QUINTIC RECIPROCITY

CHARLES HELOU

(Communicated by William W. Adams)

ABSTRACT. An expression for the rational inversion factor of the power residue symbol, of odd prime exponent $n \equiv 1 \pmod{4}$, is given. It is applied to the quintic case, where the resulting expression involves only a rational quadratic form representation of primes and the power residue character of Jacobi sums. A reciprocity relation for Jacobi sums is then deduced, for $n = 5$, and conjectured to hold for all odd prime exponents n .

1. INTRODUCTION

Let n be an odd prime number, ζ a primitive n th root of unity in the field $\mathbb{C}$ of complex numbers, $K = \mathbb{Q}(\zeta)$, and $A = \mathbb{Z}[\zeta]$ the ring of integers of K . For any two elements α, β in A , prime to n and to each other, (α/β) denotes the usual n th power residue symbol over K (e.g., [3]) and $e(\alpha, \beta) = (\alpha/\beta)(\beta/\alpha)^{-1}$ is the "inversion factor".

Let p and q be two prime numbers $\equiv 1 \pmod{n}$, and suppose that they are norms in $K/\mathbb{Q}$ of some prime elements π and ω of A , respectively. The n th power rational inversion factor for p, q is $\rho(p, q) = (p/\omega)(q/\pi)^{-1}$. An expression for $\rho(p, q)$, valid for any natural number n , was given in [2] and applied to the cases $n = 3, 4, 8$. In this paper, a formula is derived for n prime $\equiv 1 \pmod{4}$ (a slightly more complicated one is valid for $n \equiv 3 \pmod{4}$). It is then applied to the case $n = 5$, where we obtain an expression involving only power residue characters of rational integers and Jacobi sums. We note that criteria for the quintic character of some rational integers have been obtained [4, 6] along different lines, using the period equation.

2. AN EXPRESSION FOR THE RATIONAL INVERSION FACTOR

It follows from the Proposition in [2] that, if $\omega = f(\zeta)$, with f a polynomial over $\mathbb{Z}$, and z, m are rational integers satisfying

$$(1) \quad z \equiv \zeta \pmod{\pi}, \quad m \equiv \prod_{k=1}^{n-1} f(z^k)^{k'-1} \pmod{p},$$

where k, k' are positive integers such that $kk' \equiv 1 \pmod{n}$, then

$$\rho(p, q) = e(p, \omega)(m/\pi).$$

Received by the editors June 3, 1991.

1991 *Mathematics Subject Classification.* Primary 11R04, 11A15; Secondary 11L10.

© 1993 American Mathematical Society
 0002-9939/93 \$1.00 + \$.25 per page

Let λ denote the particular prime $\zeta - 1$ of A dividing n . An element α of A , prime to λ , is called primary if, for some a in $\mathbb{Z}$, $\alpha \equiv a \pmod{\lambda^2}$. Since $A = \mathbb{Z}[\lambda]$ and, for any j in $\mathbb{Z}$, $\zeta^j \equiv 1 + j\lambda \pmod{\lambda^2}$, there is a unique j between 0 and $n - 1$ such that $\zeta^j \omega$ is primary. We may thus choose ω to be primary. It then follows from Eisenstein's reciprocity law [1] that $e(p, \omega) = 1$. Hence

Theorem 1. *If ω is a primary prime in A of norm q and π is any prime in A of norm p , then $\rho(p, q) = (m/\pi)$ where m is given by (1).*

The Galois group G of $K/\mathbb{Q}$ consists of the automorphisms σ_k of K such that $\sigma_k(\zeta) = \zeta^k$, corresponding to $k \pmod{n}$, where k is in $\mathbb{Z}$, prime to n . Let r be a primitive root of the prime n . The elements of G are then the σ_{r^j} , for j integer between 1 and $n - 1$; it will be convenient to write $\sigma_{r^{-j}}$ for the inverse of σ_{r^j} in G . For every positive divisor d of $n - 1$, let K_d be the unique subfield of K of degree d over $\mathbb{Q}$; this is the fixed field of σ_{r^d} , generated over $\mathbb{Q}$ by any one of the "Gaussian periods" of order d [5]. Of particular interest are the quadratic subfield $K_2 = \mathbb{Q}(\sqrt{n^*})$, where $n^* = n$ or $-n$ according as $n \equiv 1$ or $-1 \pmod{4}$, and the maximal real subfield $K_+ = \mathbb{Q}(\zeta + \zeta^{-1})$ of K which corresponds to $d = (n - 1)/2$. Indeed, the norm of π over K_2 can be written $(a + b\sqrt{n^*})/2$, with a, b in $\mathbb{Z}$, which, upon taking its norm over $\mathbb{Q}$, yields the representation $4p = a^2 - n^*b^2$. As to the norm over K_+ of an α in A , it is the real algebraic integer $|\alpha|^2$.

To determine (α/π) , α has to be known to within an n th power factor modulo π . So, for α, β in A , prime to π , we write

$$\alpha \equiv \beta \pmod{\pi^n}$$

if, for some δ in A , $\alpha \equiv \beta\delta^n \pmod{\pi}$.

Lemma 1. *For any positive divisor d of $n - 1$, an integer m given by (1) satisfies*

$$m \equiv N_d R_d \pmod{\pi^n},$$

where

$$(2) \quad N_d = \prod_{j=1}^d \sigma_{r^{-j}}(\text{Norm}_{K/K_d} \omega)^{h_0(j)}, \quad R_d = \prod_{j=d+1}^{n-1} \sigma_{r^{-j}}(\omega)^{h_1(j)},$$

with $h_0(j) = r^j - 1$, $h_1(j) = h_0(j) - h_0(\text{res}(j, d))$, and $\text{res}(j, d)$ is the least positive residue of j modulo d (i.e., the integer between 1 and d which is $\equiv j \pmod{d}$).

Proof. Set, in (1), $k' \equiv r^j \pmod{n}$, with $0 < j < n$. Then

$$(1') \quad m \equiv \prod_{j=1}^{n-1} \sigma_{r^{-j}}(\omega)^{h_0(j)} \pmod{\pi^n}.$$

Let $n - 1 = de$. For every integer i between 1 and d , the product of all factors in (1'), which correspond to those $j \equiv i \pmod{d}$, is

$$P(i) = \sigma_{r^{-i}} \left(\prod_{k=0}^{e-1} \sigma_{r^{-kd}}(\omega) \right)^{h_0(i)} \quad R_d(i) = \sigma_{r^{-i}}(\text{Norm}_{K/K_d} \omega)^{h_0(i)} R_d(i)$$

with

$$R_d(i) = \prod_{k=1}^{e-1} \sigma_{r-(kd+i)}(\omega)^{h_1(kd+i)}.$$

The conclusion follows by noting that the right-hand side of (1') is the product of all the $P(i)$ and that the product of all the $R_d(i)$ is R_d .

Lemma 2. Let d, d' be two positive divisors of $n-1$, with $d < d'$. Then

$$m \equiv N_d N_{d,d'} R_{d,d'} \pmod{\pi^n},$$

where N_d is given by (2) and

$$(3) \quad \begin{aligned} N_{d,d'} &= \prod_{j=d+1}^{d'} \sigma_{r-j}(\text{Norm}_{K/K_{d'}} \omega)^{h_1(j)}, \\ R_{d,d'} &= \prod_{j=d'+1}^{n-1} \sigma_{r-j}(\omega)^{h_2(j)}, \end{aligned}$$

with $h_1(j)$ as in Lemma 1 and $h_2(j) = h_1(j) - h_1(\text{res}(j, d'))$.

Proof. In view of Lemma 1, one has to just write R_d as a product of terms $P'(i')$ corresponding to the various residues $i' = \text{res}(j, d')$ modulo d' , for i' between 1 and d' . One thus finds

$$P'(i') = \sigma_{r-i'}(\text{Norm}_{K/K_{d'}} \omega)^{h_1(i')} R_{d,d'}(i'),$$

where $R_{d,d'}(i')$ has a similar expression to that of $R_d(i)$, with d' replacing d and h_2 replacing h_1 . The result then follows, after noting that $h_1(i') = 0$ for $i' \leq d$ and $h_2(j) = 0$ for $j \leq d'$.

Remark. The result in Lemma 2 can be extended to any increasing sequence of positive divisors $d, d', d'', \dots, d^{(k)}$ of $n-1$. This yields an expression for $m \pmod{\pi^n}$ as a product of conjugates of the norms of ω , over the subfields of K of degrees $d^{(i)}$ over $\mathbb{Q}$, and of a remainder factor like $R_{d,d'}$. The sequence of corresponding exponents $h_0(j), h_1(j), \dots$ is then inductively defined by $h_{k+1}(j) = h_k(j) - h_k(\text{res}(j, d^{(k)}))$. However, since the norms have the simplest expressions over K_2 and K_+ , we only consider the two divisors $d = 2$ and $d' = (n-1)/2$. Hence

Corollary. For $n > 3$,

$$m \equiv N N' R \pmod{\pi^n},$$

where

$$(4) \quad \begin{aligned} N &= (\text{Norm}_{K/K_2} \omega)^{r^2-1} \sigma_r(\text{Norm}_{K/K_2} \omega)^{r-1}, \\ N' &= \prod_{j=3}^{(n-1)/2} \sigma_{r-j}(|\omega|^2)^{h_1(j)}, \quad R = \prod_{j=(n+1)/2}^{n-1} \sigma_{r-j}(\omega)^{h_2(j)}, \end{aligned}$$

with $h_1(j) = r^j - r^{\text{res}(j, 2)}$, $\text{res}(j, 2) = 1$ (resp. 2) if j is odd (resp. even), and $h_2(j) = 2r^j$ if $n \equiv 1 \pmod{4}$, $h_2(j) = 2r^j + (-1)^j(r-r^2)$ if $n \equiv 3 \pmod{4}$.

Proof. In Lemma 2, take $d = 2$, $d' = (n-1)/2$, and set $N = N_d$, $N' = N_{d,d'}$, and $R = R_{d,d'}$ (for $n = 5$, Lemma 1 suffices). Note that for j between $(n+1)/2$ and $n-1$, we have $\text{res}(j, (n-1)/2) = j - (n-1)/2$ and

$h_2(j) = r^j - r^{\text{res}(j, 2)} - r^{j-(n-1)/2} + r^{\text{res}(j-(n-1)/2, 2)}$. If $n \equiv 1 \pmod{4}$, then $\text{res}(j-(n-1)/2, 2) = \text{res}(j, 2)$ and $h_2(j) \equiv 2r^j \pmod{n}$. If $n \equiv 3 \pmod{4}$, then $\text{res}(j-(n-1)/2, 2) = 3 - \text{res}(j, 2)$ and $h_2(j) \equiv 2r^j + (-1)^j(r - r^2) \pmod{n}$.

Lemma 3. *If the norm in K/K_2 of π (resp. ω) is $(a + b\sqrt{n^*})/2$ (resp. $(c + d\sqrt{n^*})/2$), with a, b, c, d in $\mathbb{Z}$, then*

$$4p = a^2 - n^*b^2, \quad 4q = c^2 - n^*d^2,$$

and

$$\left(\frac{N}{\pi}\right) = \left(\frac{2b}{\pi}\right)^{2-r-r^2} \left(\frac{ad+bc}{\pi}\right)^{r-1} \left(\frac{ad-bc}{\pi}\right)^{r^2-1},$$

where N is given by (4).

Proof. Since $(a + b\sqrt{n^*})/2 \equiv 0 \pmod{\pi}$, we have $\sqrt{n^*} \equiv -ab' \pmod{\pi}$ and $(c \pm d\sqrt{n^*})/2 \equiv 2'(c \pm (-ab'd)) \pmod{\pi}$, where, for n in $\mathbb{Z}$ prime to p , n' denotes an inverse of $n \pmod{p}$. Thus

$$N \equiv (2'(c - ab'd))^{r^2-1} (2'(c + ab'd))^{r-1} \pmod{\pi}.$$

Multiplying both sides by $(2b)^{r^2+r-2}$ and then applying the power residue character yields the result.

Lemma 4. *For $n \equiv 1 \pmod{4}$ and N' as defined in (4), we have*

$$\left(\frac{N'}{\pi}\right) = \left(\frac{\nu}{\pi\sigma_r(\pi)}\right),$$

where

$$(5) \quad \nu = \left| \prod_{3 \leq j \leq (n-3)/2, j: \text{ odd}} \sigma_{r-j}(\omega)^{r'-r} \right|^2$$

(the product is over the odd integers between 3 and $(n-3)/2$).

Proof. For j between 3 and $(n-1)/2$, let

$$\alpha_j = \sigma_{r-j}(|\omega|^2)^{h_1(j)},$$

so that (N'/π) is the product of the (α_j/π) . If j is odd, then $h_1(j+1) = r(r^j - r) = rh_1(j)$ and

$$\alpha_{j+1} = \sigma_{r-1}(\alpha_j)^r,$$

so that $(\alpha_{j+1}/\pi) = (\alpha_j/\sigma_r(\pi))$. The result follows by pairing, in the product of the (α_j/π) , every term of odd index with its successor.

Lemma 5. *For $n \equiv 1 \pmod{4}$ and R as defined in (4), we have*

$$\left(\frac{R}{\pi}\right) = \left(\frac{\omega}{\gamma}\right)^2,$$

where

$$(6) \quad \gamma = \prod_{j=(n+1)/2}^{n-1} \sigma_{r^j}(\pi).$$

Proof. For j between $(n+1)/2$ and $n-1$, let

$$\beta_j = \sigma_{r^{-j}}(\omega).$$

Then (R/π) is the product of the terms

$$\left(\frac{\beta_j}{\pi}\right)^{2r^j} = \left(\frac{\sigma_{r^j}(\beta_j)}{\sigma_{r^j}(\pi)}\right)^2 = \left(\frac{\omega}{\sigma_{r^j}(\pi)}\right)^2.$$

Hence we have the desired result.

Remark. The element γ of A , in (6), satisfies $|\gamma|^2 = p$. It is well known that if χ is a multiplicative character of order n on the finite field with p elements $\mathbb{F}_p$, then the Jacobi sums

$$J(\chi, \chi^j) = \sum_{t \in \mathbb{F}_p} \chi(t) \chi^j(1-t)$$

for j between 1 and $n-2$ are elements of A satisfying $|J(\chi, \chi^j)|^2 = p$ [3]. In particular, when $n=5$, all such elements γ are associates of Jacobi sums, as will be shown in §3.

Putting together Theorem 1, Corollary, and Lemmas 3, 4, and 5, we obtain

Theorem 2. *If $n \equiv 1 \pmod{4}$, then*

$$\rho(p, q) = \left(\frac{2b}{\pi}\right)^{2-r-r^2} \left(\frac{ad+bc}{\pi}\right)^{r-1} \left(\frac{ad-bc}{\pi}\right)^{r^2-1} \left(\frac{\nu}{\pi\sigma_r(\pi)}\right) \left(\frac{\omega}{\gamma}\right)^2,$$

where r is a primitive root of the prime n and a, b, c, d are in $\mathbb{Z}$ such that

$$4p = a^2 - nb^2, \quad 4q = c^2 - nd^2.$$

Also, π (resp. ω) is a prime (resp. primary prime) in A whose norm in K/K_2 is $(a+b\sqrt{n})/2$ (resp. $(c+d\sqrt{n})/2$). Further, ν is the real algebraic integer and γ is the element of A satisfying $|\gamma|^2 = p$, given by (5) and (6).

3. THE QUINTIC CASE

Let $n=5$. Then A is a unique factorization domain and $K_+ = K_2 = \mathbb{Q}(\sqrt{5})$. Thus, every prime number $p \equiv 1 \pmod{5}$ is the norm, in $K/\mathbb{Q}$, of some prime element π of A , and $4p = a^2 - 5b^2$, for some rational integers a, b . Moreover,

Lemma 6. *If $4p = a^2 - 5b^2$, with a, b in $\mathbb{Z}$, and if π is a prime divisor of $x = (a+b\sqrt{5})/2$ in A , then there is an associate of π in A whose norm in K/K_+ is $|x|$.*

Proof. The norm of x in $K_+/\mathbb{Q}$ is p , which splits as a product of four primes in A . Hence, by the uniqueness of prime factorization in A , x is, to within a unit factor u in K_+ , the product of two primes, π and its complex conjugate $\bar{\pi}$. Thus $x = u \cdot \text{Norm}_{K/K_+} \pi$, and, upon taking the norms of both sides in $K_+/\mathbb{Q}$, one gets $\text{Norm}_{K_+/\mathbb{Q}} u = 1$. Since K_+ is a quadratic field in which a fundamental unit is $\varepsilon = \zeta + \zeta^{-1}$, one has $u = \pm \varepsilon^k$ with k in $\mathbb{Z}$. Also, since $\text{Norm}_{K_+/\mathbb{Q}} \varepsilon = -1$, it follows that $k = 2j$, with j integer. Noting that $\varepsilon^2 = \text{Norm}_{K/K_+}(1 + \zeta^2)$, it follows that $x = \pm \text{Norm}_{K/K_+}((1 + \zeta^2)^j \pi)$. Hence the result (norms from a cyclotomic field to $\mathbb{Q}$ being positive).

Remark. The symbol (α/π) is unchanged if π is replaced by one of its associates or if α is replaced by $-\alpha$. So, in view of Lemma 6, one may take for π , in Theorem 2, any prime divisor of $(a + b\sqrt{5})/2$ in A , where a, b are in $\mathbb{Z}$ such that $4p = a^2 - 5b^2$. On the other hand, for ω , one needs a prime of A whose norm in K/K^+ is equal to $y = (c + d\sqrt{5})/2$, where c, d are in $\mathbb{Z}$ such that $4q = c^2 - 5d^2$. This (by Lemma 6) is possible if and only if $y > 0$ (e.g., if c and d are > 0).

As a primitive root of 5, we take $r = 2$. The value of ν that is given by (5) is trivially 1; and from (6), $\gamma = \pi\sigma_3(\pi)$.

Lemma 7. *If π is a prime element of A dividing p , then $\gamma = \pi\sigma_3(\pi)$ is an associate of the Jacobi sum $J(\chi, \chi)$, for a unique multiplicative character χ of order 5 on $\mathbb{F}_p$. More precisely, $\gamma = \pm\zeta^i J(\chi, \chi)$, for some integer i between 0 and 4, and if π is primary, then $\gamma = \pm J(\chi, \chi)$.*

Proof. The norm of γ in K/K^+ is p . By the uniqueness of prime factorization in A , any α in A whose norm in K/K^+ is p has the form $\alpha = u\sigma_i(\pi)\sigma_j(\pi)$, where u is a unit of K and i, j are integers between 1 and 4 such that $i \not\equiv \pm j \pmod{5}$. Hence $\alpha = u\sigma_k(\gamma)$ for a unique k between 1 and 4. Also, since $|\alpha| = |\sigma_k(\gamma)| = \sqrt{p}$, we have $|u| = 1$ and for all $\mathbb{Q}$ -conjugates $\sigma_j(u)$ of u , $|\sigma_j(u)| = 1$. Therefore u is a root of unity in K (Kronecker) and thus $u = \pm\zeta^i$ (Kummer) (e.g., [3] or [5]). In particular, taking $\alpha = J(\chi_0, \chi_0)$, where χ_0 is a multiplicative character of order 5 on $\mathbb{F}_p$, we have $\gamma = \pm\zeta^i \sigma_j(J(\chi_0, \chi_0)) = \pm\zeta^i J(\chi_0^j, \chi_0^j)$ for unique integers $0 \leq i \leq 4$, $1 \leq j \leq 4$. Hence we have proved the first part, with $\chi = \chi_0^j$. Moreover, for any such character χ , we have $J(\chi, \chi) \equiv -1 \pmod{\lambda^2}$ where $\lambda = \zeta - 1$. Indeed, let g be a primitive root of p and $\chi(g) = \zeta^h$, with h in $\mathbb{Z}$. For any t in $\mathbb{Z}$, prime to p , let $\text{ind}(t)$ denote the index of t with respect to g (i.e., an integer defined, $\text{mod } p-1$, by $t \equiv g^{\text{ind}(t)} \pmod{p}$). Then

$$\begin{aligned} J(\chi, \chi) &= \sum_{t=2}^{p-1} \zeta^{h(\text{ind}(t) + \text{ind}(1-t))} \equiv \sum_{t=2}^{p-1} (1 + h(\text{ind}(t) + \text{ind}(1-t))\lambda) \\ &\equiv p-2 + h \left(2 \sum_{k=1}^{p-2} k \right) \lambda \equiv -1 \pmod{\lambda^2} \end{aligned}$$

(since $p-1 \equiv 0 \pmod{\lambda^4}$). Now, if π is primary, then so is γ , and since $\gamma = \pm\zeta^i J(\chi, \chi) \equiv \pm(1 + i\lambda)(-1) \pmod{\lambda^2}$, it follows that $i \equiv 0 \pmod{5}$, i.e., $\gamma = \pm J(\chi, \chi)$.

Remark. Given a prime π in A dividing p , if $\gamma = \pi\sigma_3(\pi)$ is an associate of $J(\chi, \chi)$, then the only other $\mathbb{Q}$ -conjugate of $J(\chi, \chi)$ divisible by π is $\sigma_2(J(\chi, \chi)) = J(\chi^2, \chi^2)$. One may conversely start with any character χ of order 5 on $\mathbb{F}_p$ and determine a common nonunit factor π of $J(\chi, \chi)$ and $J(\chi^2, \chi^2)$ in A . This π is then a prime in A dividing p whose corresponding $\gamma = \pi\sigma_3(\pi)$ is an associate of $J(\chi, \chi)$; the representation $4p = a^2 - 5b^2$ is obtained by taking $\text{Norm}_{K/K^+} \pi$.

In view of Theorem 2 and Lemmas 6 and 7, we have

Theorem 3. *Let p, q be two prime numbers $\equiv 1 \pmod{5}$ and $4p = a^2 - 5b^2$, $4q = c^2 - 5d^2$, with a, b, c, d in $\mathbb{Z}$ and $c, d > 0$. Let π be a prime element*

of A dividing $(a + b\sqrt{5})/2$ and ω a primary prime element of A such that $|\omega|^2 = (c + d\sqrt{5})/2$. Then

$$(7) \quad \left(\frac{p}{\omega}\right) \left(\frac{q}{\pi}\right)^{-1} = \left(\frac{2b(ad + bc)}{\pi}\right) \left(\frac{ad - bc}{\pi}\right)^3 \left(\frac{\omega}{J(\chi, \chi)}\right)^2,$$

where χ is a multiplicative character of order 5 on $\mathbb{F}_p$ such that π is a common divisor of the Jacobi sums $J(\chi, \chi)$ and $J(\chi^2, \chi^2)$.

Corollary 1. For two prime numbers $p, q \equiv 1 \pmod{5}$, let χ_p and χ_q be multiplicative characters of order 5 on $\mathbb{F}_p$ and $\mathbb{F}_q$, respectively, and $J_p = J(\chi_p, \chi_p)$, $J_q = J(\chi_q, \chi_q)$ the corresponding Jacobi sums. Let π (resp. ω) be a nonunit common divisor of J_p and $\sigma_2(J_p)$ (resp. of J_q and $\sigma_2(J_q)$, with ω primary), and $|\pi|^2 = (a + b\sqrt{5})/2$, $|\omega|^2 = (c + d\sqrt{5})/2$, with a, b, c, d in $\mathbb{Z}$. Then

$$(8) \quad \left(\frac{p}{\omega}\right) \left(\frac{q}{\pi}\right)^{-1} = \left(\frac{2b}{\pi}\right)^4 \left(\frac{a^2d^2 - b^2c^2}{\pi}\right)^3 \left(\frac{J_q}{J_p}\right)^3.$$

Proof. By Lemma 7, $J_q = \pm\omega\sigma_3(\omega)$, so that

$$\left(\frac{J_q}{J_p}\right) = \left(\frac{\omega}{J_p}\right) \left(\frac{\sigma_3(\omega)}{J_p}\right) = \left(\frac{\omega}{J_p}\right) \left(\frac{\omega}{\sigma_2(J_p)}\right)^3.$$

Also, since $(\omega/J_p) = (\omega/\pi)(\omega/\sigma_3(\pi))$,

$$\left(\frac{\omega}{\sigma_2(J_p)}\right) = \left(\frac{\omega}{\pi}\right) \left(\frac{\omega}{\sigma_2(\pi)}\right) = \left(\frac{\omega}{J_p}\right) \left(\frac{|\omega|^2}{\sigma_2(\pi)}\right).$$

Thus

$$\left(\frac{J_q}{J_p}\right) = \left(\frac{\omega}{J_p}\right)^4 \left(\frac{|\omega|^2}{\sigma_2(\pi)}\right)^3.$$

Moreover, since $\sigma_2(|\pi|^2) = (a - b\sqrt{5})/2 \equiv 0 \pmod{\sigma_2(\pi)}$, it follows that $2b|\omega|^2 = b(c + d\sqrt{5}) \equiv bc + ad \pmod{\sigma_2(\pi)}$ and

$$\left(\frac{|\omega|^2}{\sigma_2(\pi)}\right) = \left(\frac{2b}{\sigma_2(\pi)}\right)^{-1} \left(\frac{ad + bc}{\sigma_2(\pi)}\right) = \left(\frac{2b}{\pi}\right)^3 \left(\frac{ad + bc}{\pi}\right)^2.$$

Hence

$$\left(\frac{\omega}{J_p}\right) = \left(\frac{J_q}{J_p}\right)^{-1} \left(\frac{2b}{\pi}\right)^4 \left(\frac{ad + bc}{\pi}\right).$$

Substituting this in (7) yields the result.

Corollary 2. In the notation of Corollary 1, we have

$$(9) \quad \left(\frac{p}{\omega}\right) \left(\frac{q}{\pi}\right) = \left(\frac{J_q}{J_p}\right)^3.$$

Proof. Since $4p = a^2 - 5b^2$ and $4q = c^2 - 5d^2$, it follows that $a^2d^2 - b^2c^2 \equiv -4b^2q \pmod{p}$. Hence

$$\left(\frac{a^2d^2 - b^2c^2}{\pi}\right) = \left(\frac{2b}{\pi}\right)^2 \left(\frac{q}{\pi}\right).$$

Substituting this in (8) yields the result.

Since the left-hand side of (9) is symmetric in p and q , we deduce

Corollary 3. *For any two prime numbers $p, q \equiv 1 \pmod{5}$ and any multiplicative characters χ_p and χ_q , of order 5, on $\mathbb{F}_p$ and $\mathbb{F}_q$, respectively, we have*

$$\left(\frac{J(\chi_p, \chi_p)}{J(\chi_q, \chi_q)} \right) = \left(\frac{J(\chi_q, \chi_q)}{J(\chi_p, \chi_p)} \right).$$

Remark. The reciprocity relation between Jacobi sums, in Corollary 3, is, quite plausibly, valid for any odd prime n . I have checked it for $n = 3, 5, 7, 11, 13$.

ADDED IN PROOF

This reciprocity relation between Jacobi sums has now been established in general, and the proof is due to appear, shortly, elsewhere.

REFERENCES

1. G. Eisenstein, *Beweis der allgemeinsten Reciprocitätsgesetze zwischen reellen und complexen Zahlen*, Math. Werke, 2, Chelsea, New York, 1975, pp. 712–721.
2. C. Helou, *On rational reciprocity*, Proc. Amer. Math. Soc. **108** (1990), 861–866.
3. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Springer, New York, 1990.
4. E. Lehmer, *The quintic character of 2 and 3*, Duke Math. J. **18** (1951), 11–18.
5. L. Washington, *Introduction to cyclotomic fields*, Springer, New York, 1982.
6. K. S. Williams, *Explicit criteria for quintic residuacity*, Math. Comp. **30** (1976), 847–853.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, DELAWARE COUNTY CAMPUS, MEDIA, PENNSYLVANIA 19063-5596

E-mail address: cxh22@psuvm.psu.edu