ON JACOBI SUMS OF CERTAIN COMPOSITE ORDERS(1)

BY
JOSEPH B. MUSKAT

The Jacobi sums play a fundamental role in the theory of cyclotomy. Some criteria for power residuacity can be expressed in terms of them; e.g., [9]. Formulas for the number of solutions $(h, k)_e$ of

$$g^{es+h}+1 \equiv g^{et+k} \pmod{p}, \qquad 0 \leqq s, t < (p-1)/e,$$

where p is a prime $\equiv 1 \pmod{e}$ and g is a primitive root of p, can be expressed in terms of the Jacobi sums of order e [12, (2.7)].

In 1935, L. E. Dickson published a series of three papers which reviewed and extended the theory of cyclotomy. In the first he gave relationships between the Jacobi sums of orders e, $e \leqq 6$, $e=8$, 10, and 12 [3]. He discussed the sums of prime order and of order twice a prime, then treated explicitly $e=14$ and 22, in the second paper [4]. In his final contribution he studied $e=9$ and 18. (Sign omissions in formulas (37) were noted in [1]; an ambiguous sign in (44) was also resolved.) The last part of this paper is entitled

THEORY FOR $\phi(e) = 8$, $e = 15, 16, 20, 24, 30$.

One relation associated with $e=16$ was omitted. The case $e=15$ was left with an undetermined sign. Only sketchy discussions were given to $e=20$ and 24, while $e=30$ was ignored completely [5].

In this paper the sign ambiguity for $e=15$ is resolved, and complete analyses for $e=24$ and 30 are given. Progress is also made toward fixing the sign of a fourth root of unity which arises in connection with the Jacobi sums of order 12. Complete treatments of $e=16$ and 20 are found in [11] and [13], respectively.

The Jacobi sum $R(m, n)$ of order e is defined by

$$R(m, n) = \sum_{a=2}^{p-1} \beta^{m \operatorname{ind}_g a + n \operatorname{ind}_g (1-a)}, \qquad \beta = \exp(2\pi i/e). \tag{1}$$

Closely related to the Jacobi sum is the Gaussian sum

$$\tau(s) = \sum_{k=1}^{p-1} \beta^{s \operatorname{ind}_g k} \zeta^k, \qquad \zeta = \exp(2\pi i/p). \tag{2}$$

Received by the editors December 27, 1966 and, in revised form, August 20, 1967.

(1) This research was partially supported by National Science Foundation Grants GP-2091 and GP-5308.

The relation is

$$R(m, n) = \tau(m)\tau(n)/\tau(m+n), \tag{3}$$

provided e does not divide m, n, or $m+n$ [2, (0.6)].

Let $f=(p-1)/e$. Consequences of these definitions are

$$\tau(s)\tau(-s) = (-1)^{sf}p \quad \text{if } e\nmid s, \tag{4}$$

$$R(m, n) = R(n, m) = (-1)^{nf}R(-m-n, n), \tag{5}$$

$$R(m, n)R(m+n, r) = R(m, r)R(m+r, n). \tag{6}$$

(The use of (6) will be noted by displaying alongside the equation the bracketed triple $[m, n, r]$.)

By (3) and (4), if e does not divide m, n or $m+n$, then

$$R(m, n)R(-m, -n) = p. \tag{7}$$

If $(j, e)=1$, let σ_j denote the automorphism which maps β onto β^j. Then

$$\sigma_j R(m, n) = R(jm, jn), \qquad \sigma_j\tau(s) = \tau(js). \tag{8}$$

Let $e=xy$. If $R_x(m, n)$ denotes a Jacobi sum of order x,

$$R_x(m, n) = R(ym, yn) \qquad [5, (3)]. \tag{9}$$

Three special cases of the identity

$$\prod_{k=0}^{y-1} \tau(kx+t) = \beta^{-ty \operatorname{ind}_g y}\tau(ty)\prod_{k=1}^{y-1} \tau(kx) \qquad [2, (0.9_1)]$$

will be used, corresponding to $y=2$, 3, and 5:

$$\tau(t)\tau(t+e/2) = \beta^{-2tZ}\tau(2t)\tau(e/2), \text{ where } Z = \operatorname{ind}_g 2. \tag{10}$$

$$\tau(t)\tau(t+e/3)\tau(t+2e/3) = \beta^{-3tT}\tau(3t)p, \text{ where } T = \operatorname{ind}_g 3. \tag{11}$$

$$\begin{aligned}\tau(t)\tau(t+e/5)\tau(t+2e/5)\tau(t+3e/5)\tau(t+4e/5)\\ = \beta^{-5tF}\tau(5t)p^2, \text{ where } F = \operatorname{ind}_g 5.\end{aligned} \tag{12}$$

In this study it is assumed that the $R(m, n)$ for which the greatest common divisor of m, n and e is greater than 1 are already known, as they are in fact Jacobi sums of orders which are proper divisors of e, by (9). The remaining sums are grouped into classes of conjugates, each class consisting of the automorphic images of a single sum. Accordingly, relationships will be presented in terms of a single representative of each conjugate class. By (5), a Jacobi sum may be expressible in the form $R(m, n)$ in several ways. Thus $R(1, n)$ and $R(1, e-1-n)$ would not both be representatives.

If in a numbered formula a certain value of e is assumed, the value of e will appear as a subscript to the formula number.

The Jacobi sums of order 12 are conjugate to $R(1, 1)$, $R(1, 2)$, $R(1, 3)$, $R(1, 4)$, $R(1, 5)$, and Jacobi sums of lower orders. The following relations were determined by Dickson: [3, pp. 417–418]

$$(13_{12}) \qquad R(1, 1) = \beta^{-2Z+3T}R(3, 3),$$

$$(14_{12}) \qquad cR(1, 2) = R(2, 4),$$

$$(15_{12}) \qquad cR(1, 3) = R(3, 3),$$

$$(16_{12}) \qquad R(1, 4) = (-1)^f\beta^{-2Z}R(2, 4) = R(4, 4),$$

$$(17_{12}) \qquad R(1, 5) = (-1)^f\beta^{3T}R(3, 3),$$

where $c=R(1, 3)/R(1, 5)$. He also showed that $c^2=(-1)^f\beta^{3T}$, so that c is a fourth root of unity. More precise information is given by Theorem 1, and equations (28) and (78).

The Jacobi sums of order 24 are conjugate to $R(1, n)$, $1 \leqq n \leqq 11$, and Jacobi sums of lower orders. All the Jacobi sums of order 12 must now be expressed as if $e=24$; e.g., (13) becomes

$$R(2, 2) = \beta^{-4Z+6T}R(6, 6).$$

The first two relations below were derived from (11) by Dickson (who omitted the $(-1)^f$ factor from the former): [5, p. 200]

$$(18_{24}) \qquad R(1, 6) = (-1)^f\beta^{-3T}R(3, 6),$$

$$(19_{24}) \qquad R(1, 9) = \beta^{-3T}\sigma_7R(1, 2).$$

By (10), with $t=3$,

$$\tau(3)\tau(15) = \beta^{-6Z}\tau(6)\tau(12).$$

$$R(3, 15) = (-1)^fR(3, 6) = \beta^{-6Z}R(6, 12) = \beta^{-6Z}R(6, 6),$$

by (3) and (5). Combine with (18):

$$(20_{24}) \qquad R(1, 6) = \beta^{6Z-3T}R(6,6),$$

since $\beta^{12Z}=1$. Also, $\beta^{12T}=1$, so

$$(21_{24}) \qquad \sigma_5R(1, 6) = \sigma_{13}R(1, 6) = \sigma_{17}R(1, 6) = R(1, 6).$$

$$R(1, 6)\sigma_5R(1, 11) = \sigma_5R(1, 6)R(1, 11) \qquad [6, 1, 5].$$

$$(22_{24}) \qquad \sigma_5R(1, 11) = R(1, 11),$$

by (21). Since $\sigma_7=\sigma_5\sigma_{11}$,

$$(23_{24}) \qquad \sigma_7R(1, 11) = R(1, 11).$$

By (10), with $t=1$,

$$(24_{24}) \qquad \tau(1)\tau(13) = \beta^{-2Z}\tau(2)\tau(12).$$

$$(25_{24}) \qquad R(1, 1) = (-1)^f\beta^{-2Z}R(1, 11),$$

by (3) and (5). By (23),

$$(26_{24}) \qquad \sigma_7 R(1, 1) = R(1, 1).$$

$\tau(8)\tau(8) = p\tau(2)/\tau(10)$ follows from (16) and (4). Setting $p = \tau(14)\tau(10)$ gives $\tau(8)\tau(8) = \tau(2)\tau(14)$. Then

$$\frac{\tau(1)\tau(7)}{\tau(8)}\frac{\tau(1)\tau(7)}{\tau(8)} = \frac{\tau(1)\tau(1)}{\tau(2)}\frac{\tau(7)\tau(7)}{\tau(14)}.$$

$$R(1, 7)^2 = R(1, 1)\sigma_7 R(1, 1).$$

$$(27_{24}) \qquad R(1, 7) = dR(1, 1),$$

by (26), where $d = \pm 1$. d is specified completely in equation (94).

$$R(1, 1)R(2, 6) = R(1, 6)R(1, 7) \qquad [1, 1, 6].$$

$$R(6, 6)/c = \beta^{6Z-3T}R(6, 6)d,$$

by (15), (20), and (27). Thus

$$(28_{24}) \qquad c = d\beta^{6Z+3T}.$$

From (24), with two applications of (5),

$$(-1)^f R(1, 10) = \beta^{-2Z}R(2, 10).$$

$$(29_{24}) \qquad R(1, 10) = (-1)^f\beta^{-2Z+6T}R(6, 6),$$

by (17). Combine with (20):

$$(30_{24}) \qquad R(1, 10) = (-1)^f\beta^{4Z-3T}R(1, 6).$$

$$R(1, 5)R(1, 6) = R(1, 1)\sigma_5 R(1, 10) \qquad [1, 5, 1].$$

$$R(1, 5)\sigma_5 R(1, 6) = R(1, 1)\sigma_5 R(1, 10),$$

by (21). Divide by equation (30) to which σ_5 has been applied:

$$(31_{24}) \qquad R(1, 5) = (-1)^f\beta^{-4Z-3T}R(1, 1).$$

$$R(1, 4)R(1, 5) = R(1, 1)R(2, 4) \qquad [1, 4, 1].$$

$$R(1, 4) = (-1)^f\beta^{4Z+3T}R(4, 8)/c,$$

by (31) and (14). By (28) and (16),

$$(32_{24}) \qquad R(1, 4) = (-1)^f\, d\beta^{2Z}R(8, 8).$$

$$R(1, 7)R(1, 8) = R(1, 1)(-1)^f\sigma_7 R(1, 9) \qquad [1, 7, 1].$$

$$(33_{24}) \qquad R(1, 8) = d(-1)^f\sigma_7 R(1, 9),$$

by (27).

$$R(1, 3)R(4, 4) = R(1, 4)(-1)^f\sigma_5 R(1, 8) \qquad [1, 3, 4].$$

Since

$$R(4, 4) = \beta^{-4Z}R(8, 8) \qquad [3, (84)],$$

$$(34_{24}) \qquad R(1, 3) = d\beta^{6Z}\sigma_5 R(1, 8),$$

by (32).

For $e=15$, Jacobi sums are conjugate to $R(1, 1)$, $R(1, 2)$, $R(1, 3)$, $R(1, 4)$, $R(1, 5)$, and Jacobi sums of lower orders, for by (5) and (8)

$$(35_{15}) \qquad R(1, 6) = R(1, 8) = \sigma_8 R(1, 2),$$

$$(36_{15}) \qquad R(1, 7) = R(7, 7) = \sigma_7 R(1, 1).$$

Dickson showed [5, pp. 198–199] that

$$(37_{15}) \qquad R(1, 3) = \beta^{-3T}R(3, 3),$$

$$(38_{15}) \qquad \sigma_2 R(1, 2) = \beta^{3T}R(1, 2),$$

$$(39_{15}) \qquad R(1, 5) = b\beta^{6T-5F}R(1, 1),$$

$$(40_{15}) \qquad R(1, 4) = b\beta^{-3T+5F}R(1, 2),$$

where $b=\pm 1$. b is specified completely by equation (102).

Now let $e=30$. Since

$$(41_{30}) \qquad \sigma_7 R(1, 13) = R(1, 7), \quad \sigma_{23}R(1, 12) = R(1, 6),$$

the Jacobi sums of order 30 are conjugate to $R(1, n)$, $1 \leqq n \leqq 11$, $R(1, 14)$, $R(2, 3)$, and Jacobi sums of lower orders.

From (10), with $t=1$,

$$(42_{30}) \qquad \tau(1)\tau(16) = \beta^{-2Z}\tau(2)\tau(15).$$

$$(43_{30}) \qquad R(1, 1) = (-1)^f\beta^{-2Z}R(1, 14),$$

by (3) and (5). Also from (42),

$$\tau(1)\tau(14)/\tau(15) = \beta^{-2Z}\tau(2)\tau(14)/\tau(16).$$

$$R(1, 14) = \beta^{-2Z}R(2, 14).$$

$$(44_{30}) \qquad R(1, 14) = \beta^{-2Z}\sigma_7 R(2, 2),$$

by (36).

$$\sigma_{13}R(1, 7)R(1, 14) = R(1, 1)\sigma_{13}R(1, 14) \qquad [1, 13, 1].$$

$$\sigma_{13}R(1, 7) = (-1)^f\beta^{-2Z}\sigma_{13}R(1, 14),$$

by (43). Apply the automorphism σ_7:

$$(45_{30}) \qquad R(1, 7) = (-1)^f\beta^{-14Z}R(1, 14).$$

$$R(1, 7)R(1, 8) = R(1, 1)(-1)^f\sigma_7 R(1, 3) \qquad [1, 7, 1].$$

$$(46_{30}) \qquad R(1, 8) = (-1)^f\beta^{12Z}\sigma_7 R(1, 3),$$

by (43) and (45).

From (11) with $t=1$ and $p=\tau(22)\tau(8)$,

$$R(1, 21) = \beta^{-3T}R(3, 8).$$

$$(47_{30}) \qquad R(1, 8) = (-1)^f\beta^{-3T}\sigma_{19}R(1, 2).$$

$$R(1, 6)R(1, 7) = R(1, 1)R(2, 6) \qquad [1, 6, 1].$$

$$(48_{30}) \qquad R(1, 6) = \beta^{12Z}R(2, 6),$$

$$(49_{30}) \qquad R(1, 6) = \beta^{12Z-6T}R(6, 6),$$

by (37).

$$R(1, 3)\sigma_{17}R(2, 6) = R(1, 14)(-1)^f R(3, 12) \qquad [1, 3, 14].$$

$$R(1, 3)\beta^{-12T}\sigma_{17}R(6, 6) = R(1, 14)(-1)^f\beta^{-6Z}R(12, 12),$$

by (37) and [12, (2.24)]. Hence

$$(50_{30}) \qquad R(1, 3) = (-1)^f\beta^{-6Z+12T}R(1, 14).$$

$$R(1, 1)R(2, 3) = R(1, 3)R(1, 4) \qquad [1, 1, 3].$$

By (43) and (50),

$$(51_{30}) \qquad R(2, 3) = \beta^{-4Z+12T}R(1, 4).$$

Combine (39) with (44): Since $\beta^{15F}=1$,

$$(52_{30}) \qquad \sigma_7R(2, 10) = b\beta^{2Z-6T+5F}R(1, 14).$$

$$R(1, 9)\sigma_7R(2, 10) = R(1, 6)(-1)^f\sigma_7R(1, 2) \qquad [1, 9, 6].$$

$$(53_{30}) \qquad R(1, 9) = b\beta^{-2Z-3T-5F}R(1, 6),$$

by (52), (47), (46), and (50).

$$R(1, 6)\sigma_7R(1, 5) = R(1, 5)R(6, 6) \qquad [1, 6, 5].$$

$$(54_{30}) \qquad \sigma_7R(1, 5) = \beta^{-12Z+6T}R(1, 5),$$

by (49).

$$R(1, 11)(-1)^f\sigma_{13}R(1, 5) = R(1, 5)\sigma_{11}R(1, 6) \qquad [1, 11, 5].$$

Divide by equation (54) to which σ_{13} has been applied; then apply σ_{11}:

$$(55_{30}) \qquad R(1, 11) = (-1)^f\beta^{-6Z-12T}R(1, 6).$$

$$R(1, 5)\sigma_7R(2, 10) = R(1, 14)R(5, 15) \qquad [1, 5, 14].$$

By (10), with $t=5$,

$$R(5, 5) = \beta^{-10Z}R(5, 15) = (-1)^f\beta^{10Z}R(10, 10).$$

Hence by (52),

$$(56_{30}) \qquad R(1, 5) = b\beta^{8Z+6T-5F}R(5, 5) = (-1)^f b\beta^{-12Z+6T-5F}R(10, 10).$$

$$\sigma_{11}R(1, 4)\sigma_{11}R(5, 5) = \sigma_{11}R(1, 5)\sigma_7R(2, 10) \qquad [11, 14, 25].$$

By (52), and with σ_{11} applied to (56),

$$\sigma_{11}R(1, 4) = \beta^{-5F}R(1, 14). \tag{57_{30}}$$

$$R(1, 10)(-1)^f\sigma_{11}R(1, 4) = R(1, 5)\sigma_7 R(2, 10) \qquad [1, 10, 5].$$

$$R(1, 10) = (-1)^f b\beta^{2Z-6T-5F}R(1, 5), \tag{58_{30}}$$

by (57) and (52).

More information about the incompletely determined factors c, d, and b, defined by (15), (27), and (40), respectively, can be gained from further investigation of the theory of cyclotomy of orders 12, 24, and 15, respectively. Since in each case e has two distinct prime factors, each Jacobi sum of order e has a representation of the form $R(n, vn)$, v an integer. (By contrast, this is not true for $R(2, 3)$, $e=30$.) Collecting the exponents of β in (1) which are in the same residue class (mod e) yields the following expansion of $R(n, vn)$ in a finite Fourier series:

$$R(n, vn) = (-1)^{vnf}\sum_{i=0}^{e-1} B(i, v)\beta^{ni} \qquad [10, (2.6)]. \tag{59}$$

Let $(h, k)_e$ denote the number of solutions of

$$g^{es+h}+1 \equiv g^{et+k} \pmod p, \quad 0 \leqq s, t \leqq f-1.$$

The $(h, k)_e$ are called cyclotomic numbers. The coefficients $B(i, v)$ in (59) are Dickson-Hurwitz sums [10, (2.7)] defined by

$$B(i, v) = \sum_{h=0}^{e-1} (h, i-vh)_e. \tag{60}$$

It follows that if $e=xy$, and if $B_x(i, v)$ denotes a Dickson-Hurwitz sum of order x,

$$B_x(i, v) = \sum_{j=0}^{y-1} B(i+jx, v). \tag{61}$$

A. L. Whiteman proved that if $(v, e)=1$, then

$$B(i, v) = B(iv', v'), \text{ where } vv' \equiv 1 \pmod e \qquad [12, \text{Lemma } 1]. \tag{62}$$

The cyclotomic numbers satisfy [3, p. 394]

$$(h, k)_e = (e-h, k-h)_e, \tag{63}$$

$$\begin{aligned}(h, k)_e &= (k, h)_e, && f \text{ even},\\ &= (k+\tfrac{1}{2}e, h+\tfrac{1}{2}e)_e, && f \text{ odd},\end{aligned} \tag{64}$$

$$\begin{aligned}\sum_{k=0}^{e-1}(h, k)_e &= f-1, && \text{if } f \text{ is even and } h \equiv 0 \pmod e,\\ &= f-1, && \text{if } f \text{ is odd and } h \equiv \tfrac{1}{2}e \pmod e,\\ &= f, && \text{otherwise.}\end{aligned} \tag{65}$$

An immediate consequence is

$$\sum_{h=0}^{e-1}(h,k) = f-1, \quad \text{if } k \equiv 0 \pmod{e}, \tag{66}$$
$$= f, \qquad \text{otherwise.}$$

It follows that

$$B(i,0) = f-1, \quad e|i, \tag{67}$$
$$= f, \qquad e\nmid i.$$

From (60) and (63),

$$B(i,v) = B(i, e-v-1). \tag{68}$$

Combining (67) and (68) gives

$$B(i, e-1) = f-1, \quad e|i, \tag{69}$$
$$= f, \qquad e\nmid i.$$

If e is even and $E=e/2$,

$$(h,k)_E = (h,k)_e+(h+E,k)_e+(h,k+E)_e+(h+E,k+E)_e \quad [11, (2.6)]. \tag{70}$$

Let Q denote the field of rationals. Let $e=12$. $Q(\beta)$ is a fourth-degree extension of Q. $\{1, \beta, \beta^2, \beta^3\}$ is a basis for $Q(\beta)$ over Q. Let $D(i,v)=B(i,v)-B(i+6,v)$. Then $D(i,v)=-D(i+6,v)$. Since $1+\beta^4+\beta^8=0$,

$$(-1)^{vf}R(1,v) = \sum_{i=0}^{11} B(i,v)\beta^i = \sum_{i=0}^{5} D(i,v)\beta^i = D(0,v)-D(4,v)$$
$$+[D(1,v)-D(5,v)]\beta+[D(2,v)+D(4,v)]\beta^2+[D(3,v)+D(5,v)]\beta^3.$$

A column vector notation will be used to represent Jacobi sums in terms of the basis to simplify visualizing the equating of coefficients of basis elements. The nth component, $0 \leqq n \leqq \phi(e)-1$, will be the coefficient of β^n. Thus

$$(-1)^{vf}R(1,v) = \begin{bmatrix} D(0,v)-D(4,v) \\ D(1,v)-D(5,v) \\ D(2,v)+D(4,v) \\ D(3,v)+D(5,v) \end{bmatrix}.$$

$$D(0,3)+D(4,3)+D(8,3) = D_4(0,3) = -1, \tag{71_{12}}$$

by (61) and (69). Similarly,

$$D(1,3)+D(5,3)+D(9,3) = 0. \tag{72_{12}}$$

Since c is a fourth root of unity, it follows from (15) that $R(1, 3)$ is invariant under the automorphism σ_5.

$$(73_{12})\qquad (-1)^f R(1,3) = \begin{bmatrix} D(0,3)-D(4,3) \\ D(1,3)-D(5,3) \\ -D(8,3)+D(4,3) \\ -D(9,3)+D(5,3) \end{bmatrix} \qquad (-1)^f \sigma_5 R(1,3) = \begin{bmatrix} D(0,3)-D(8,3) \\ D(5,3)-D(1,3) \\ -D(4,3)+D(8,3) \\ -D(9,3)+D(1,3) \end{bmatrix}.$$

Equate coefficients of β:

$$(74_{12})\qquad D(1,3) = D(5,3).$$

Combining with (72) shows that

$$(75_{12})\qquad -D(9,3)+D(1,3) = 3D(1,3).$$

Equate coefficients of β^2:

$$(76_{12})\qquad D(4,3) = D(8,3).$$

Combine with (71):

$$(77_{12})\qquad D(0,3)-D(4,3) = -1-3D(4,3).$$

Substituting (74), (75), (76), and (77) into (73) yields

$$(-1)^f R(1,3) = -1-3D(4,3)+3D(1,3)i.$$

$$R(3,3) = -X+2Yi, \quad X \equiv 1 \pmod 4,\ X^2+4Y^2 = p \quad [3, \text{pp. } 400\text{–}401].$$

By (15),

$$(78_{12})\qquad c[-1-3D(4,3)+3D(1,3)i] = (-1)^f(-X+2Yi).$$

If $c=1$, equating real parts in (78) gives

$$-1 \equiv (-1)^f(-X) \pmod 3; \quad X \equiv (-1)^f \pmod 3.$$

If $c=-1$, $X \equiv -(-1)^f \pmod 3$.

If $c=i$, equating imaginary parts in (78) yields

$$-1 \equiv (-1)^f 2Y \pmod 3; \quad Y \equiv (-1)^f \pmod 3.$$

If $c=-i$, $Y \equiv -(-1)^f \pmod 3$.

This proves that $c=\pm 1$ if and only if $3 \mid Y$, and also

THEOREM 1. *Let* $p \equiv 1 \pmod{12}$, $p=X^2+4Y^2$, $X \equiv 1 \pmod 4$. *If f is even and* $X \equiv 1 \pmod{12}$ *or f is odd and* $X \equiv 5 \pmod{12}$, *then* $c=1$. *If f is even and* $X \equiv 5 \pmod{12}$ *or f is odd and* $X \equiv 1 \pmod{12}$, *then* $c=-1$.

If $c=\pm i$, the analogue of Theorem 1 cannot be formulated without knowing $R_4(1, 1)$, or something equivalent, explicitly, because the sign of Y depends upon the choice of the primitive root g.

Let $e=24$. $Q(\beta)$ is an eighth-degree extension of Q. Let $D(i, v)=B(i, v)-B(i+12, v)$. A basis representation for $(-1)^{vf}R(1, v)$ is given in Figure 1. The fact that $1+\beta^8+\beta^{16}=0$ is used in determining the components.

$$(79_{24})\qquad \begin{bmatrix} D(0, v)-D(8, v) \\ D(1, v)-D(9, v) \\ D(2, v)-D(10, v) \\ D(3, v)-D(11, v) \\ D(4, v)+D(8, v) \\ D(5, v)+D(9, v) \\ D(6, v)+D(10, v) \\ D(7, v)+D(11, v) \end{bmatrix}$$

FIGURE 1

Apply (62) to the $D(i, 11)$:

$$(80_{24})\qquad \begin{aligned} &D(1, 11) = D(11, 11),\ D(2, 11) = -D(10, 11),\ D(3, 11) = D(9, 11), \\ &D(4, 11) = -D(8, 11),\ D(5, 11) = D(7, 11),\ D(6, 11) = -D(6, 11) = 0. \end{aligned}$$

Incorporating (80) into (79) gives the following representations for $(-1)^f R(1, 11)$ and $(-1)^f\sigma_5 R(1, 11)$ shown in Figure 2:

$$(-1)^f R(1, 11) = \begin{bmatrix} D(0, 11)+D(4, 11) \\ D(1, 11)-D(3, 11) \\ 2D(2, 11) \\ D(3, 11)-D(1, 11) \\ 0 \\ D(5, 11)+D(3, 11) \\ -D(2, 11) \\ D(1, 11)+D(5, 11) \end{bmatrix} \qquad (-1)^f\sigma_5 R(1, 11) = \begin{bmatrix} D(0, 11)+D(4, 11) \\ D(5, 11)+D(3, 11) \\ -2D(2, 11) \\ -D(3, 11)-D(5, 11) \\ 0 \\ D(1, 11)-D(3, 11) \\ D(2, 11) \\ D(5, 11)+D(1, 11) \end{bmatrix}$$

FIGURE 2

$\sigma_5 R(1, 11)=R(1, 11)$, by (22), so coefficients may be equated. For β^6, $D(2, 11)=0$. Equate coefficients of β:

$$D(1, 11)-D(3, 11) = D(3, 11)+D(5, 11).$$

Then

$$2[D(1, 11)-D(3, 11)] = D(1, 11)+D(5, 11).$$

Thus if

$$U = D(0, 11)+D(4, 11), \qquad W = D(1, 11)-D(3, 11),$$
$$(-1)^f R(1, 11) = U+W(\beta-\beta^3+\beta^5+2\beta^7) = U+W(-6)^{1/2}.$$

By (7), $U^2+6W^2=p$. Since $p\equiv U^2\equiv 1 \pmod{24}$, W is even. Hence if $W=2V$, $p=U^2+24V^2$, and

$$(81_{24}) \qquad (-1)^f R(1,11) = U+2(-6)^{1/2}V, \quad U = D(0,11)+D(4,11),$$
$$V = \tfrac{1}{2}[D(1,11)-D(3,11)].$$

From (25) and (27),

$$\beta^{2Z}(-1)^f\, dR(1,7) = R(1,11).$$

$$R(1,11) = \beta^{-6Z}(-1)^f\, d\beta^{8Z}R(1,7) = \beta^{6Z}\, d\sum_{i=0}^{23} B(i,7)\beta^{i+8Z}.$$

$$R(1,11) = \beta^{6Z}\, d\sum_{i=0}^{23} B(i-8Z,7)\beta^{i}.$$

$$\beta^{6Z}d\begin{bmatrix} D(-8Z,7)-D(8-8Z,7) \\ D(1-8Z,7)-D(9-8Z,7) \\ D(2-8Z,7)-D(10-8Z,7) \\ D(3-8Z,7)-D(11-8Z,7) \\ D(4-8Z,7)+D(8-8Z,7) \\ D(5-8Z,7)+D(9-8Z,7) \\ D(6-8Z,7)+D(10-8Z,7) \\ D(7-8Z,7)+D(11-8Z,7) \end{bmatrix} = R(1,11) = (-1)^f\begin{bmatrix} U \\ 2V \\ 0 \\ -2V \\ 0 \\ 2V \\ 0 \\ 4V \end{bmatrix}$$

FIGURE 3

Equate coefficients of β^4:

$$D(8-8Z,7) = -D(4-8Z,7) = D(16-8Z,7).$$

By (69) and (61),

$$(82_{24}) \qquad -1 = D_8(0,7) = D(-8Z,7)+D(8-8Z,7)+D(16-8Z,7)$$
$$= D(-8Z,7)+2D(8-8Z,7).$$

Equate coefficients of 1:

$$\beta^{6Z}\, d[D(-8Z,7)-D(8-8Z,7)] = (-1)^f U.$$
$$\beta^{6Z}\, d[D(-8Z,7)+2D(8-8Z,7)] \equiv (-1)^f U \pmod 3.$$

By (82),

$$(83_{24}) \qquad d \equiv -(-1)^f\beta^{6Z}U \pmod 3.$$

If k is odd and $(j,k)=1$, let $(j|k)$ denote the Jacobi symbol. If k is prime, let $(j|k)_4$ denote the quartic residue symbol:

$(j|k)_4 = 1$ if j is a quartic residue (mod k);

$(j|k)_4 = -1$ if $(j|k) = 1$ but j is not a quartic residue (mod k).

The symbol $(j|k)_4$ will not be used if $(j|k)=-1$.

Since $\beta^{6Z}=(2|p)_4$ and $U\equiv(U|3)$ (mod 3), (83) becomes

$$d = -(-1)^f(2|p)_4(U|3). \tag{84}$$

To simplify (84), further study of the cyclotomic numbers is necessary. The following was proved by Emma Lehmer [6, Lemma I]:

LEMMA. *Let* $Z\equiv\operatorname{ind} 2 \pmod e$. *The cyclotomic number* $(0, Z)_e$ *is odd. All other cyclotomic numbers* $(0, k)_e$, $0\leqq k\leqq e-1$, *are even.*

Now assume $4|e$, and let $e=2E$. Let $D(i, v)=B(i, v)-B(i+E, v)$.

THEOREM 2.

$$D(0, E) = 1+2\sum_{h=0}^{\frac{1}{2}E-1}(0, 2h)_E-4\sum_{j=0}^{E-1}(2j, E)_e.$$

Proof. $D(0, E)=\sum_{h=0}^{e-1}[(h, -Eh)_e-(h, E-Eh)_e]$, by (60). According to (66) $\sum_{h=0}^{e-1}[(h, 0)_e-(h, E)_e]=-1$. Thus

$$\begin{aligned} D(0, E)-1 &= \sum_{h=0}^{e-1}[(h, -Eh)_e-(h, E-Eh)_e+(h, 0)_e-(h, E)_e] \\ &= 2\sum_{j=0}^{E-1}[(2j, 0)_e-(2j, E)_e] \\ &= 2\sum_{j=0}^{E-1}[(2j, 0)_e+(2j, E)_e-2(2j, E)_e] \\ &= 2\sum_{h=0}^{\frac{1}{2}E-1}(2h, 0)_E-4\sum_{j=0}^{E-1}(2j, E)_e, \end{aligned}$$

by (70),

$$= 2\sum_{h=0}^{\frac{1}{2}E-1}(0, 2h)_E-4\sum_{j=0}^{E-1}(2j, E)_e,$$

by (64).

COROLLARY 1. *Let* $8|e$. *Then*

$$D(0, E) \equiv 1-4f+2\sum_{h=0}^{\frac{1}{2}E-1}(0, 2h)_E \pmod 8.$$

Proof. If f is even, by (63) and (64), $(2j, E)_e=(E, 2j)_e=(E, 2j-E)_e=(2j-E, E)_e$.

$$4\sum_{j=0}^{E-1}(2j, E)_e = 8\sum_{h=0}^{\frac{1}{2}E-1}(2h, E)_e \equiv 0 \equiv 4f \pmod 8.$$

If f is odd, by (64), $(2j, E)_e=(0, 2j+E)_e$.

$$4\sum_{j=0}^{E-1}(2j, E)_e = 4\sum_{k=0}^{E-1}(0, 2k)_e \equiv 4 \equiv 4f \pmod 8,$$

for as $(2|p)=1$, exactly one of the terms in the last sum is odd, by the lemma.

COROLLARY 2. *Let* $e=8$. *Then* $D(0, 4)\equiv 7-2\operatorname{ind} 2 \pmod 8$.

Proof. $2\sum_{h=0}^{1}(0, 2h)_4 = 2[(0, 0)_4 + (0, 2)_4] = 2(0, 0)_2 - 4(0, 2)_4$, by (63), (64), and (70). By the lemma, as $(2|p)=1$,

$$2(0, 2)_4 \equiv \text{ind } 2 \pmod 4.$$
$$2(0, 0)_2 = 4f-2 \qquad [3, (18)].$$

By Corollary 1,

$$D(0, 4) \equiv 1+4f-2-2 \text{ ind } 2-4f \equiv 7-2 \text{ ind } 2 \pmod 8.$$

THEOREM 3. *If* $p \equiv 1 \pmod{24}$, $p = U^2+24V^2$, *then* $(6|U)=(U|p)$, $(V|p)=1$.

Proof. If q is a prime divisor of U,

$$p \equiv 24V^2 \pmod q. \quad 6p \equiv 144V^2 \pmod q.$$
$$1 = (6p|q) = (6|q)(p|q) = (6|q)(q|p),$$

by the Law of Quadratic Reciprocity. Hence

$$(6|U) = \prod_{q|U}(6|q) = \prod_{q|U}(q|p) = (U|p).$$

Now let q be an odd prime divisor of V.

$$p \equiv U^2 \pmod q. \quad (p|q) = 1 = (q|p). \prod_{q|V;\, q \text{ odd}}(q|p) = 1.$$

Since $(2|p)=1$, $(V|p)=1$.

(I am indebted to Professor Louis Sacks for suggesting the technique of this proof.)

$$\text{ind } 12 \equiv -\sum_{h=0}^{11}(h, 0)_{12}h \pmod{12} \qquad [8, \text{Theorem } 1]$$

for $e=12$, $p \equiv 1 \pmod{24}$. Apply (64), then add (65) with $h=0$:

$$\text{ind } 4+\text{ind } 3 \equiv (p-1)/12-1-\sum_{h=0}^{11}(h+1)(0, h)_{12} \pmod{12}. \tag{85}$$

If (85) is taken (mod 4), ind 4 drops out. The terms containing $(0, h)_{12}$, h odd, also drop out, for according to the lemma, they are even, and their coefficients $h+1$ are even.

$$\begin{aligned}\text{ind } 3 \equiv{}& (p-1)/12-1-(0, 0)_{12}-(0, 4)_{12}-(0, 8)_{12}+(0, 2)_{12}\\ &+(0, 6)_{12}+(0, 10)_{12} \pmod 4.\end{aligned} \tag{86}$$

Now let $e=24$. By Corollary 1,

$$D(0, 12) \equiv 1-4f+2\sum_{h=0}^{5}(0, 2h)_{12} \pmod 8. \tag{87_{24}}$$

$$D_8(0, 4) = D(0, 12)+D(8, 12)+D(16, 12), \tag{88_{24}}$$

by (61). By (80) and (68), $D(8, 12)=D(16, 12)$. Apply Corollary 2 to (88):

$$D(0, 12)+2D(8, 12) \equiv 7-2 \text{ ind } 2 \pmod 8. \tag{89_{24}}$$

Subtract (87) from (89) and divide by 2; then subtract (86):

$$(90_{24}) \qquad D(8, 12) - \text{ind } 3 \equiv -\text{ind } 2 - 2(0, 2)_{12} - 2(0, 6)_{12} - 2(0, 10)_{12} \pmod 4.$$

Since ind $2 \equiv 2 \pmod 4$ if and only if one of the three cyclotomic numbers $(0, 2)_{12}$, $(0, 6)_{12}$, or $(0, 10)_{12}$ is odd,

$$(91_{24}) \qquad D(8, 12) \equiv \text{ind } 3 \pmod 4.$$

$$U = D(0, 12) - D(8, 12) = D_8(0, 4) - 3D(8, 12),$$

by (81), (80), (68), and (88). Apply Corollary 2 and (91):

$$(92) \qquad U \equiv 3 - 3 \text{ ind } 3 \pmod 4,$$

$$-U \equiv 1 - \text{ind } 3 \pmod 4,$$

$$(93) \qquad -(-1|U) = (3|p)_4.$$

Now apply (93) to (84):

$$\begin{aligned} d &= -(-1)^f(2|p)_4(U|3) = -(-1)^f(2|p)_4(3|U)(-1|U) \\ &= (-1)^f(2|p)_4(3|U)(3|p)_4 = (-1)^f(12|U)(6|p)_4 \\ &= (-1)^f(2|U)(6|U)(6|p)_4 = (-1)^{f+(U^2-1)/8}(U|p)(6|p)_4, \end{aligned}$$

by Theorem 3,

$$\begin{aligned} &= (-1)^{f+(p-1-24V^2)/8}(6U^2|p)_4 = (-1)^{f+3f-3V^2}(6(p-24V^2)|p)_4 \\ &= (-1)^V(-144V^2|p)_4 = (-1)^V(V^2|p)_4 = (-1)^V(V|p). \end{aligned}$$

By Theorem 3,

$$(94) \qquad d = (-1)^V.$$

Equations (81) and (94) can be combined with equations (13)–(34) to give the following summary of the relations between the Jacobi sums of order 24:

$$\begin{aligned} U + 2(-6)^{1/2}V &= (-1)^f R(1, 11) = \beta^{2Z}R(1, 1) \\ &= (-1)^V\beta^{2Z}R(1, 7) = (-1)^f\beta^{6Z+3T}R(1, 5), \\ -X + 2(-1)^{1/2}Y &= R(6, 6) = \beta^{4Z-6T}R(2, 2) \\ &= (-1)^V\beta^{6Z+3T}R(2, 6) = \beta^{-6T}R(2, 10) \\ &= \beta^{6Z+3T}R(1, 6) = (-1)^f\beta^{2Z+6T}R(1, 10), \\ R(8, 8) &= \beta^{-4Z}R(4, 8) = (-1)^V\beta^{2Z+3T}R(2, 4) \\ &= R(2, 8) = (-1)^{f+V}\beta^{-2Z}R(1, 4), \\ R(1, 2) &= (-1)^{f+V}\beta^{-3T}R(1, 8) = \beta^{-3T}\sigma_7 R(1, 9) \\ &= (-1)^f\beta^{6Z-3T}\sigma_5 R(1, 3). \end{aligned}$$

Given $p = X^2 + 4Y^2 = U^2 + 24V^2$, ind 3 (mod 4) can be determined from X and Y (see Theorem 1): ind $3 \equiv 0 \pmod 4$ if and only if $3 | Y$. Then the sign of U can be determined from (92).

Now let $e=15$. $Q(\beta)$ is an eighth-degree extension of Q. Since $1+\beta^5+\beta^{10}=1+\beta^3+\beta^6+\beta^9+\beta^{12}=0$, a basis representation for $R(1, v)$ is given in Figure 4:

$$R(1, v) = \begin{bmatrix} B(0, v)+B(13, v)+B(14, v)-B(8, v)-B(9, v)-B(10, v) \\ B(1, v)+B(8, v)-B(11, v)-B(13, v) \\ B(2, v)+B(9, v)-B(12, v)-B(14, v) \\ B(3, v)+B(14, v)-B(8, v)-B(9, v) \\ B(4, v)+B(8, v)-B(13, v)-B(14, v) \\ B(5, v)+B(13, v)-B(8, v)-B(10, v) \\ B(6, v)+B(14, v)-B(9, v)-B(11, v) \\ B(7, v)+B(8, v)+B(9, v)-B(12, v)-B(13, v)-B(14, v) \end{bmatrix}$$

FIGURE 4

From (38) and (40),

$$\sigma_2[\beta^{-5F}R(1, 4)] = \beta^{-5F}R(1, 4).$$

$$\beta^{-5F}R(1, 4) = \sum_{i=0}^{14} B(i, 4)\beta^{i-5F} = \sum_{i=0}^{14} B(i+5F, 4)\beta^i,$$

$$\sigma_2[\beta^{-5F}R(1, 4)] = \sum_{i=0}^{14} B(i, 4)\beta^{2i-10F} = \sum_{i=0}^{14} B(8i+5F, 4)\beta^i.$$

Applying (62) to the $B(i, 4)$ yields

$$B(1+5j, 4) = B(4+5j, 4), B(2+5j, 4) = B(8+5j, 4), \qquad j = 0, 1, 2.$$

Define for $j=0$, 5, and 10

$$G_j = B(j+5F, 4)-\tfrac{1}{2}[B(j+12+5F, 4)+B(j+6+5F, 4)],$$
$$H_j = \tfrac{1}{2}[B(j+12+5F, 4)-B(j+6+5F, 4)].$$

By (61) and (69),

$$(95_{15}) \qquad G_0+G_5+G_{10} = B_5(0, 4)-\tfrac{1}{2}[B_5(2, 4)+B_5(1, 4)]=-1,$$

$$(96_{15}) \qquad H_0+H_5+H_{10} = B_5(2, 4)-B_5(1, 4) = 0.$$

$\beta^{-5F}R(1, 4)$ and $\sigma_2[\beta^{-5F}R(1, 4)]$ can be represented in terms of G_j and H_j, $j=0$, 5, 10, as shown in Figure 5:

$$\beta^{-5F}R(1, 4)=\begin{bmatrix} G_0+H_0-2H_5-G_{10}+H_{10} \\ 2H_5-2H_{10} \\ -2H_0+2H_5 \\ 2H_0-2H_5 \\ 2H_5-2H_{10} \\ G_5-H_5-G_{10}+H_{10} \\ 0 \\ -2H_0+2H_5 \end{bmatrix} \quad \sigma_2[\beta^{-5F}R(1, 4)]=\begin{bmatrix} G_0-H_0-G_5-H_5+2H_{10} \\ 2H_5-2H_{10} \\ 2H_0-2H_{10} \\ -2H_0+2H_{10} \\ 2H_5-2H_{10} \\ -G_5-H_5+G_{10}+H_{10} \\ 0 \\ 2H_0-2H_{10} \end{bmatrix}$$

FIGURE 5

Equate coefficients of β^5:

$$(97_{15}) \qquad G_5 = G_{10}.$$

Then by (95),

$$(98_{15}) \qquad G_0 = -1-2G_5.$$

Equate coefficients of β^2:

$$4H_0 = 2H_5+2H_{10}.$$

By (96), $6H_0=2(H_0+H_5+H_{10})=0$. Hence

$$(99_{15}) \qquad H_0 = 0, \quad H_{10} = -H_5.$$

For brevity, let $L_i=B(i+3T, 2)$.

$$\beta^{-3T}R(1, 2) = \sum_{i=0}^{14} B(i, 2)\beta^{i-3T} = \sum_{i=0}^{14} B(i+3T, 2)\beta^i = \sum_{i=0}^{14} L_i\beta^i.$$

$$\beta^{-3T}R(1, 2) = \begin{bmatrix} L_0+L_{13}+L_{14}-L_8-L_9-L_{10} \\ L_1+L_8-L_{11}-L_{13} \\ L_2+L_9-L_{12}-L_{14} \\ L_3+L_{14}-L_8-L_9 \\ L_4+L_8-L_{13}-L_{14} \\ L_5+L_{13}-L_8-L_{10} \\ L_6+L_{14}-L_9-L_{11} \\ L_7+L_8+L_9-L_{12}-L_{13}-L_{14} \end{bmatrix} \qquad \beta^{-5F}R(1, 4) = \begin{bmatrix} -1-3G_5-3H_5 \\ 4H_5 \\ 2H_5 \\ -2H_5 \\ 4H_5 \\ -2H_5 \\ 0 \\ 2H_5 \end{bmatrix}$$

FIGURE 6

Since by (40), $\beta^{-3T}R(1, 2)=b\beta^{-5F}R(1, 4)$, coefficients may be equated up to the factor b. Adding the coefficients of 1, β^3, and β^6 and subtracting the coefficients of β^2 and β^5 yields $-1-3G_5-5H_5$ and

$$L_0+L_3+L_6+L_9+L_{12}+5L_{14}-L_2-L_5-L_8-L_{11}-L_{14}-5L_9$$
$$= B_3(0, 2)-B_3(2, 2)+5(L_{14}-L_9) = 5(L_{14}-L_9)-1,$$

by (61) and (69). Hence

$$(100_{15}) \qquad -1-3G_5 \equiv -b \pmod 5.$$

$$\beta^{-5F}R(1, 4) = -1-3G_5+H_5[-3+4\beta+2\beta^2-2\beta^3+4\beta^4-2\beta^5+2\beta^7]$$
$$= -1-3G_5+H_5(-15)^{1/2}.$$

$$(101_{15}) \qquad \beta^{-5F}R(1, 4) = -M+N(-15)^{1/2}, \quad M = 1+3G_5, \quad N = H_5.$$

$p=M^2+15N^2$, by (7). Combine with (100):

$$M \equiv b \pmod 5, \; M \equiv 1 \pmod 3.$$

(102) $M \equiv 1 \pmod{15}$ implies $b = 1$, $M \equiv 4 \pmod{15}$ implies $b = -1$.

The relationships between the Jacobi sums of orders 15 and 30 will now be summarized. The notation corresponding to $e=30$ will be used. The factor$(-1)^f$ will be replaced by its equivalent β^{15T}.

$$\begin{aligned}
R(2,2) &= b\beta^{-12T-5F}R(2,10) = \beta^{-4Z}\sigma_{13}R(1,14)\\
&= \beta^{-2Z+15T}\sigma_{13}R(1,7) = \beta^{-2Z+15T}R(1,13)\\
&= \beta^{-8Z+15T}\sigma_{13}R(1,1) = \beta^{14Z+9T}\sigma_{13}R(1,3)\\
&= \beta^{-4Z-6T}\sigma_{19}R(1,8) = \beta^{-4Z+12T}R(1,2)\\
&= \beta^{-4Z+5F}\sigma_{23}R(1,4) = \beta^{-2Z-6T+5F}\sigma_{23}R(2,3),\\
R(6,6) &= \beta^{6T}R(2,6) = \beta^{-12Z+6T}R(1,6)\\
&= b\beta^{-10Z+9T+5F}R(1,9) = \beta^{-6Z+3T}R(1,11)\\
&= \beta^{-12Z+6T}\sigma_{23}R(1,12),\\
R(10,10) &= \beta^{10Z-5F}R(1,10) = b\beta^{12Z+9T+5F}R(1,5),\\
R(2,4) &= b\beta^{6T+5F}R(2,8).
\end{aligned}$$

All the Jacobi sums of order 30 can be expressed in terms of Jacobi sums of lower orders. This property holds for Jacobi sums of orders 6, 10, 14, and 18, but not 22 [3, p. 408], [4, pp. 372–373], [5, pp. 194–195].

To conclude, an application of the theory of cyclotomy of order 15 will be presented. The proof given here is a variation of Emma Lehmer's original proof of Marguerite Dunton's conjecture.

LEMMA *Let* $z\equiv g^f \pmod p$. *For a fixed* v, $1\leqq v\leqq e-1$,

$$\operatorname{ind}_g(1-z^v) \equiv (p-1)/2+\sum_{u=0}^{e-1} u(u,v)_e \pmod e.$$

Proof. Define the set $S_v=\{n \mid 2\leqq n\leqq p-1, \operatorname{ind} n\equiv v \pmod e\}$. The zeros of $x^f-z^v \pmod p$ are the elements of S_v. Thus if $\sum_v$ and $\prod_v$ denote the sum and product, respectively, over the elements of S_v,

$$x^f-z^v \equiv \prod_v (x-n) \pmod p.$$

Set $x=1$:

$$1-z^v \equiv \prod_v (1-n) \pmod p.$$

$$\begin{aligned}
\operatorname{ind}(1-z^v) &\equiv \sum_v \operatorname{ind}(1-n) \equiv f\operatorname{ind}(-1)+\sum_v \operatorname{ind}(n-1)\\
&\equiv \operatorname{ind}(-1)+\sum_{u=0}^{e-1} u(u,v)_e \equiv (p-1)/2+\sum_{u=0}^{e-1} u(u,v)_e \pmod e.
\end{aligned}$$

THEOREM 4. *Let* $p=15f+1=M^2+15N^2$ *and let* $\theta=(1+\sqrt{5})/2$. *Then* θ *is a cubic residue* (mod p) *if and only if* N *is a multiple of* 3 [7, p. 138].

Proof. Let $e=15$ and $z\equiv g^f \pmod p$.

$$(103_{15}) \qquad \theta = (1+\sqrt{5})/2 \equiv 1+z^3+z^{12} \equiv -z^6-z^9 \pmod p.$$

$$\operatorname{ind}(1-z^v) \equiv \sum_{u=0}^{14} u(u, v)_{15} \pmod{15},$$

since f is even.

$$(104_{15}) \qquad \operatorname{ind}(1-z^v) \equiv \sum_{t=0}^{4} [(3t+1, v)_{15}-(3t+2, v)_{15}] \pmod 3.$$

Adding once, then twice

$$f = \sum_{u=0}^{14} (u, v)_{15}$$

(see (66)) to (104) gives

$$(105_{15}) \qquad \operatorname{ind}(1-z^v)+f \equiv \sum_{t=0}^{4} [(3t, v)_{15}-(3t+1, v)_{15}] \pmod 3,$$

$$(106_{15}) \qquad \operatorname{ind}(1-z^v)-f \equiv \sum_{t=0}^{4} [(3t+2, v)_{15}-(3t, v)_{15}] \pmod 3.$$

By (99) and (101),

$$\begin{aligned} 4N &= 2(H_5-H_{10}) = B(2+5F, 4)-B(11+5F, 4)-B(7+5F, 4)+B(1+5F, 4) \\ &= B(2+5F, 10)-B(11+5F, 10)-B(7+5F, 10)+B(1+5F, 10), \end{aligned}$$

by (68),

$$= \sum_{h=0}^{14} [(h, 2+5F-10h)_{15}-(h, 11+5F-10h)_{15}-(h, 7+5F-10h)_{15} + (h, 1+5F-10h)_{15}],$$

by (60). In the last two terms of the above summation, replace h by $h-1$:

$$\begin{aligned} 4N &= \sum_{h=0}^{14} [(h, 2+5F-10h)_{15}-(h, 11+5F-10h)_{15}-(h-1, 2+5F-10h)_{15} \\ &\qquad + (h-1, 11+5F-10h)_{15}] \\ &= \sum_{h=0}^{14} [(h, 2+5F+5h)_{15}-(h-1, 2+5F+5h)_{15}-(h, 11+5F+5h)_{15} \\ &\qquad + (h-1, 11+5F+5h)_{15}] \\ &= \sum_{t=0}^{4} [(3t, 2+5F)_{15}-(3t+2, 2+5F)_{15}+(3t+1, 7+5F)_{15}-(3t, 7+5F)_{15} \\ &\quad + (3t+2, 12+5F)_{15}-(3t+1, 12+5F)_{15}-(3t, 11+5F)_{15}+(3t+2, 11+5F)_{15} \\ &\quad - (3t+1, 1+5F)_{15}+(3t, 1+5F)_{15}-(3t+2, 6+5F)_{15}+(3t+1, 6+5F)_{15}]. \end{aligned}$$

Replace the cyclotomic numbers by their equivalents as given in (104), (105), and (106):

$$\begin{aligned}
4N \equiv N \equiv\ & -\operatorname{ind}(1-z^{2+5F})+f-\operatorname{ind}(1-z^{7+5F})-f-\operatorname{ind}(1-z^{12+5F}) \\
& +\operatorname{ind}(1-z^{11+5F})-f+\operatorname{ind}(1-z^{1+5F})+f+\operatorname{ind}(1-z^{6+5F}) \\
\equiv\ & -\operatorname{ind}(1-z^2)-\operatorname{ind}(1-z^7)-\operatorname{ind}(1-z^{12})+\operatorname{ind}(1-z)+\operatorname{ind}(1-z^{11}) \\
& +\operatorname{ind}(1-z^6) \\
\equiv\ & -\operatorname{ind}(1+z)-\operatorname{ind}(1+z^{11})-\operatorname{ind}(1+z^6) \\
\equiv\ & -\operatorname{ind}(1+z)-\operatorname{ind}(z^4+1)-\operatorname{ind}(z^{12}+z^3)-\operatorname{ind} z^{14} \\
\equiv\ & -\operatorname{ind}(1+z+z^4+z^5)-\operatorname{ind}(z^{12}+z^3)-14\operatorname{ind} z \\
\equiv\ & -\operatorname{ind}(z+z^4-z^{10})+\operatorname{ind}(z^6+z^9)+\operatorname{ind} z \pmod 3,
\end{aligned}$$

since $1+z^5+z^{10}\equiv 0 \pmod p$ and $(z^{12}+z^3)(z^6+z^9)\equiv -1 \pmod p$.

$$\begin{aligned}
N \equiv\ & -\operatorname{ind} z^{10}-\operatorname{ind}(z^6+z^9-1)+\operatorname{ind}(z^6+z^9)+\operatorname{ind} z \\
\equiv\ & -10\operatorname{ind} z-\operatorname{ind}(-(z^6+z^9)^2)+\operatorname{ind}(z^6+z^9)+\operatorname{ind} z \\
\equiv\ & -\operatorname{ind}(-(z^6+z^9))\equiv -\operatorname{ind}\theta \pmod 3,
\end{aligned}$$

by (103).

Although the prime ideal decompositions of the Jacobi sums in $Q(\beta)$ [5, Theorem 4] were not mentioned, they were used to advantage in this study. The Jacobi sums were computed for a number of primes p. The numerical values were of considerable value in formulating and later checking the results. These computations were performed on facilities of the Computer Center of the University of Pittsburgh: the IBM 7090/1401 system, partially supported by NSF grant G11309, and the IBM 360/50 system, supported in part by NIH grant FR-00250-01A1.

Bibliography

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

2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182.

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

4. ———, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. **37** (1935), 363–380.

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

6. Emma Lehmer, *On residue difference sets*, Canad. J. Math. **5** (1953), 425–432.

7. ———, *On the quadratic character of the Fibonacci root*, Fibonacci Quart. **4** (1966), 135–138.

8. J. B. Muskat, *On the solvability of* $x^e\equiv e \pmod p$, Pacific J. Math. **14** (1964), 257–260.

9. ———, *Reciprocity and Jacobi sums*, Pacific J. Math. **20** (1967), 275–280.

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

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

12. ———, *The cyclotomic numbers of order ten*, Proc. Sympos. Appl. Math., Vol. 10, Amer. Math. Soc., Providence, R. I., 1960, pp. 95–111.

13. A. L. Whiteman and J. B. Muskat, *The cyclotomic numbers of order twenty*, Acta Arith. (to appear).

UNIVERSITY OF PITTSBURGH,
PITTSBURGH, PENNSYLVANIA