	41
21	23	26	23	26	39	33	33	40	40
17	28	37	20	36	30	30	39	36	32
22	29	21	27	24	26	37	42	49	34
12	24	23	24	25	36	22	30	36	37
25	26	29	22	28	37	40	37	37	42
25	17	23	27	19	36	41	35	34	43
20	24	24	20	27	34	30	34	49	49
22	19	28	24	28	34	38	35	41	40
26	16	21	34	28	39	40	42	35	44
29	19	35	24	24	42	40	44	45	46
16	25	35	23	35	29	37	46	42	27
21	19	26	27	27	27	39	41	46	39
16	30	22	24	24	24	34	44	47	40
22	24	23	24	24	43	26	26	32	44
21	22	23	28	30	40	36	37	42	46
19	22	21	30	29	30	36	37	33	39
26	34	18	36	33	32	44	40	39	39
28	20	23	36	37	35	44	42	34	43
24	21	32	19	31	37	35	36	37	35
18	31	21	33	24	32	37	40	38	46
23	23	28	23	27	42	31	33	34	47
24	23	24	32	35	39	40	39	35	45
21	27	31	33	29	30	27	39	44	37
20	23	28	23	35	33	39	46	34	43
21	21	25	22	27	38	36	34	41	43
26	26	24	28	20	35	36	42	47	46
27	21	28	31	29	41	35	39	29	41
20	15	32	29	30	32	35	50	41	36
25	19	27	23	31	34	41	37	51	35

p	421	701	821	1301	1901	2221	3701	7901
(3,17)	2	2	4	3	8	6	12	18
(3,18)	2	4	3	0	5	5	6	15
(3,19)	1	1	2	4	5	1	5	21
(4, 0)	1	1	1	3	7	6	13	17
(4, 1)	0	1	2	7	4	6	6	19
(4, 2)	1	3	3	2	7	7	15	23
(4, 3)	1	1	2	3	4	6	11	20
(4, 4)	0	2	2	3	2	5	7	19
(4, 5)	0	2	2	3	4	6	12	24
(4,18)	1	1	1	5	6	4	6	21
(4,19)	1	2	5	3	4	10	9	26
(5, 0)	1	0	2	6	5	7	9	16
(5, 1)	1	2	1	3	9	3	7	21
(5, 2)	0	2	0	2	3	3	10	24
(5, 3)	2	0	0	7	6	6	12	13
(5, 4)	2	1	1	3	3	3	7	19
(6, 2)	0	1	1	3	3	7	11	23
(6, 3)	2	3	4	2	7	7	8	13

Table 3 (continued)

8861	9221	10141	10861	11261	13901	14461	15461	15901	16301
26	22	22	30	22	28	44	42	40	42
30	29	21	27	23	37	45	42	44	51
23	22	23	22	21	48	34	27	40	43
20	25	21	30	30	28	34	39	37	36
17	22	27	26	26	34	24	35	42	42
21	21	19	35	33	31	41	49	38	41
26	24	26	26	26	35	38	34	49	40
28	28	27	27	27	37	35	37	44	43
21	22	34	24	34	31	34	45	38	32
15	23	25	21	28	39	31	33	37	38
29	15	30	23	24	42	43	37	47	50
18	22	24	27	23	30	31	37	46	45
20	25	21	23	27	27	39	42	39	35
21	22	24	36	37	37	32	39	29	31
12	26	25	24	30	29	28	32	42	34
28	17	25	27	27	40	41	32	41	41
19	23	37	21	31	30	33	43	47	31
23	32	21	26	21	35	40	41	38	51

TABLE 4. Formulas for the cyclotomic numbers $(h, 0)$ in five classes, used in studying difference sets

f odd, $\operatorname{ind} 2 \equiv 1 \pmod{10}$, $\operatorname{ind} 5 \equiv 0 \pmod 4$, $c \equiv 1 \pmod{10}$

(h,k) p	1	c	d	x	u	v	w
1600 (0, 0) = 4	−156	40	0	−1	−150	−100	−75
1600 (1, 0) = 4	−76	−48	0	6	−40	20	150
1600 (2, 0) = 4	−76	40	0	19	70	40	−75
1600 (3, 0) = 4	−76	−88	0	−4	−30	−10	−50
1600 (4, 0) = 4	−76	40	0	−6	−10	30	200
1600 (5, 0) = 4	−76	−8	0	11	130	60	25
1600 (6, 0) = 4	−76	80	0	−26	−40	20	−250
1600 (7, 0) = 4	−76	−8	0	11	−10	−120	125
1600 (8, 0) = 4	−76	−40	0	4	−70	110	−50
1600 (9, 0) = 4	−76	−8	0	−14	150	−50	0

d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
8	8	8	8	8	0	0	0	0	0
24	−56	−56	24	24	0	0	0	0	0
8	8	88	8	−72	0	0	0	0	0
24	−56	24	−56	24	0	0	0	0	0
8	8	8	−72	88	0	0	0	0	0
−136	24	24	24	24	0	0	0	0	0
8	88	−72	8	8	0	0	0	0	0
24	24	−56	24	−56	0	0	0	0	0
8	−72	8	88	8	0	0	0	0	0
24	24	24	−56	−56	0	0	0	0	0

f odd, $\operatorname{ind} 2 \equiv 1 \pmod{10}$, $\operatorname{ind} 5 \equiv 0 \pmod 4$, $c \equiv 9 \pmod{10}$

(h,k) p	1	c	d	x	u	v	w
1600 (0, 0) = 4	−156	8	0	−9	−70	60	125
1600 (1, 0) = 4	−76	−80	0	−26	−40	20	150
1600 (2, 0) = 4	−76	8	0	11	−10	−120	125
1600 (3, 0) = 4	−76	40	0	4	130	−90	150
1600 (4, 0) = 4	−76	8	0	−14	150	−50	0
1600 (5, 0) = 4	−76	−40	0	19	50	−100	−175
1600 (6, 0) = 4	−76	48	0	6	−40	20	−250
1600 (7, 0) = 4	−76	−40	0	19	70	40	−75
1600 (8, 0) = 4	−76	88	0	−4	−230	190	−250
1600 (9, 0) = 4	−76	−40	0	−6	−10	30	200

d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
136	−24	−24	−24	−24	0	0	0	0	0
−8	−88	72	−8	−8	0	0	0	0	0
−24	−24	56	−24	56	0	0	0	0	0
−8	72	−8	−88	−8	0	0	0	0	0
−24	−24	−24	56	56	0	0	0	0	0
−8	−8	−8	−8	−8	0	0	0	0	0
−24	56	56	−24	−24	0	0	0	0	0
−8	−8	−88	−8	72	0	0	0	0	0
−24	56	−24	56	−24	0	0	0	0	0
−8	−8	−8	72	−88	0	0	0	0	0

f odd, $\operatorname{ind} 2 \equiv 5 \pmod{10}$,

(h,k) p	1	c	d	x	u	v	w
1600 (0, 0) = 4	−156	0	0	64	0	0	0
1600 (1, 0) = 4	−76	−8	0	−14	80	160	50
1600 (2, 0) = 4	−76	40	0	−6	120	40	−50
1600 (3, 0) = 4	−76	−8	0	−14	−160	80	−50
1600 (4, 0) = 4	−76	40	0	−6	40	−120	50
1600 (5, 0) = 4	−76	−128	0	16	0	0	0
1600 (6, 0) = 4	−76	40	0	−6	−40	120	50
1600 (7, 0) = 4	−76	−8	0	−14	160	−80	−50
1600 (8, 0) = 4	−76	40	0	−6	−120	−40	−50
1600 (9, 0) = 4	−76	−8	0	−14	−80	−160	50

f odd, $\operatorname{ind} 2 \equiv 5 \pmod{10}$,

(h,k) p	1	c	d	x	u	v	w
1600 (0, 0) = 4	−156	128	0	96	0	0	0
1600 (1, 0) = 4	−76	−40	0	−6	160	320	−150
1600 (2, 0) = 4	−76	8	0	−14	−40	120	−250
1600 (3, 0) = 4	−76	−40	0	−6	−320	160	150
1600 (4, 0) = 4	−76	8	0	−14	120	40	250
1600 (5, 0) = 4	−76	0	0	−16	0	0	0
1600 (6, 0) = 4	−76	8	0	−14	−120	−40	250
1600 (7, 0) = 4	−76	−40	0	−6	320	−160	150
1600 (8, 0) = 4	−76	8	0	−14	40	−120	−250
1600 (9, 0) = 4	−76	−40	0	−6	−160	−320	−150

f odd, $\operatorname{ind} 2 \equiv 5 \pmod{10}$,

(h,k) p	1	c	d	x	u	v	w
1600 (0, 0) = 4	−156	−64	0	80	0	0	0
1600 (1, 0) = 4	−76	16	40	−10	120	240	−50
1600 (2, 0) = 4	−76	16	40	−10	40	80	−150
1600 (3, 0) = 4	−76	16	−40	−10	−240	120	50
1600 (4, 0) = 4	−76	16	−40	−10	80	−40	150
1600 (5, 0) = 4	−76	−64	0	0	0	0	0
1600 (6, 0) = 4	−76	16	−40	−10	−80	40	150
1600 (7, 0) = 4	−76	16	−40	−10	240	−120	50
1600 (8, 0) = 4	−76	16	40	−10	−40	−80	−150
1600 (9, 0) = 4	−76	16	40	−10	−120	−240	−50

A copy of all the formulas may be obtained from the first author. A copy has been placed in the Unpublished Mathematical Tables repository maintained by Mathematics of Computation.

The authors wish to express their appreciation to the University of Pittsburgh's Computer Center for granting access to its IBM7070/1401, IBM7090/1401, and IBM360/50 systems, partially supported under NSF grants G-11309 and GP-2310, and NIH grant FR-00250, respectively.

Table 4 (continued)

$\operatorname{ind} 5 \equiv 0 \pmod 4$, $c \equiv 1 \pmod{10}$

d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
8	8	8	8	8	0	0	0	0	0
24	−56	−56	24	24	0	0	0	0	0
8	8	88	8	−72	0	0	0	0	0
24	−56	24	−56	24	0	0	0	0	0
8	8	8	−72	88	0	0	0	0	0
−136	24	24	24	24	0	0	0	0	0
8	88	−72	8	8	0	0	0	0	0
24	24	−56	24	−56	0	0	0	0	0
8	−72	8	88	8	0	0	0	0	0
24	24	24	−56	−56	0	0	0	0	0

$\operatorname{ind} 5 \equiv 0 \pmod 4$, $c \equiv 9 \pmod{10}$

d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
136	−24	−24	−24	−24	0	0	0	0	0
−8	−88	72	−8	−8	0	0	0	0	0
−24	−24	56	−24	56	0	0	0	0	0
−8	72	−8	−88	−8	0	0	0	0	0
−24	−24	−24	56	56	0	0	0	0	0
−8	−8	−8	−8	−8	0	0	0	0	0
−24	56	56	−24	−24	0	0	0	0	0
−8	−8	−88	−8	72	0	0	0	0	0
−24	56	−24	56	−24	0	0	0	0	0
−8	−8	−8	72	−88	0	0	0	0	0

$\operatorname{ind} 5 \equiv 2 \pmod 4$, $c \equiv 6 \pmod{10}$

d_0	d_4	d_8	d_{12}	d_{16}	d_1	d_5	d_9	d_{13}	d_{17}
72	−8	−8	−8	−8	16	−64	16	16	16
8	−72	8	8	8	16	16	16	−64	16
−8	−8	72	−8	−8	−64	16	16	16	16
8	8	8	−72	8	16	16	−64	16	16
−8	−8	−8	−8	72	16	16	16	16	−64
−72	8	8	8	8	16	−64	16	16	16
−8	72	−8	−8	−8	16	16	16	−64	16
8	8	−72	8	8	−64	16	16	16	16
−8	−8	−8	72	−8	16	16	−64	16	16
8	8	8	8	−72	16	16	16	16	−64

6. Application to residue difference sets. A difference set of modulus v, order k, and multiplicity λ is a set of k distinct residues $r_1, r_2, \ldots, r_k \pmod v$ such that the congruence $r_i - r_j \equiv d \pmod v$ has exactly λ solutions for each $d \not\equiv 0 \pmod v$.

A residue difference set is a difference set consisting of the nonzero eth power residues, modulo a prime p. A difference set formed by zero and the eth power residues is called a modified residue difference set.

Emma Lehmer proved that f is odd is a necessary condition for the existence of a residue difference set or a modified residue difference set. Necessary and sufficient conditions are given, respectively, by

(6.1) $(i,0) = (f-1)/e, \quad i = 0,1,\ldots,E-1$ ([10], Theorem III),

(6.2) $1+(0,0) = (i,0) = (f+1)/e, \quad i = 1,2,\ldots,E-1$ ([10], Theorem III').

THEOREM 14. *If 5 is a biquadratic residue of a prime $p \equiv 1 \pmod{20}$, then the twentieth power residues, with or without zero, do not form a difference set.*

Proof. The arguments to be presented hold both for residue difference sets and modified residue difference sets, as no reference is made to $(0,0)$. It suffices to consider $\operatorname{ind} 2 \equiv 1, 5 \pmod{10}$, for if $\operatorname{ind} 2 \equiv 3, 7$ or $9 \pmod{10}$, one could choose another primitive root g' such that $\operatorname{ind}_{g'} 2 \equiv 1 \pmod{10}$ and the difference set is independent of the choice of g.

The contradictions are obtained from (4.1). The cyclotomic number formulas which are needed have been included in Table 4. Note that by (2.1) and (2.2), $(h,0) = (-h,-h) = (10-h,10-h)$.

First consider $\operatorname{ind} 2 \equiv 5 \pmod{10}$. If $c \equiv 1 \pmod{10}$,

$$4[(1,0)-(9,0)+(2,0)-(8,0)] = u+v = 0,$$

$$4[(4,0)-(6,0)-(3,0)+(7,0)] = u-v = 0.$$

Thus $u = v = 0$. This implies $xw = 0$, so that $16p$ is either a perfect square or divisible by 125; either is impossible.

If $c \equiv 9 \pmod{10}$,

$$4[(1,0)-(9,0)-(2,0)+(8,0)] = u+v = 0,$$

$$4[(4,0)-(6,0)+(3,0)-(7,0)] = -u+v = 0.$$

Again $u = v = 0$, a contradiction.

Now let $\operatorname{ind} 2 \equiv 1 \pmod{10}$. If $c \equiv 1 \pmod{10}$,

$$16[-(1,0)-(3,0)+(7,0)+(9,0)-(2,0)+(4,0)-(6,0)+(8,0)] = u-v+5w = 0,$$

$$16[-(1,0)+(3,0)+3(7,0)-3(9,0)+(2,0)+(4,0)-(6,0)-(8,0)] = -3u-3v+6w+x = 0.$$

Thus $v = u+5w$, $x = 3u+3(u+5w)-6w = 6u+9w$. Then by (4.1)

$$(6u+9w)w = (u+5w)^2-u^2-4u(u+5w),$$

$$16w^2-16wu-4u^2 = 0. \quad (4w-2u)^2 = 2(2u)^2.$$

This equation has only the solution $u = w = 0$. Then $v = 0$, which is impossible.

If $c \equiv 9 \pmod{10}$,

$$16[(1,0)-(3,0)+(7,0)-(9,0)-(2,0)-(4,0)+(6,0)+(8,0)] = -5u+5v-9w = 0,$$

$$16[(1,0)+(3,0)-(7,0)-(9,0)-3(2,0)+3(4,0)+(6,0)-(8,0)] = 7u-v-2w-x = 0.$$

Thus $9w = 5v-5u$, $9x = 73u-19v$. By (4.1),

$$5(v-u)(73u-19v) = 81(v^2-u^2-4uv), \quad 176v^2-784uv+284u^2 = 0.$$

Multiply by 11/4:

$$(22v-49u)^2 = 5(18u)^2.$$

Then $u = v = 0$, which is impossible.

If 5 is a biquadratic nonresidue of p, it suffices to consider just two classes — $\operatorname{ind} 2 \equiv 1$ or $5 \pmod{10}$, $c \equiv 6 \pmod{10}$, because replacing g by g^t, where $t \equiv 11 \pmod{20}$ and t is relatively prime to $p-1$, would leave $\operatorname{ind} 2 \pmod{10}$ unchanged but would yield $c \equiv 4 \pmod{10}$. The formulas for $(h,0)$, $0 \leqslant h \leqslant 9$, for the two classes mentioned above are included in Tables 1 and 4, respectively.

Efforts to prove that there are no residue difference sets or modified residue difference sets for these two classes were unsuccessful.

References

[1] P. Bachmann, *Die Lehre von der Kreisteilung*, Zweite Aufl., Leipzig und Berlin 1921.

[2] L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. 21 (1967), pp. 204–219.

[3] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1934), pp. 151–182.

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

[5] — *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), pp. 363–380.

[6] — *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. 38 (1935), pp. 187–200.

[7] R. E. Giudici, J. B. Muskat and S. F. Robinson, *On the evaluation of Brewer's character sums* (in preparation).

[8] Marshall Hall, Jr., *Combinatorial theory*, Waltham, Mass., 1967.

[9] Helmut Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, *Reziprozitätsgesetz*, Würzburg–Wien 1965.

[10] E. Lehmer, *On residue difference sets*, Canad. J. Math. 5 (1953), pp. 425–432.

[11] E. Lehmer, *On the number of solutions of* $u^k+D \equiv w^2 (\mathrm{mod}\, p)$, Pacific J. Math. 5 (1955), pp. 103–118.

[12] J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. 11 (1966), pp. 263–279.

[13] A. L. Whiteman, *Finite Fourier series and equations in finite fields*, Trans. Amer. Math. Soc. 74 (1953), pp. 78–98.

[14] — *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), pp. 401–413.

[15] — *The cyclotomic numbers of order ten*, Proceedings of the Symposia in Applied Mathematics 10, pp. 95–111, American Mathematical Society, Providence, Rhode Island 1960.

[16] — *The cyclotomic numbers of order twelve*, Acta Arith. 6 (1960), pp. 53–76.

[17] — *Theorems on Brewer and Jacobsthal sums*, Proceedings of Symposia in Pure Mathematics 8, pp. 44–55, American Mathematical Society, Providence, Rhode Island 1965.

UNIVERSITY OF PITTSBURGH
THE INSTITUTE FOR ADVANCED STUDY
UNIVERSITY OF SOUTHERN CALIFORNIA

Received on 19. 6. 1969

ACTA ARITHMETICA
XVII (1970)

A metric inequality associated with valuated fields

by

P. E. Blanksby (Cambridge)

1. Introduction. Suppose that $\boldsymbol{F}$ is a field with a valuation $\| \ \|$, mapping $\boldsymbol{F}$ into $\boldsymbol{R}$, the real numbers. Let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be two points in the cartesian product $\boldsymbol{F}^n = \boldsymbol{F} \times \ldots \times \boldsymbol{F}$, with coordinates $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ respectively. We can define a function from $\boldsymbol{F}^n \times \boldsymbol{F}^n$ to $\boldsymbol{R}$ as follows:

$$d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \min_{\sigma \in S_n} \max_{1 \leqslant j \leqslant n} \|\alpha_j - \beta_{\sigma(j)}\|,$$

where S_n is the symmetric group on n objects. It is clear that if we write $\sigma\boldsymbol{\alpha} = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$, then for any σ, τ in S_n we have $d(\sigma\boldsymbol{\alpha}, \tau\boldsymbol{\beta}) = d(\boldsymbol{\alpha}, \boldsymbol{\beta})$.

It follows that $d(\boldsymbol{\alpha}, \boldsymbol{\beta})$ satisfies the triangle inequality since we may suppose, by taking a suitable permutation of the coordinates if necessary, that

$$d(\boldsymbol{\alpha}, \boldsymbol{\gamma}) = \max_{1 \leqslant j \leqslant n} \|\alpha_j - \gamma_j\|,$$

and

$$d(\boldsymbol{\gamma}, \boldsymbol{\beta}) = \max_{1 \leqslant j \leqslant n} \|\gamma_j - \beta_j\|.$$

Hence

$$d(\boldsymbol{\alpha}, \boldsymbol{\beta}) \leqslant \max_{1 \leqslant j \leqslant n} \|\alpha_j - \beta_j\| \leqslant \max_{1 \leqslant j \leqslant n} \|\alpha_j - \gamma_j\| + \max_{1 \leqslant j \leqslant n} \|\gamma_j - \beta_j\| = d(\boldsymbol{\alpha}, \boldsymbol{\gamma}) + d(\boldsymbol{\gamma}, \boldsymbol{\beta}).$$

Thus $d(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is a pseudo-metric on $\boldsymbol{F}^n$.

We define the real quantities

$$\mathfrak{M}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathfrak{M} = \max_{1 \leqslant j \leqslant n} \max \{\|\alpha_j\|, \|\beta_j\|\},$$

$$\mathfrak{N}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathfrak{N} = \prod_{j,k} \|\alpha_j - \beta_k\|.$$

In this paper we seek lower bounds on $d(\boldsymbol{\alpha}, \boldsymbol{\beta})$ in terms of $\mathfrak{M}$ and $\mathfrak{N}$. If $\| \ \|$ is a non-archimedean valuation, then it readily follows that if $\mathfrak{M} > 0$, then

$$d(\boldsymbol{\alpha}, \boldsymbol{\beta}) \geqslant \frac{\mathfrak{N}^{1/n}}{\mathfrak{M}^{n-1}}.$$