PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 28, No. 1, April 1971

THE JACOBI SUMS OF ORDER TWENTY-TWO

YUN-CHENG ZEE

ABSTRACT. This paper completes the analysis of the Jacobi sums of order 22 outlined by L. E. Dickson. Furthermore, it is shown that a prime p of the form $22f+1$ has the binary quadratic decomposition $4p=u^2+11v^2$ and that certain Jacobi sums can be evaluated in terms of u and v, where u satisfies $u\equiv 9 \pmod{11}$.

1. **Introduction.** Let p be a prime of the form $ef+1$ and g a fixed primitive root of p. Let $\beta=\exp(2\pi i/e)$. If $a\equiv g^j \pmod{p}$, write $\operatorname{ind} a=j$. The *Jacobi sum* of order e is defined by

$$R(m, n) = \sum_{a=2}^{p-1} \beta^{m \operatorname{ind} a+n \operatorname{ind}(1-a)}. \tag{1}$$

In 1935, Dickson published three papers [3], [4], [5] on cyclotomy which analyzed Jacobi sums of various orders. Further analyses were later given by Whiteman ($e=10$ [14], 12 [15], 16 [13]), Muskat ($e=15$, 24, 30 [9], 14 [8]), Baumert and Fredricksen ($e=9$, 18 [1]), and the author ($e=13$, 60 [16]). For $e=20$, see [10].

According to Dickson [4, p. 368, p. 371], $R(m, n)$ is said to be *conjugate* to $R(m', n')$ if, for some integer s prime to e, $R(m', n') = \pm\sigma_s R(m, n)$, where σ_s is the automorphism: $\beta\to\beta^s$. The Jacobi sums can thus be partitioned into conjugate classes whose representatives form a set of *reduced* Jacobi sums [3, §16]. For $e=22$ [4, p. 373], Dickson chose $R(1, k)$, $k=1$, 3, 5, 7, 11, 13, $R(2, 2)$ and $R(2, 4)$ as the reduced Jacobi sums and stated how $R(1, 1)$, $R(1, 5)$, $R(1, 11)$ and $R(1, 13)$ could be obtained linearly from $R(2, 2)$ and $R(2, 4)$ and that $R(1, 7)$ and $R(1, 3)$ could be obtained from the equations

$$R(1, 7) = (-1)^f\sigma_7 R(1, 5)\sigma_5 R(2, 4)/\sigma_{13}R(1, 5),$$
$$R(1, 3) = (-1)^f R(1, 1)R(2, 2)/\sigma_{19}R(1, 7).$$

It is the purpose of this paper to derive the linear relations between the reduced Jacobi sums of order 22 outlined by Dickson and to evaluate $R(1, 3)$ in terms of a binary quadratic decomposition of $4p$. The results are drawn in part from the author's doctoral disserta-

Received by the editors February 20, 1970.
AMS 1969 *subject classifications.* Primary 1041, 1016; Secondary 1066.
Key words and phrases. Cyclotomy, cyclotomic field, Jacobi sum, reduced Jacobi sum, conjugate, cyclotomic number, Gaussian sum, Davenport and Hasse identity, Dickson-Hurwitz sum, binary quadratic decomposition.

tion under the direction of Professor Muskat at the University of Pittsburgh.

2. **Cyclotomy.** In this section basic properties concerning the Jacobi sums are gathered for later reference.

A complete set of reduced Jacobi sums of order e may be determined by repeated applications of the following formulas [3, §16]:

$$R(m, n) = R(n, m) = (-1)^{nf}R(-m - n, n), \tag{2}$$

$$\sigma_s R(m, n) = R(sm, sn), \qquad s \text{ prime to } e. \tag{3}$$

Both can be derived from (1).

The Jacobi sum is related to the *Gaussian sum* $\tau(n) = \sum_{a=1}^{p-1} \beta^{n \text{ ind } a} \zeta^a$, where $\zeta = \exp(2\pi i/p)$, by [3, (26)]

$$R(m, n) = \tau(m)\tau(n)/\tau(m + n), \tag{4}$$

where none of m, n and $m+n$ is divisible by e.

The Gaussian sum satisfies [3, (25)]

$$\tau(n)\tau(-n) = (-1)^{nf}p \tag{5}$$

if e does not divide n, and [3, (80)]

$$\tau(t)\tau(t + e/2) = \beta^{-2tZ}\tau(2t)\tau(e/2), \qquad Z = \text{ind } 2, \tag{6}$$

if e is even. Equation (6) is a special case of an identity $[2, (0.9)_1]$ established by Davenport and Hasse.

It is immediate from (4) and (5) that if e does not divide m, n or $m+n$, then

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

The Jacobi sum is important to the determination of the *cyclotomic numbers* of order e, denoted by (h, k). For fixed h and k, (h, k) is the number of solutions t, z of

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

It is known [14, (2.6)] that

$$R(m, n) = (-1)^{mf} \sum_{h,k=0}^{e-1} (h, k)\beta^{mh+nk}.$$

If $m = nv$, $R(m, n)$ can be expanded into a finite Fourier series [14, (2.8)] by collecting the exponents of β which are congruent modulo e:

$$R(vn, n) = (-1)^{vnf} \sum_{a=0}^{e-1} B(a, v)\beta^{na}, \tag{8}$$

where $B(a, v) = \sum_{h=0}^{e-1} (h, a-vh)$. $B(a, v)$ is called a *Dickson-Hurwitz sum* of order e and satisfies [**14**, (2.12)]

$$B(a, v) = B(a, e - v - 1) \tag{9}$$

and [**14**, (2.13)]

$$\begin{aligned} B(a, 0) &= f - 1 \qquad (a = 0), \\ &= f \qquad\quad (1 \leqq a \leqq e - 1). \end{aligned} \tag{10}$$

If $xy = e$ and if $B_x(a, v)$ denotes a Dickson-Hurwitz sum of order x, then [**9**, (61)]

$$B_x(a, v) = \sum_{b=0}^{y-1} B(a + bx, v). \tag{11}$$

3. **Linear relations.** Let $e = 22$. Two special cases of (6) corresponding to $t = 1$ and 5 will be used:

$$\tau(1)\tau(12) = \beta^{-2Z}\tau(2)\tau(11), \tag{12}$$

$$\tau(5)\tau(16) = \beta^{-10Z}\tau(10)\tau(11). \tag{13}$$

Rearranging (12) and using (4), we get

$$R(1, 10) = \beta^{-2Z}R(2, 10). \tag{14}$$

By (2) and (3), $R(2, 10) = R(10, 10) = \sigma_5 R(2, 2)$, so that

$$R(1, 10) = \beta^{-2Z}\sigma_5 R(2, 2). \tag{15}$$

Applying (4) to (12) gives the equation $R(1, 1) = \beta^{-2Z}R(1, 11)$. But $R(1, 11) = (-1)^f R(1, 10)$. Hence

$$R(1, 1) = \beta^{-2Z}R(1, 11) = (-1)^f\beta^{-4Z}\sigma_5 R(2, 2). \tag{16}$$

By (5), $\tau(6)\tau(16) = (-1)^f\tau(11)\tau(11)$. From this equation and (13) we obtain $\tau(1)\tau(5)/\tau(6) = (-1)^f\beta^{-10Z}\tau(1)\tau(10)/\tau(11)$. Hence by (4) and (15),

$$R(1, 5) = (-1)^f\beta^{10Z}\sigma_5 R(2, 2). \tag{17}$$

$R(1, 4)R(1, 5) = R(1, 1)R(2, 4)$ follows from (4). Hence by (16) and (17), $R(1, 4) = \beta^{8Z}R(2, 4)$. The application of σ_{13} to the last equation yields $R(13, 8) = \beta^{-6Z}\sigma_{13}R(2, 4)$. Hence by (2),

$$R(1, 13) = (-1)^f \beta^{-6Z} \sigma_{13} R(2, 4). \tag{18}$$

We have thus found all the linear relations between the reduced Jacobi sums.

4. **Evaluation of** $R(1, 3)$. Let q be an odd prime and let $\theta = \exp(2\pi i/q)$. It was first proved by Gauss that

$$\sum_{r=0}^{q-1} \theta^r = \sqrt{q} \quad \text{if } q \equiv 1 \pmod 4,$$

$$= i\sqrt{q} \quad \text{if } q \equiv 3 \pmod 4.$$

Since then several proofs based on different methods have appeared (see [7, pp. 197–218], [6]). The following lemma is an immediate consequence of this result.

LEMMA 1. *Let* $R = \sum \theta^t$, $N = \sum \theta^s$, *where* t (*resp.* s) *runs through the quadratic residues* (*resp. nonresidues*) *modulo* q. *Then*

$$R = (-1 + \sqrt{q})/2 \quad \text{if } q \equiv 1 \pmod 4,$$

$$= (-1 + i\sqrt{q})/2 \quad \text{if } q \equiv 3 \pmod 4;$$

$$N = (-1 - \sqrt{q})/2 \quad \text{if } q \equiv 1 \pmod 4,$$

$$= (-1 - i\sqrt{q})/2 \quad \text{if } q \equiv 3 \pmod 4.$$

LEMMA 2. *For* $e = 22$, $\beta^{8Z} R(1, 3)$ *is invariant under the automorphisms* σ_k, $k = 1, 3, 5, 9, 15$.

PROOF. Combining (12) and (13), we get $\tau(2)\tau(5)\tau(16) = \beta^{-8Z}\tau(1)\tau(10)\tau(12)$. By (5), $\tau(10)\tau(12) = \tau(6)\tau(16)$, so that $\tau(2)\tau(5) = \beta^{-8Z}\tau(1)\tau(6)$. Hence

$$R(2, 5) = \beta^{-8Z} R(1, 6) = (-1)^f \beta^{-8Z} R(1, 15). \tag{19}$$

But $\sigma_9 R(2, 5) = R(18, 1) = (-1)^f R(1, 3)$, $\sigma_9 R(1, 15) = R(9, 3) = \sigma_3 R(1, 3)$. Hence applying σ_9 to (19), we obtain $\sigma_3[\beta^{8Z} R(1, 3)] = \beta^{8Z} R(1, 3)$. Since $\sigma_3^2 = \sigma_9$, $\sigma_3^3 = \sigma_5$, $\sigma_3^4 = \sigma_{15}$, the proof is complete.

Let $\mathcal{Q}$ denote the field of rational numbers. The cyclotomic field $\mathcal{Q}(\beta)$ has basis $\{1, \beta, \cdots, \beta^9\}$ with β satisfying

$$\beta^{11} + 1 = 0, \tag{20}$$

$$\sum_{k=0}^{10} (-1)^k \beta^k = 0. \tag{21}$$

According to Lemma 2, it is clear that $\beta^{8Z} R(1, 3)$ lies in a quadratic extension field over $\mathcal{Q}$.

THEOREM. *Let p be a prime of the form $22f+1$. Then*

$$R(1, 3) = (-1)^f\beta^{-8 \text{ ind } 2}(u + iv\sqrt{11})/2,$$

where u and v are rational integers satisfying

$$4p = u^2 + 11v^2, \qquad u \equiv 9 \pmod{11}.$$

PROOF. Let $\delta=(-1)^f\beta^{8Z}R(1, 3)$. By (8),

$$\delta = \beta^{8Z}\sum_{j=0}^{21} B(j, 3)\beta^j = \sum_{k=0}^{21} L_k\beta^k,$$

where $L_k=B(k-8Z, 3)$, $k=0, 1, \cdots, 21$. By means of reduction formulas (20) and (21) we obtain

$$\delta = \sum_{k=0}^{10}(L_k - L_{k+11})\beta^k = \sum_{k=0}^{9} d_k\beta^k, \tag{22}$$

where

$$d_k = (L_k - L_{k+11}) + (-1)^k(L_{21} - L_{10}), \qquad k = 0, 1, \cdots, 9. \tag{23}$$

Applying σ_3 to (22) and simplifying by means of (20) and (21), we get

$$\begin{aligned}\sigma_3\delta = {} & (d_0 + d_7) + (-d_4 - d_7)\beta + (d_8 + d_7)\beta^2 + (d_1 - d_7)\beta^3 \\ & + (-d_5 + d_7)\beta^4 + (d_9 - d_7)\beta^5 + (d_2 + d_7)\beta^6 \\ & + (-d_6 - d_7)\beta^7 + d_7\beta^8 + (d_3 - d_7)\beta^9.\end{aligned} \tag{24}$$

It follows from Lemma 2 that $\sigma_3\delta=\delta$. Hence by the uniqueness of representation with respect to the basis of $\mathbb{Q}(\beta)$ we can equate the corresponding coefficients in (22) and (24):

$$\begin{aligned}&d_0=d_0+d_7, \quad d_1=-d_4-d_7, \quad d_2=d_8+d_7, \quad d_3=d_1-d_7, \quad d_4=-d_5+d_7,\\ &d_5=d_9-d_7, \quad d_6=d_2+d_7, \quad d_7=-d_6-d_7, \quad d_8=d_7, \quad d_9=d_3-d_7.\end{aligned}$$

The ten linear equations yield

$$d_2 = d_6 = d_7 = d_8 = 0, \qquad d_1 = d_3 = -d_4 = d_5 = d_9. \tag{25}$$

Hence (22) becomes

$$\delta = d_0 + d_1(\beta + \beta^3 - \beta^4 + \beta^5 + \beta^9) = d_0 - d_1(\theta^6 + \theta^7 + \theta^2 + \theta^8 + \theta^{10}),$$

where $\theta=\beta^2=\exp(2\pi i/11)$. By Lemma 1,

$$\delta = d_0 + d_1(1 + i\sqrt{11})/2 = (u + iv\sqrt{11})/2,$$

where $u=2d_0+d_1$, $v=d_1$. By (7), $|\delta|^2=p$, so that $4p=u^2+11v^2$. It remains to show that $u\equiv9 \pmod{11}$. By (23),

$$\sum_{k=0}^{9}(-1)^k d_k = (L_0 + L_2 + \cdots + L_{20}) - (L_1 + L_3 + \cdots + L_{21}) + 11L_{21} - 11L_{10}.$$

On the other hand, by (25), $\sum_{k=0}^{9}(-1)^k d_k = d_0 - 5d_1$. Hence

$$\begin{aligned} d_0 - 5d_1 &\equiv (L_0 + L_2 + \cdots + L_{20}) - (L_1 + L_3 + \cdots + L_{21}) \\ &\equiv \sum_{k=0}^{10} B(2k - 8Z, 3) - \sum_{k=0}^{10} B(2k + 1 - 8Z, 3) \\ &\equiv B_2(0, 1) - B_2(1, 1) \pmod{11}, \end{aligned}$$

by (11). But by (9) and (10), $B_2(0, 1) = B_2(0, 0) = 11f - 1$. Similarly, $B_2(1, 1) = B_2(1, 0) = 11f$. Hence $d_0 - 5d_1 \equiv -1 \pmod{11}$. Then $u \equiv 2(d_0 - 5d_1) \equiv 9 \pmod{11}$. This completes the proof.

The solvability of $4p = u^2 + 11v^2$ can also be derived from a general theorem in quadratic forms [12, p. 273]. The representation of a prime in the form $ax^2 + by^2$, $a > 0$, $b > 0$, is known to be unique except for the signs of x and y. A proof may be found in [11, pp. 190–191]. With a slight modification of the proof it can be shown that $4p = u^2 + 11v^2$ has an essentially unique solution. In the evaluation of $R(1, 3)$ the sign of u is fixed by the congruence $u \equiv 9 \pmod{11}$, whereas that of v depends on the choice of the primitive root g [3, pp. 409–410].

References

1. L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. **21** (1967), 204–219. MR **36** #6370.

2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 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. T. Estermann, *On the sign of the Gaussian sum*, J. London Math. Soc. **20** (1945), 66–67. MR **7**, 414.

7. E. Landau, *Elementary number theory*, Teubner, Leipzig, 1927; English transl., Chelsea, New York, 1958. MR **19**, 1159.

8. J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. **11** (1966), 263–279. MR **33** #1302.

9. ———, *On Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. **134** (1968), 483–502. MR **38** #1075.

10. J. B. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. **17** (1970), 185–216.

11. T. Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York, 1964. MR **30** #4714.

12. H. J. S. Smith, *Report on the theory of numbers*, Chelsea, New York, 1965.

13. A. L. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. **86** (1957), 401–413. MR **19**, 1160.

14. ———, *The cyclotomic numbers of order ten*, Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., Providence, R.I., 1960, pp. 95–111. MR **22** #4682.

15. ———, *The cyclotomic numbers of order twelve*, Acta Arith. **6** (1960), 53–76. MR **22** #9480.

16. Y. C. Zee, *The Jacobi sums of orders thirteen and sixty and related quadratic decompositions*, Math. Z. **115** (1970), 259–272.

California State College, Fullerton, California 92631