Literaturverzeichnis

[1] P. Barrucand and H. Cohn, *A rational genus, class number divisibility and unit theory for pure cubic fields*, J. Number Theory 2 (1970), S. 7–21.

[2] — — *Remarks on principal factors in a relative cubic field*, ibid. 3 (1971), S. 226–239.

[3] T. Callahan, *The 3-class groups of non-Galois cubic fields I, II*, Mathematika 21 (1974), S. 72–89 und 168–188.

[4] A. Fröhlich, *The genus field and genus group in finite number fields*, ibid. 6 (1959), S. 40–46.

[5] G. Gras, *Sur les l-classes d'idéaux des extensions non galoisiennes de $\boldsymbol{Q}$ de degré premier impair l à cloture galoisienne diédrale de degré 2l*, J. Math. Soc. Japan 26 (1974), S. 677–685.

[6] — *Sur le 3-rang des corps cubiques non galoisiens*, erscheint demnächst.

[7] F. Halter-Koch, *Eine Bemerkung über kubische Einheiten*, Archiv d. Math. 27 (1976), S. 593–595.

[8] M. P. Lee, *Integral representations of dihedral groups of order 2p*, Trans. Amer. Math. Soc. 110 (1964), S. 213–231.

[9] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédrale d'ordre 2p*, Ann. Inst. Fourier 19 (1969), S. 1–90.

[10] M. Moriya, *Über die Klassenzahl eines relativ-zyklischen Körpers vom Primzahlgrad*, Jap. J. Math. 10 (1933), S. 1–18.

[11] N. Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de $\boldsymbol{Q}$*, Asterisque 24/25 (1975), S. 29–35.

[12] A. Scholz, *Idealklassen und Einheiten in kubischen Körpern*, Monatshefte Math. Phys. 40 (1933), S. 211–222.

[13] H. Yokoi, *On the class number of a relatively cyclic number field*, J. Math. Soc. Japan 20 (1968), S. 411–418.

Eingegangen am 30. 12. 1975
und in revidierter Form am 18. 5. 1976 (802)

ACTA ARITHMETICA
XXXIII (1977)

A rational sixteenth power reciprocity law

by

PHILIP A. LEONARD* (Tempe, Ariz.) and
KENNETH S. WILLIAMS* (Ottawa, Canada)

1. Introduction. Let p and q be distinct primes $\equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. There are integers a, b, A, B satisfying

$$\begin{aligned} p &= a^2+b^2, \qquad a-1 \equiv b \equiv 0 \pmod 2, \\ q &= A^2+B^2, \qquad A-1 \equiv B \equiv 0 \pmod 2. \end{aligned} \tag{1.1}$$

Moreover, it is well known that $\left(\frac{B}{q}\right) = (-1)^{(q-1)/4}$. If $k \not\equiv 0 \pmod q$ is a 2^l-th power modulo q, we set

$$\left(\frac{k}{q}\right)_{2^{l+1}} = \begin{cases} +1, & \text{if } k \text{ is a } 2^{l+1}\text{-th power } (\bmod q), \\ -1, & \text{otherwise.} \end{cases}$$

In 1969, Burde [1] proved the following rational biquadratic reciprocity law.

THEOREM 1.

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(q-1)/4} \left(\frac{aB-bA}{q}\right).$$

If p and q are $\equiv 1 \pmod 8$, and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, it follows from Burde's law that $\left(\frac{aB-bA}{q}\right) = 1$, and from the classical law of biquadratic reciprocity that $\left(\frac{B}{q}\right)_4 = 1$. Integers c, d, C, D exist satisfying

$$p = c^2+2d^2, \quad q = C^2+2D^2, \tag{1.2}$$

*This research was supported by National Research Council of Canada Grant A-7233.

with $\left(\frac{D}{q}\right) = 1$. Recently, one of us [7] has proved the following octic analogue of Burde's law.

THEOREM 2.

$$\left(\frac{p}{q}\right)_8\left(\frac{q}{p}\right)_8 = \left(\frac{aB-bA}{q}\right)_4\left(\frac{cD-dC}{q}\right).$$

In this paper we shall obtain a similar result for sixteenth powers. Henceforth, p and q are $\equiv 1 \pmod{16}$, and we suppose that $\left(\frac{p}{q}\right)_8 = \left(\frac{q}{p}\right)_8 = 1$. It follows from Theorem 2 that

$$\left(\frac{aB-bA}{q}\right)_4 = \left(\frac{cD-dC}{q}\right). \tag{1.3}$$

Our results involve two additional representations of p and q. There are integers e, f, E, F satisfying

$$p = e^2-2f^2, \quad q = E^2-2F^2, \tag{1.4}$$

with $\left(\frac{F}{q}\right) = 1$, and integers x, u, v, w, X, U, V, W satisfying

$$\begin{aligned} p &= x^2+2u^2+2v^2+2w^2, & 2xv &= u^2-2uw-w^2, \\ q &= X^2+2U^2+2V^2+2W^2, & 2XV &= U^2-2UW-W^2. \end{aligned} \tag{1.5}$$

The solutions of (1.4) arise from the factorizations of p and q in $Z[\sqrt{2}]$; if, for example, $q = E^2-2F^2 = E_1^2-2F_1^2$, then

$$E_1+F_1\sqrt{2} = \pm(3+2\sqrt{2})^n(E\pm F\sqrt{2})$$

for some integer n. The representation (1.5) appears in the work of Giudici, Muskat and Robinson ([3], (6.1), (6.2)), and corresponds to factoring p and q as products of reciprocal factors in $Z[\zeta+\zeta^7]$, where $\zeta = \exp(\pi i/8)$. In complete analogy with the well known system of L. E. Dickson ([2], pp. 401–405) for primes $p \equiv 1 \pmod 5$, all solutions of $p = x^2+2u^2+2v^2+2w^2$, $2xv = u^2-2uw-w^2$ are given, in terms of a fixed one (x, u, v, w), by $\pm(x, u, v, w)$, $\pm(x, -u, v, -w)$, $\pm(x, w, -v, -u)$, $\pm(x, -w, -v, u)$.

It is convenient to note that each solution (x, u, v, w) satisfies

$$(x^2-2v^2)^2 \equiv 2(u^2+2uw-w^2)^2 \pmod p,$$

so that given a, b, c, d from (1.1) and (1.2) we can distinguish the four solutions $\pm(x, \pm u, v, \pm w)$ from the four solutions $\pm(x, \pm w, -v, \mp u)$ by means of the congruence

$$bd(x^2-2v^2) \equiv ac(u^2+2uw-w^2) \pmod p. \tag{1.6}$$

In a similar way, given A, B, C, D from (1.1) and (1.2), we may distinguish (E, F) from $(E, -F)$ by means of the congruence

$$2BDF \equiv ACE \pmod q, \tag{1.7}$$

and then require (X, U, V, W) to satisfy the congruence

$$E(X^2-2V^2) \equiv 2F(U^2+2UW-W^2) \pmod q. \tag{1.8}$$

Finally, we have the congruences

$$E\big((E\mp F)W\mp FU\big)^2 \equiv (\pm EF-E^2)(\pm FX-EV)^2 \pmod q, \tag{1.9}$$

which show that $EF-E^2 \equiv G^2 \pmod q$ and $-EF-E^2 \equiv H^2 \pmod q$, for suitable choices of G and H, and $G^2H^2 \equiv E^2F^2 \pmod q$. Moreover, (1.8) guarantees that, if G and H are defined by

$$G(FX-EV) \equiv E\big((E-F)W-FU\big) \pmod q \tag{1.10}$$

and

$$H(-FX-EV) \equiv E\big((E+F)W+FU\big) \pmod q, \tag{1.11}$$

then we have $GH \equiv EF \pmod q$.

We are now in a position to state our result.

THEOREM 3. *For any choices of a, b, A, B from* (1.1), *c, d, C, D from* (1.2), *(x, u, v, w) from* (1.5) *subject to* (1.6), *(E, F) from* (1.4) *subject to* (1.7), *and any G, H satisfying*

$$G^2 \equiv EF-E^2, \quad H^2 \equiv -EF-E^2, \quad GH \equiv EF \pmod q, \tag{1.12}$$

we have

(1.13)

$$\left(\frac{p}{q}\right)_{16}\left(\frac{q}{p}\right)_{16} = \left(\frac{B}{q}\right)_8\left(\frac{D}{q}\right)_4\left(\frac{(aB-bA)(cD-dC)^2}{q}\right)_8\left(\frac{Fx-Ev+Gw+Hu}{q}\right).$$

It will be shown that the sixteenth power reciprocity law (1.13) is independent of the choices of solutions, subject to the conditions given. We note that, if $\left(\frac{cD-dC}{q}\right) = 1$, then in (1.13) we can replace $\left(\frac{(aB-bA)(cD-dC)^2}{q}\right)_8$ by $\left(\frac{aB-bA}{q}\right)_8\left(\frac{cD-dC}{q}\right)_4$. Moreover in this case the restrictions governing the choices of (E, F) and (x, u, v, w) are not necessary, as will be apparent in the course of the proof.

Finally, we observe that if (X, U, V, W) satisfies (1.8) and G, H are defined by (1.10) and (1.11), we have

$$\left(\frac{Fx-Ev+Gw+Hu}{q}\right)=\left(\frac{(E-F)W-FU}{q}\right)\times \left(\frac{\big((E-F)W-FU\big)(Fx-Ev)-\big((E-F)w-Fu\big)(FX-EV)}{q}\right), \tag{1.14}$$

so that Theorem 3 can be given entirely in "rational" form, that is, with no need of solving any congruences in order to apply the law.

The proof of Theorem 3 is similar to (but more complicated than) the proof of the rational octic reciprocity law given in [7]. It depends on properties of Gauss and Jacobi sums, which we introduce in § 4. After some technical lemmas in § 2, we establish in § 3 that our law is independent of the choice of solutions to (1.1), (1.2), (1.4), (1.5) subject to the restrictions (1.6) and (1.7), and thereafter we work with a particular choice. The proof of Theorem 3 is presented in § 6.

2. Technical lemmas. Let $\zeta=\exp(\pi i/8)$, let π be a prime factor of p in $Z[\zeta]$, let σ_i, $i=1,3,5,7,9,11,13,15$, denote the automorphism of $Z[\zeta]$ determined by $\sigma_i(\zeta)=\zeta^i$, and let $\sigma_i(\pi)=\pi_i$, so that $p=\pi_1\pi_3\dots\pi_{15}$. The elements of $Z[\zeta]$ fixed by σ_5 and σ_9 make up $Z[i]$ hose fixed by σ_3 and σ_9 make up $Z[\sqrt{-2}]$, those fixed by σ_7 comprise $Z[\zeta+\zeta^7]$, and those fixed by σ_7 and σ_9 give $Z[\sqrt{2}]$. Thus, for example, $\pi_1\pi_5\pi_9\pi_{13}$ is in $Z[i]$. Replacing π by $\zeta\pi$ if necessary, we may assume $\pi_1\pi_5\pi_9\pi_{13}\equiv 1\pmod 2$. We define $a, b, c, d, e, f, x, u, v, w$ by setting

$$\begin{aligned} a+bi &= \pi_1\pi_5\pi_9\pi_{13}, \qquad a-1\equiv b\equiv 0\pmod 2,\\ c+d\sqrt{-2} &= \pi_1\pi_3\pi_9\pi_{11},\\ e+f\sqrt{2} &= \pi_1\pi_7\pi_9\pi_{15},\\ x+u(\zeta+\zeta^7)+v\sqrt{2}+w(\zeta^3+\zeta^5) &= \pi_1\pi_7\pi_{11}\pi_{13}. \end{aligned} \tag{2.1}$$

The first lemma establishes that these values satisfy (1.6).

LEMMA 1. *If $a, b, c, d, e, f, x, u, v, w$ are specified by* (2.1), *then*

$$bd(x^2-2v^2)\equiv ac(u^2+2uw-w^2)\pmod p.$$

Proof. We have $\pi_3\pi_{11}+\pi_7\pi_{15}=r+si$, where $r, s\in Z$. From (2.1) we obtain

$$\begin{aligned}(a+bi)(r+si)^2 &= (c+d\sqrt{-2})(e-f\sqrt{2})+(c-d\sqrt{-2})(e+f\sqrt{2})+2p\\ &= 2\{(ce+p)-2dfi\},\end{aligned}$$

giving

$$2(ce+p)=a(r^2-s^2)-2brs, \qquad -4df=2ars+b(r^2-s^2). \tag{2.2}$$

Solving the equations in (2.2) for r^2-s^2, and reducing modulo p, we obtain

$$ace\equiv 2bdf\pmod p. \tag{2.3}$$

In addition, we have $\pi_3\pi_5+\pi_{11}\pi_{13}=l+m\sqrt{2}$, where $l, m\in Z$. From (2.1) we obtain, with $\alpha=\pi_1\pi_7\pi_{11}\pi_{13}$,

$$\begin{aligned}(e+f\sqrt{2})(l+m\sqrt{2})^2 &= \alpha\cdot\sigma_{11}(\alpha)+\sigma_3(\alpha)\cdot\sigma_9(\alpha)+2p\\ &= 2\big((x^2-2v^2+p)+(u^2+2uw-w^2)\sqrt{2}\big),\end{aligned}$$

giving

$$\begin{aligned}2(x^2-2v^2+p) &= e(l^2+2m^2)+4flm,\\ 2(u^2+2uw-w^2) &= 2elm+f(l^2+2m^2).\end{aligned} \tag{2.4}$$

Solving the equations in (2.4) for l^2+2m^2, and reducing modulo p, we obtain

$$(x^2-2v^2)e\equiv 2(u^2+2uw-w^2)f\pmod p. \tag{2.5}$$

The lemma now follows on eleminating e and f from (2.3) and (2.5).

LEMMA 2. *For c, d, e and f given by* (2.1) *and any pairs (C, D) from* (1.2) *and (E, F) from* (1.4), *we have*

$$\left(\frac{cD-dC}{q}\right)=\left(\frac{eF-fE}{q}\right).$$

Proof. Let (A, B) be a solution from (1.1). Using $A^2\equiv -B^2\pmod q$ in (2.2), we obtain

$$2B^2\{(ce+p)B-2dfA\}\equiv(aB+bA)(rB+sA)^2\pmod q.$$

Since $\left(\frac{aB+bA}{q}\right)=\left(\frac{aB-bA}{q}\right)=1$, this implies that $(ce+p)B-2dfA$ is a square modulo q. The result now follows from the congruences

$$\begin{aligned}2D(cD-dC)(c+z) &\equiv \big((c+z)D-dC\big)^2\pmod q,\\ 2F(eF-fE)(e+z) &\equiv \big((e+z)F-fE\big)^2\pmod q,\\ 2B(c+z)(e+z)\big((ce+p)B-2dfA\big) &\equiv \big(B(c+z)(e+z)-2dfA\big)^2\pmod q,\end{aligned}$$

where z satisfies $z^2\equiv p\pmod q$.

LEMMA 3. *For any choice of c, d, C, D from* (1.2), *any choice of (x, u, v, w) from* (1.5), *and any z satisfying $z^2\equiv p\pmod q$, we have*

$$\left(\frac{cD-dC}{q}\right)=\left(\frac{x^2-2v^2+p+2xz}{q}\right).$$

Proof. Suppose c, d, e, f, x, u, v, w are given by (2.1), and let (E, F) be a solution from (1.4). Using $E^2\equiv 2F^2\pmod q$ in (2.4) we obtain

$$2F^2\big(F(x^2-2v^2+p)-E(u^2+2uw-w^2)\big)\equiv(eF-fE)(lF-mE)^2\pmod q.$$

With $z^2 \equiv p \pmod q$, we have the congruence

$$2F\big(F(x^2-2v^2+p)-E(u^2+2uw-w^2)\big)(x^2-2v^2+p+2xz)$$
$$\equiv \{F(x^2-2v^2+p+2xz)-E(u^2+2uw-w^2)\}^2 \pmod q.$$

The assertion follows, for c, d, x, u, v, w given by (2.1), and any C, D from (1.2), from Lemma 2 and the above congruences. As $(cD-dC)\times$ $\times(cD+dC) \equiv D^2p \pmod q$, the left hand side of the assertion is independent of the choice of (c, d), and as

$$(x^2-2v^2+p)^2-4px^2 = 2(u^2+2uw-w^2)^2,$$

the right hand side is independent of the choices of (x, u, v, w) and of z.

Lemma 4. *For (x, u, v, w) from (1.5), (E, F) from (1.4), G, H satisfying (1.12), and any z satisfying $z^2 \equiv p \pmod q$, we have*

$$\left(\frac{Fx-Ev+Gw+Hu}{q}\right) = \left(\frac{Fx-Ev+Fz}{q}\right).$$

Proof. The result follows immediately from the congruence

$$2(Fx-Ev+Fz)(Fx-Ev+Gw+Hu) \equiv (Fx-Ev+Gw+Hu+Fz)^2 \pmod q.$$

3. Independence of choice of solutions. In this section we show that the symbols appearing in Theorem 3 are independent of the choices of solutions to (1.1), (1.2), (1.4) and (1.5), subject to (1.6) and (1.7). Here all congruences are taken modulo q.

First, we note the two congruences

$$(aB-bA)(aB+bA) \equiv B^2p \quad \text{and} \quad (cD-dC)(cD+dC) \equiv D^2p.$$

When $\left(\frac{cD-dC}{q}\right) = 1$, these give

$$\left(\frac{aB-bA}{q}\right)_8 = \left(\frac{aB+bA}{q}\right)_8 \quad \text{and} \quad \left(\frac{cD-dC}{q}\right)_4 = \left(\frac{cD+dC}{q}\right)_4,$$

so that in this case $\left(\frac{(aB-bA)(cD-dC)^2}{q}\right)_8$ is invariant under all changes of solutions in (1.1) and (1.2). When $\left(\frac{cD-dC}{q}\right) = -1$, they imply that the expression $\frac{BD}{AC}\left(\frac{(aB-bA)(cD-dC)^2}{q}\right)_8$ is invariant under all changes of solutions in (1.1) and (1.2). Also the symbol $\left(\frac{Fx-Ev+Gw+Hu}{q}\right)$ is invariant under $(G, H)\to(-G, -H)$ as $(Fx-Ev)^2-(Gw+Hu)^2 \equiv F^2p$.

Next, appealing to Lemma 4, we check that

$$\left(\frac{Fx-Ev+Fz}{q}\right), \quad \text{if} \quad \left(\frac{cD-dC}{q}\right) = +1,$$

and

$$\frac{F}{E}\left(\frac{Fx-Ev+Fz}{q}\right), \quad \text{if} \quad \left(\frac{cD-dC}{q}\right) = -1,$$

are invariant under $(E, F)\to(3E+4F, 2E+3F)$, and $(E, F)\to(3E-4F, -2E+3F)$. The invariance under the first of these transformations follows from the congruences

$$F^2(Fx-Ev-Fz)\big((2E+3F)x-(3E+4F)v+(2E+3F)z\big)$$
$$\equiv \big((2E+3F)Gu+FHw\big)^2,$$

and $\frac{2E+3F}{3E+4F} \equiv \frac{F}{E}$, and the second from the congruences

$$F^2(Fx-Ev-Fz)\big(-(2E+3F)x-(3E-4F)v+(-2E+3F)z\big)$$
$$\equiv \big(-(2E+3F)Hw+FGu\big)^2,$$

and $\frac{-2E+3F}{3E-4F} \equiv \frac{F}{E}$, since

$$(Fx-Ev+Fz)(Fx-Ev-Fz) \equiv (Hu+Gw)^2. \tag{3.1}$$

Moreover (3.1) shows that $\left(\frac{Fx-Ev+Fz}{q}\right)$ is invariant under (x, u, v, w) $\to\pm(x, \pm u, v, \pm w)$ and $z\to -z$. Further it is clear from the congruence

$$(Fx-Ev+Fz)(Fx+Ev+Fz) \equiv F^2(x^2-2v^2+p+2xz) \tag{3.2}$$

and Lemma 3 that the condition (1.6) is necessary precisely when $\left(\frac{cD-dC}{q}\right) = -1$.

This completes the proof that the symbols

$$\left(\frac{Fx-Ev+Gw+Hu}{q}\right), \quad \text{if} \quad \left(\frac{cD-dC}{q}\right) = +1,$$

and

$$\frac{F}{E}\left(\frac{Fx-Ev+Gw+Hu}{q}\right), \quad \text{if} \quad \left(\frac{cD-dC}{q}\right) = -1,$$

are independent of the choices of solutions from (1.1), (1.2), (1.4), (1.5), (1.12), subject to the restrictions (1.6) and (1.7). Henceforth we assume that $a, b, c, d, e, f, x, u, v, w$ are given by (2.1).

4. Gauss and Jacobi sums. With π as defined in §2, we define the symbol $\left(\frac{x}{\pi}\right)_{16}$ for rational integers x by setting

$$\left(\frac{x}{\pi}\right)_{16} = \begin{cases} \zeta^k, & \text{if } x \not\equiv 0 \pmod{p} \text{ and } x^{(p-1)/16} \equiv \zeta^k \pmod{\pi},\ 0 \leqslant k \leqslant 15, \\ 0, & \text{if } x \equiv 0 \pmod{p}. \end{cases}$$

For rational integers k and l, the Gauss and Jacobi sums are defined by

$$G(k) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_{16}^k \exp\left(\frac{2\pi i x}{p}\right) \quad \text{and} \quad J(k,l) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_{16}^k \left(\frac{1-x}{\pi}\right)_{16}^l.$$

The following properties of these sums will be used:

$$J(k,l) = \frac{G(k)G(l)}{G(k+l)}, \quad \text{for} \quad k, l, k+l \not\equiv 0 \pmod{16}, \tag{4.1}$$

$$G(8) = p^{1/2}, \tag{4.2}$$

$$G(k)G(-k) = (-1)^{\frac{p-1}{16}\cdot k} p, \quad \text{for} \quad k \not\equiv 0 \pmod{16}, \tag{4.3}$$

$$J(k,l)\overline{J(k,l)} = p, \quad \text{for} \quad k, l, k+l \not\equiv 0 \pmod{16}, \tag{4.4}$$

$$J(k,l) = (-1)^{\frac{p-1}{16}\cdot k} J\big(k, -(k+l)\big), \quad \text{for} \quad k, l, k+l \not\equiv 0 \pmod{16}, \tag{4.5}$$

$$J(4,4) \equiv 1 \pmod{2}, \tag{4.6}$$

$$G(8)G(2k) = \zeta^{2km} G(k)G(8+k), \quad m \text{ even}. \tag{4.7}$$

(For (4.1)–(4.6), see [5]; for (4.7), Jacobi's Theorem, see [4], eqn. (8), p. 442.)

From (4.1), we have

$$\{J(1,1)\}^8 \{J(2,2)\}^4 \{J(4,4)\}^2 = \frac{\{G(1)\}^{16}}{\{G(8)\}^2},$$

which (using (4.2)) gives

$$\{G(1)\}^{16} = p\{J(1,1)\}^8 \{J(2,2)\}^4 \{J(4,4)\}^2. \tag{4.8}$$

We relate the Jacobi sums in (4.8) to the quantities specified in (2.1), by means of Stickelberger's determination (see for example [6]) of the prime decomposition of Jacobi sums.

As $\left(\frac{x}{\pi}\right)_{16}^4 = 0, \pm 1$ or $\pm i$, $J(4,4)$ lies in $Z[i]$, and by Stickelberger's Theorem, $J(4,4) \sim \pi_1\pi_5\pi_9\pi_{13}$ in $Z[i]$. Therefore, $J(4,4) = u\pi_1\pi_5\pi_9\pi_{13}$ where $u = \pm 1, \pm i$. But $J(4,4) \equiv \pi_1\pi_5\pi_9\pi_{13} \equiv 1 \pmod{2}$ (using (2.1) and (4.6)), so that $u = \pm 1$, and we have

$$\{J(4,4)\}^2 = (\pi_1\pi_5\pi_9\pi_{13})^2 = (a+bi)^2. \tag{4.9}$$

Now, by (4.1) (with $k = 2$, $l = 2, 8$) and (4.7) (with $k = 2$) we have $J(2,2) = \zeta^{-4m} J(2,8)$. By Stickelberger's Theorem, $J(2,8) \sim \pi_1\pi_3\pi_9\pi_{11}$, and as

$$\sigma_3\big(J(2,8)\big) = J(6,8) = \frac{G(6)G(8)}{G(14)} = \frac{G(2)G(8)}{G(10)} = J(2,8),$$

$J(2,8)$ lies in $Z[\sqrt{-2}]$. Thus $J(2,2) = \pm\zeta^{-4m}\pi_1\pi_3\pi_9\pi_{11}$, and we have

$$\{J(2,2)\}^4 = (\pi_1\pi_3\pi_9\pi_{11})^4 = \tfrac{1}{4}(c+d\sqrt{-2})^4. \tag{4.10}$$

Finally, using (4.7) with $k = 7$, and the other properties of these sums, we have

$$\begin{aligned} \sigma_7\big(J(1,1)\big) = J(7,7) &= \frac{\{G(7)\}^2}{G(14)} \cdot \frac{\{G(15)\}^2}{\{G(15)\}^2} = \frac{p\{G(14)\}^2}{\zeta^{12m} G(14)\{G(15)\}^2} \\ &= \zeta^{4m}(-1)^{(p-1)/16} G(1)G(15)\cdot G(14)/\{G(15)\}^2 \\ &= \zeta^{4m}(-1)^{(p-1)/16} J(1,14) = \zeta^{4m} J(1,1) = \pm J(1,1) \end{aligned}$$

as m is even. Thus $\{J(1,1)\}^2 \in Z[\zeta+\zeta^7]$. As $\pi_1\pi_7\pi_{11}\pi_{13} \in Z[\zeta+\zeta^7]$, and $J(1,1) \sim \pi_1\pi_7\pi_{11}\pi_{13}$ by Stickelberger's Theorem, we have $\{J(1,1)\}^2 = u(\pi_1\pi_7\pi_{11}\pi_{13})^2$, where u is a unit of $Z[\zeta+\zeta^7]$. By (4.4), $u\bar{u} = 1$, so that $u = \pm 1$, and we have

$$J(1,1)^8 = (\pi_1\pi_7\pi_{11}\pi_{13})^8 = \{x + u(\zeta+\zeta^7) + v\sqrt{2} + w(\zeta^3+\zeta^5)\}^8. \tag{4.11}$$

Raising (4.8) to the power $(q-1)/16$, and using (4.8)–(4.11), we have the following result.

LEMMA 5.

$$G(1)^{q-1} = p^{(q-1)/16}(a+bi)^{(q-1)/8}(c+d\sqrt{-2})^{(q-1)/4}\big(x + u(\zeta+\zeta^7) + v\sqrt{2} + w(\zeta^3+\zeta^5)\big)^{(q-1)/2}.$$

5. Evaluations modulo q. In this section, we determine the residues $(\mathrm{mod}\, q)$ of the expressions appearing in Lemma 5.

First, $B(a+bi) \equiv aB - bA \pmod{A+Bi}$ and $B(a+bi) \equiv aB + bA \pmod{A-Bi}$. Moreover, $(aB-bA)(aB+bA) \equiv pB^2 \pmod{q}$ implies $(aB+bA)^{(q-1)/8} \equiv (aB-bA)^{3(q-1)/8} \pmod{q}$. Using these facts together with (1.3), we obtain

$$(a+bi)^{(q-1)/8} \equiv \left(\frac{B}{q}\right)_8 (aB-bA)^{(q-1)/8} \pmod{A+Bi}, \tag{5.1}$$

and

$$(a+bi)^{(q-1)/8} \equiv \left(\frac{cD-dC}{q}\right)\left(\frac{B}{q}\right)_8 (aB-bA)^{(q-1)/8} \pmod{A-Bi}. \tag{5.2}$$

Combining (5.1) and (5.2), we have (mod q)

$$(5.3)\quad (a+bi)^{(q-1)/8} \equiv \begin{cases} \left(\frac{B}{q}\right)_8 \left(\frac{aB-bA}{q}\right)_8, & \text{if } \left(\frac{cD-dC}{q}\right)=1, \\ -\frac{Bi}{A}\left(\frac{B}{q}\right)_8 (aB-bA)^{(q-1)/8}, & \text{if } \left(\frac{cD-dC}{q}\right)=-1. \end{cases}$$

Next, $D(c+d\sqrt{-2}) \equiv cD-dC \pmod{C+D\sqrt{-2}}$ and $D(c+d\sqrt{-2}) \equiv cD+dC \pmod{C-D\sqrt{-2}}$. Moreover, $(cD-dC)(cD+dC) \equiv pD^2 \pmod q$ implies $(cD+dC)^{(q-1)/4} \equiv (cD-dC)^{3(q-1)/4} \pmod q$. Thus, we have

$$(5.4)\quad (c+d\sqrt{-2})^{(q-1)/4} \equiv \left(\frac{D}{q}\right)_4 (cD-dC)^{(q-1)/4} \pmod{C+D\sqrt{-2}},$$

and

$$(5.5)\quad (c+d\sqrt{-2})^{(q-1)/4} \equiv \left(\frac{cD-dC}{q}\right)\left(\frac{D}{q}\right)_4 (cD-dC)^{(q-1)/4} \pmod{C-D\sqrt{-2}}.$$

Combining (5.4) and (5.5) we have (mod q)

$$(5.6)\quad (c+d\sqrt{-2})^{(q-1)/4} \equiv \begin{cases} \left(\frac{D}{q}\right)_4 \left(\frac{cD-dC}{q}\right)_4, & \text{if } \left(\frac{cD-dC}{q}\right)=1, \\ -\frac{D\sqrt{-2}}{C}\left(\frac{D}{q}\right)_4 (cD-dC)^{(q-1)/4}, & \text{if } \left(\frac{cD-dC}{q}\right)=-1. \end{cases}$$

Finally, we observe that

$$2F(Fx-Ev+Fz)\left(x+u(\zeta+\zeta^7)+v\sqrt{2}+w(\zeta^3+\zeta^5)\right) \equiv \left\{(Fx-Ev+Fz)+\left(Fu-(E-F)w\right)(\zeta+\zeta^7)\right\}^2 \pmod{E+F\sqrt{2}}$$

from which we have

$$(5.7)\quad \{x+u(\zeta+\zeta^7)+v\sqrt{2}+w(\zeta^3+\zeta^5)\}^{(q-1)/2} \equiv \left(\frac{Fx-Ev+Fz}{q}\right) \pmod{E+F\sqrt{2}}.$$

In a similar manner we obtain

$$(5.8)\quad \{x+u(\zeta+\zeta^7)+v\sqrt{2}+w(\zeta^3+\zeta^5)\}^{(q-1)/2} \equiv \left(\frac{Fx+Ev+Fz}{q}\right) \pmod{E-F\sqrt{2}}.$$

Combining (5.7) and (5.8) using Lemma 3 and (3.2), we have (mod q)

$$(5.9)\quad \{x+u(\zeta+\zeta^7)+v\sqrt{2}+w(\zeta^3+\zeta^5)\}^{(q-1)/2} \equiv \begin{cases} \left(\frac{Fx-Ev+Fz}{q}\right), & \text{if } \left(\frac{cD-dC}{q}\right)=1, \\ -\frac{F\sqrt{2}}{E}\left(\frac{Fx-Ev+Fz}{q}\right), & \text{if } \left(\frac{cD-dC}{q}\right)=-1. \end{cases}$$

6. Proof of Theorem 3. As has already been noted, we may prove Theorem 3 for the values of $a, b, c, d, e, f, x, u, v, w$ given in (2.1). We have

$$\{G(1)\}^q = \left\{\sum_{x=0}^{p-1}\left(\frac{x}{\pi}\right)_{16} \exp\left(\frac{2\pi i x}{p}\right)\right\}^q,$$

so that, working modulo q, we obtain

$$\{G(1)\}^q \equiv \sum_{x=0}^{p-1}\left(\frac{x}{\pi}\right)_{16}^q \exp\left(\frac{2\pi i q x}{p}\right) \equiv \left(\frac{q}{\pi}\right)_{16}^{-1} \sum_{y=0}^{p-1}\left(\frac{y}{\pi}\right)_{16} \exp\left(\frac{2\pi i y}{p}\right) \equiv \left(\frac{q}{\pi}\right)_{16}^{-1} G(1),$$

where we have set $qx \equiv y \pmod p$.

Thus we have $\left(\frac{q}{\pi}\right)_{16}\{G(1)\}^q \equiv G(1) \pmod q$, and as $p \neq q$ and q is a rational integer, this implies

$$\left(\frac{q}{p}\right)_{16}\{G(1)\}^{q-1} \equiv 1 \pmod q.$$

Since $p^{(q-1)/16} \equiv \left(\frac{p}{q}\right)_{16} \pmod q$, this congruence and Lemma 5 imply that we have (mod q)

$$(6.1)\quad \left(\frac{p}{q}\right)_{16}\left(\frac{q}{p}\right)_{16} \equiv (a+bi)^{(q-1)/8}(c+d\sqrt{-2})^{(q-1)/4}\left(x+u(\zeta+\zeta^7)+v\sqrt{2}+w(\zeta^3+\zeta^5)\right)^{(q-1)/2}.$$

Theorem 3 now follows from (1.7), (5.3), (5.6), (5.9), (6.1) and Lemma 4.

7. Numerical examples. We illustrate our results with some numerical examples.

EXAMPLE 1. $p = 113$, $q = 97$.

We choose any solutions to $113 = a^2+b^2 = c^2+2d^2$ with a odd, say $(a, b) = (7, 8)$, $(c, d) = (9, 4)$. To satisfy (1.6), we take $(x, u, v, w) = (1, 6, 4, 2)$ in (1.5). For $q = 97$, we take $(A, B) = (9, 4)$, $(C, D) = (5, 6)$, and satisfy (1.7) by choosing $(E, F) = (13, -6)$. Then $(G, H) = (74, -43)$ satisfies (1.12). Evaluating the symbols in (1.13) we have

$$\left(\frac{B}{q}\right)_8 = -1, \quad \left(\frac{D}{q}\right)_4 = +1, \quad \left(\frac{(aB-bA)(cD-dC)^2}{q}\right)_8 = +1,$$

$$\left(\frac{Fx-Ev+Gw+Hu}{q}\right) = -1,$$

and

$$\left(\frac{p}{q}\right)_{16} = \left(\frac{q}{p}\right)_{16} = -1,$$

verifying Theorem 3 in this case. We note that $\left(\frac{cD-dC}{q}\right) = -1$ in this example.

EXAMPLE 2. $p = 433$, $q = 449$.

We begin with $(a, b) = (17, 12)$, $(A, B) = (7, 20)$ from (1.1) and $(c, d) = (19, 6)$, $(C, D) = (21, 2)$ from (1.2). In this case we have $\left(\frac{cD-dC}{q}\right) = +1$. We choose $(E, F) = (29, 14)$, so that (1.7) is satisfied. The solutions $(x, u, v, w) = (1, 2, -14, 4)$ and $(X, U, V, W) = (9, 12, -2, 6)$ for (1.5) are such that (1.6) and (1.8) are satisfied as well. Using the "rational" form (1.14) of Theorem 3, we have

$$\left(\frac{p}{q}\right)_{16} = \left(\frac{433}{449}\right)_{16} = -1, \quad \left(\frac{q}{p}\right)_{16} = \left(\frac{449}{433}\right)_{16} = -1,$$

$$\left(\frac{B}{q}\right)_8 = -1, \left(\frac{D}{q}\right)_4 = -1, \left(\frac{aB-bA}{q}\right)_8 = +1, \left(\frac{cD-dC}{q}\right)_4 = -1,$$

$$\left(\frac{(E-F)W-FU}{q}\right) = +1,$$

$$\left(\frac{((E-F)W-FU)(Fx-Ev)-((E-F)w-Fu)(FX-EV)}{q}\right)$$

$$= \left(\frac{415}{449}\right) = -1,$$

verifying this form of Theorem 3 for $p = 433$ and $q = 449$.

References

[1] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), pp. 175–184.

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

[3] R. E. Giudici, J. B. Muskat and S. F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc. 171 (1972), pp. 317–347.

[4] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin, Göttingen, Heidelberg 1950.

[5] K. Ireland and M. I. Rosen, *Elements of number theory*, Bogden and Quigley, Tarrytown-on-Hudson, New York 1972.

[6] A. Weil, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. 73 (1952), pp. 487–495.

[7] K. S. Williams, *A rational octic reciprocity law*, Pacific J. Math. 63 (1976), pp. 563–570.

ARIZONA STATE UNIVERSITY
Tempe, Arizona, U. S. A.
CARLETON UNIVERSITY
Ottawa, Ontario, Canada

Received on 24. 1. 1976 (808)