ILLINOIS JOURNAL OF MATHEMATICS
Volume 36, Number 1, Spring 1992

ROOT NUMBERS OF JACOBI-SUM HECKE CHARACTERS

BY

DAVID E. ROHRLICH[1]

Let p be an odd prime and n a positive integer, and let K be the cyclotomic field of p^n-th roots of unity. Let a, b, and c be nonzero integers satisfying $a + b + c = 0$. We assume that none of the integers a, b, and c is divisible by p^n and that at most one of them is divisible by p. The unitary Jacobi-sum Hecke character χ associated to these data is defined as follows. Given a prime ideal $\mathfrak{l}$ of K, relatively prime to p, and an element x of the ring of integers of K, relatively prime to $\mathfrak{l}$, let $\left(\frac{x}{\mathfrak{l}}\right)_{p^n}$ denote the unique p^n-th root of unity such that

$$\left(\frac{x}{\mathfrak{l}}\right)_{p^n} \equiv x^{(N\mathfrak{l}-1)/p^n} (\operatorname{mod} \mathfrak{l}).$$

Put

$$J(\mathfrak{l}) = -\sum_x \left(\frac{x}{\mathfrak{l}}\right)_{p^n}^a \left(\frac{1-x}{\mathfrak{l}}\right)_{p^n}^b,$$

where x runs over representatives for the distinct residue classes modulo $\mathfrak{l}$, the classes of 0 and 1 being omitted. Now extend J by complete multiplicativity to the group $I(p)$ of fractional ideals of K relatively prime to p, and embed K into $\mathbf{C}$, so that J becomes a homomorphism from $I(p)$ to $\mathbf{C}^\times$. Then J is a Hecke character (Weil [8]). The associated unitary Hecke character is

$$\chi(\mathfrak{a}) = J(\mathfrak{a})(\mathrm{N}\mathfrak{a})^{-1/2},$$

where $\mathfrak{a}$ denotes an arbitrary element of $I(p)$.

In his original paper of 1952, Weil posed the problem of determining the conductor $\mathfrak{f}(\chi)$ of χ. While the case $n = 1$ was settled by Hasse [4] soon thereafter, the determination of $\mathfrak{f}(\chi)$ for arbitrary n was accomplished only recently, by Coleman and McCallum [1]. The present note gives an application of their result. At issue is the root number in the functional equation of

Received July 9, 1990
1980 Mathematics Subject Classification (1985 Revision). Primary 11R42.

[1] Research partially supported by a grant from the National Science Foundation.

the Hecke L-function $L(s,\chi)$. Put

$$D = p^{(np-n-1)p^{n-1}},$$
$$g = (p-1)p^{n-1}/2,$$

and

$$\Lambda(s,\chi) = (D\mathbf{N}\mathfrak{f}(\chi))^{s/2}((2\pi)^{-s}\Gamma(s+1/2))^{g}L(s,\chi),$$

so that the functional equation has the form

$$\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\chi)$$

with $W(\chi) = \pm 1$. The work of Coleman and McCallum will enable us to determine $W(\chi)$ precisely, just as the earlier result of Hasse made it possible to determine $W(\chi)$ precisely in the case $n = 1$ [3].

Given a nonzero element ν of $\mathbf{Q}_p$, let $v_p(\nu)$ denote the p-adic ordinal of ν and let ν' denote the quotient of ν by $p^{v_p(\nu)}$, so that $\nu = p^{v_p(\nu)}\nu'$. It is suggestive, although not especially efficient, to divide our result into a "first case" and a "second case" according as abc is prime to p or divisible by p.

THEOREM. (1) *Suppose that $p \nmid abc$. Put*

$$u = v_p\left((a^a b^b c^c)^{p-1} - 1\right)$$

and

$$d = \frac{(a^a b^b c^c)^{p-1} - 1}{p^u}.$$

Then

$$W(\chi) = \begin{cases} -\left(\dfrac{abcd}{p}\right)\left(\dfrac{-1}{p}\right)^n, & \text{if } u \le n, \\ \left(\dfrac{2}{p}\right), & \text{if } u > n. \end{cases}$$

(2) *Suppose that $p | abc$. Put*

$$u = v_p(abc)$$

and

$$d = \begin{cases} \dfrac{v_p(a^a b^b c^c)}{u}(1-u), & \text{if } u \not\equiv 1 \pmod{p}, \\ -v_p(a^a b^b c^c), & \text{if } u \equiv 1 \pmod{p}. \end{cases}$$

Then $d' = d/p^u$ *and*

$$W(\chi) = -\left(\frac{a'b'c'd'}{p}\right)\left(\frac{-1}{p}\right)^{n+u}.$$

I am indebted to the referee for an important comment regarding the second case of the theorem: If p divides abc, then

$$\left(\frac{a'b'c'd'}{p}\right) = \left(\frac{u-1}{p}\right)$$

or

$$\left(\frac{a'b'c'd'}{p}\right) = 1$$

according as $u \not\equiv 1 \pmod{p}$ or $u \equiv 1 \pmod{p}$. This is an easy consequence of the definitions: for example, if $u \equiv 1 \pmod{p}$ and it is a which is divisible by p, then $d = -au$, so that $d' \equiv -a' \pmod{p}$. Since we also have $b \equiv -c \pmod{p}$, we find that $a'b'c'd'$ is a square modulo p. The referee has also pointed out that the proof of the theorem affords a more nearly uniform definition of the number d' than is evident from the final statement. This remark will be clarified at the end of §8.

So far we have regarded n as fixed. In the following corollary, we let n vary. As before, p is a fixed odd prime and a, b, and c are fixed nonzero integers summing to 0, with at most one of a, b, and c divisible by p. If n is sufficiently large, then none of a, b, and c is divisible by p^n, so that the hypotheses in force until now are still satisfied.

COROLLARY. *If n is sufficiently large, then $(-1/p)^n W(\chi)$ is independent of n.*

I would like to thank Robert Coleman for suggesting the problem treated in this note. I am also grateful to him for help with the use of his explicit reciprocity law.

Finally, I would like to take this opportunity to correct an error in [7]. Contrary to what is asserted in [7], the normalization of the Hilbert symbol used by Iwasawa in his paper on explicit reciprocity laws is the same as that of Artin-Tate. Consequently, the Hilbert symbol as defined on p. 101 of [7] is the inverse of the correct symbol, given our subsequent quotation of Iwasawa's reciprocity laws. In the present paper we follow the convention of [1] for the Hilbert symbol, which is the inverse of the convention of Iwasawa and Artin-Tate.

1. Local root numbers

We shall recall a few formulas which are needed for the calculations that follow. Let H be a local field of characteristic 0, let θ be a unitary character of $H^\times$, and let ψ be a nontrivial unitary character of H. The local root number $W(\theta, \psi)$ associated to these data is defined by the equation

$$(1) \qquad W(\theta, \psi) = \varepsilon(\theta, \psi, dx)/|\varepsilon(\theta, \psi, dx)|,$$

where dx is any Haar measure on H and the epsilon factor is as in [2], p. 526, formula (3.3.1). The dependence of $W(\theta, \psi)$ on ψ can be read from formula (3.3.3) of [2]: any other nontrivial unitary character of H has the form

$$\psi_y : x \mapsto \psi(xy)$$

for some $y \in H^\times$, and we have

$$(2) \qquad W(\theta, \psi_y) = \theta(y)W(\theta, \psi).$$

Now suppose that H is nonarchimedean, let $\mathcal{O}$ be the ring of integers of H, and let π be a uniformizer in $\mathcal{O}$. We write $m(\psi)$ for the largest integer μ such that ψ is trivial on $\pi^{-\mu}\mathcal{O}$, and $\pi^{f(\theta)}\mathcal{O}$ for the conductor of θ. Thus $f(\theta)$ is an integer ≥ 0, and $f(\theta) > 0$ if and only if θ is ramified. We call $f(\theta)$ the conductor-exponent of θ. If θ is ramified, then the following integral formula holds, where $U = \mathcal{O}^\times, \beta$ is an arbitrary element of $H^\times, dx$ is any Haar measure on H, q is the order of $\mathcal{O}/\pi\mathcal{O}$, and meas $\mathcal{O}$ is the measure of $\mathcal{O}$ with respect to dx:

$$(3) \quad \int_U \theta^{-1}(x)\psi(\beta x)\,dx = \begin{cases} q^{-f(\theta)/2}(\text{meas } \mathcal{O})\theta(\beta)W(\theta, \psi), & \text{if } \beta \in \pi^{-f(\theta)-m(\psi)}U, \\ 0, & \text{otherwise.} \end{cases}$$

The validity of (3) follows from formulas (3.4.3.2) and (5.7.2) of [2].

2. Relative local root numbers

Next we recall a computational device used in [6]. Let F be a local field of characteristic 0 and let K be an F-algebra of one of the following three types:

(i) K is a ramified quadratic extension of F.
(ii) K is an unramified quadratic extension of F.
(iii) $K = F \oplus F$.

Let κ be the quadratic character of $F^\times$ associated to the extension K/F by class field theory, and let χ be any unitary character of $K^\times$ which coincides with κ on $F^\times$:

$$\chi | F^\times = \kappa. \tag{4}$$

In case (iii) our conditions mean that κ is trivial and that if we write $\chi = \chi_1 \oplus \chi_2$ on $F^\times \oplus F^\times$, then $\chi_1 = \chi_2^{-1}$. Now fix a nontrivial unitary character $\psi_F \colon F \to \mathbf{C}^\times$ and put

$$\psi_K = \psi_F \circ \mathrm{tr}_{K/F}, \tag{5}$$

where $\mathrm{tr}_{K/F}$ denotes the trace function of the F-algebra K. In cases (i) and (ii) the notation $W(\chi, \psi_K)$ requires no explanation. In case (iii) we define

$$W(\chi, \psi_K) = W(\chi_1, \psi_F) W(\chi_2, \psi_F).$$

In all three cases we define a relative local root number $W(\kappa, \chi)$ by the formula

$$W(\kappa, \chi) = W(\chi, \psi_K)/W(\kappa, \psi_F). \tag{6}$$

It follows from (2), (4), and (5) that the right-hand side of (6) is independent of the choice of ψ_F.

To show how relative local root numbers can be used to compute global root numbers, suppose now that F is a number field and that K is a quadratic extension of F. Let κ be the quadratic Hecke character of F associated to the extension K/F, and let χ be any unitary Hecke character of K which coincides with κ on the ideles of F. Given a place v of F, we write F_v for the completion of F at v and K_v for $K \otimes_F F_v$. Then K_v is an F_v-algebra of type (i), (ii), or (iii) above according as v ramifies, remains prime, or splits in K. (Strictly speaking, when v splits in K we must also fix an ordering of the two primes of K above v in order to identify K_v with $F_v \oplus F_v$.) The v-components of κ and χ will be denoted κ_v and χ_v respectively. Then $W(\kappa_v, \chi_v)$ is defined, and we have

$$W(\chi) = \prod_v W(\kappa_v, \chi_v), \tag{7}$$

where v runs over the places of F (see [6], p. 530).

In order to apply (7), we need to know the local constants $W(\kappa_v, \chi_v)$. The critical case for us is the case where v is a finite prime of odd residue characteristic which ramifies in the extension K/F.

3. An expression for the local constant: first form

In this section and the next, p denotes an odd prime, F a finite extension of $\mathbf{Q}_p$, and K a ramified quadratic extension of F. We write $\mathscr{O}_F$ and $\mathscr{O}_K$ for the corresponding rings of integers, U_F and U_K for the multiplicative groups of units in these rings, and π_F and π_K for generators of their maximal ideals, chosen so that

$$\pi_F = \pi_K^2. \tag{8}$$

Finally, we put

$$q = |\mathscr{O}_F/\pi_F\mathscr{O}_F| = |\mathscr{O}_K/\pi_K\mathscr{O}_K|, \tag{9}$$

where the vertical bars denote cardinality.

Our goal is to compute $W(\kappa, \chi)$, where κ is the quadratic character of $F^\times$ associated to the extension K/F by class field theory and χ is a unitary character of $K^\times$ satisfying $\chi|F^\times = \kappa$. We begin with some observations concerning the conductors of these characters. First, since p is odd and K/F is a ramified quadratic extension, we have $f(\kappa) = 1$. Second, either $f(\chi) = 1$ or else $f(\chi)$ is an even integer ≥ 2. Indeed, since $\chi|F^\times = \kappa$ and κ is ramified we certainly have $f(\chi) \geq 1$. Now if $f(\chi)$ were an odd integer strictly greater than 1, then we would have $\chi(1 + x\pi_F^{(f(\chi)-1)/2}) \neq 1$ for some $x \in \mathscr{O}_F$. This would contradict the fact that $f(\kappa) = 1$, because $\chi|F^\times = \kappa$.

The starting point for the calculation is a formula which expresses $W(\kappa, \chi)$ as an integral over the quotient group $V = U_K/U_F$. Let d_Fx and d_Ky denote fixed Haar measures on F and on K, and observe that the restrictions of these measures to U_F and U_K respectively are Haar measures on the latter groups. We write dz for the quotient measure d_Ky/d_Fx on V, so that

$$\int_V \left(\int_{U_F} g(xz)\, d_Fx \right) dz = \int_{U_K} g(y)\, d_Ky \tag{10}$$

for continuous functions $g\colon U_K \to \mathbf{C}$. Let $\operatorname{meas}_F S$ and $\operatorname{meas}_K S$ denote the measure of a measurable subset S of F or K respectively, and for y in K put

$$\lambda(y) = \begin{cases} 1, & \text{if } \operatorname{tr}_{K/F} y \in U_F, \\ 0, & \text{otherwise.} \end{cases}$$

We observe that the function $y \mapsto \lambda(y/\pi_K^{f(\chi)-1})$ on U_K is constant on cosets of U_F and therefore may be regarded as a function on V. The same is true for the function

$$y \mapsto \chi^{-1}(y/\pi_K^{f(\chi)-1})\kappa(\operatorname{tr}_{K/F}(y/\pi_K^{f(\chi)-1}))$$

(where we make the convention that $\kappa(0) = 0$) because $\chi|F^\times = \kappa$.

PROPOSITION 1. *Put $f = f(\chi)$. Then*

$$W(\kappa, \chi) = q^{(f-1)/2} \frac{\operatorname{meas}_F U_F}{\operatorname{meas}_K U_K} \int_V \chi^{-1}\left(\frac{z}{\pi_K^{f-1}}\right) \kappa\left(\operatorname{tr}_{K/F}\left(\frac{z}{\pi_K^{f-1}}\right)\right) \lambda\left(\frac{z}{\pi_K^{f-1}}\right) dz.$$

Proof. The formula is only a slight extension of Prop. 7 of [6], but for the sake of completeness we give a brief proof. Fix a nontrivial unitary character $\psi_F \colon F \to \mathbf{C}^\times$ and let $\psi_K = \psi_F \circ \operatorname{tr}_{K/F}$; put $m = m(\psi_F)$. Then $m(\psi_K) = 1 + 2m$, because π_K generates the different ideal of K/F. Let us apply (3) with $\theta = \kappa$ and $\theta = \chi$, taking account of (9) and of the fact that $\kappa^{-1} = \kappa$. We obtain the formulas

$$(11) \quad \int_{U_F} \kappa(x)\psi_F(\beta x)\, d_F x$$
$$= \begin{cases} q^{-1/2}(\operatorname{meas}_F \mathcal{O}_F)\kappa(\beta) W(\kappa, \psi_F), & \text{if } \beta \in \pi_F^{-1-m} U_F, \\ 0, & \text{otherwise} \end{cases}$$

and

(12)
$$\int_{U_K} \chi^{-1}(y)\psi_K\left(\frac{y}{\pi_K^{f+1+2m}}\right) d_K y = q^{-f/2}(\operatorname{meas}_K \mathcal{O}_K)\chi(\pi_K^{-f-1-2m}) W(\chi, \psi_K).$$

Now the integral in (12) can be evaluated using (10), and we find

$$q^{-f/2}(\operatorname{meas}_K \mathcal{O}_K)\chi(\pi_K^{-f-1-2m}) W(\chi, \psi_K)$$
$$= \int_V \chi^{-1}(z)\left(\int_{U_F} \kappa(x)\psi_F\left(\operatorname{tr}_{K/F}\left(\frac{z}{\pi_K^{f-1}}\right)\frac{x}{\pi_F^{1+m}}\right) d_F x\right) dz$$
$$= q^{-1/2}(\operatorname{meas}_F \mathcal{O}_F)\kappa(\pi_F^{1+m}) W(\kappa, \psi_F)$$
$$\times \int_V \chi^{-1}(z)\kappa\left(\operatorname{tr}_{K/F}\left(\frac{z}{\pi_K^{f-1}}\right)\right)\lambda\left(\frac{z}{\pi_K^{f-1}}\right) dz,$$

by virtue of (8) and (11). Recalling the definition (6), and making some simplifications, we arrive at the stated formula.

4. An expression for the local constant: second form

We retain the notation and hypotheses of §3, but we make the additional assumption that $q = p$. As we have remarked in §3, $f(= f(\chi))$ is either 1 or a positive even integer. In the latter case, the function $x \mapsto \chi(1 + x\pi_K^{f-1})$ is a nontrivial character of $\mathcal{O}_F$ with values in the p-th roots of unity. Hence there is an invertible residue class l modulo p such that

$$\chi(1 + \pi_K^{f-1}) = e^{2\pi i l/p}. \tag{13}$$

Of course l depends on the choice of uniformizer π_K. Put

$$\delta = \begin{cases} 0, & \text{if } p \equiv 1 \pmod 4, \\ 1, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{14}$$

PROPOSITION 2.

$$W(\kappa, \chi) = \begin{cases} \left(\dfrac{-2l}{p}\right)\chi(\pi_K^{f-1})i^{\delta}, & \text{if } f > 1, \\ \left(\dfrac{2}{p}\right), & \text{if } f = 1. \end{cases}$$

Proof. If j is a positive integer we write V_j for the image in V of the subgroup $1 + \pi_K^j\mathcal{O}_K$ of U_K. If j is even, then we have

$$|V/V_j| = q^{j/2} = p^{j/2}, \tag{15}$$

because the assignment $x \mapsto 1 + \pi_K x \, (x \in \mathcal{O}_F)$ induces a bijection of $\mathcal{O}_F/\pi_F^{j/2}\mathcal{O}_F$ onto V/V_j. Indeed, $U_K = U_F + \pi_K\mathcal{O}_F$, so that every element of V has a unique representative of the form $1 + \pi_K x$ with $x \in \mathcal{O}_F$.

According to Prop. 1, we have

$$W(\kappa, \chi) = \gamma \int_V \chi^{-1}(z)\kappa\left(\operatorname{tr}_{K/F}\left(\frac{z}{\pi_K^{f-1}}\right)\right)\lambda\left(\frac{z}{\pi_K^{f-1}}\right) dz \tag{16}$$

with

$$\gamma = p^{(f-1)/2}\frac{\operatorname{meas}_F U_F}{\operatorname{meas}_K U_K}\chi(\pi_K^{f-1}). \tag{17}$$

If $f = 1$, then the integrand in (16) is identically equal to $\kappa(2)$, as one sees by choosing a representative for z of the form $1 + \pi_K x$ with $x \in \mathscr{O}_F$ (recall (8)). Therefore

$$W(\kappa, \chi) = \kappa(2) = \left(\frac{2}{p}\right)$$

in this case.

If f is a positive even integer, then the integrand is at least constant on cosets of V_f, so that (15), (16), and (17) give

$$(18)\quad W(\kappa,\chi) = \chi\left(\pi_K^{f-1}\right)p^{-1/2}\sum_z \chi^{-1}(z)\kappa\left(\mathrm{tr}_{K/F}\left(\frac{z}{\pi_K^{f-1}}\right)\right)\lambda\left(\frac{z}{\pi_K^{f-1}}\right),$$

where z runs over a set of representatives in U_K for the cosets of V_f in V. Now if $z = 1 + \pi_K x$ with $x \in \mathscr{O}_F$, then

$$\mathrm{tr}_{K/F}\left(\frac{z}{\pi_K^{f-1}}\right) = 2x\pi_F^{1-f/2},$$

and this number is a unit if and only if

$$x \in \pi_F^{f/2-1}U_F = \pi_K^{f-2}U_F.$$

Hence if we confine our attention to the nonzero terms in (18), then we see that we can choose $x = j\pi_K^{f-2}$ $(1 \le j \le p-1)$, i.e.

$$z = 1 + \pi_K x = 1 + j\pi_K^{f-1} \quad (1 \le j \le p-1).$$

Then in view of (13) we can rewrite (18) as follows:

$$\begin{aligned} W(\kappa,\chi) &= \chi\left(\pi_K^{f-1}\right)p^{-1/2}\sum_{j=1}^{p-1}\kappa(2j)e^{-2\pi i l j/p} \\ &= \kappa(-2l)\chi\left(\pi_K^{f-1}\right)p^{-1/2}\sum_{j=1}^{p-1}\kappa(j)e^{2\pi i j/p}. \end{aligned}$$

The stated formula now follows from the standard evaluation of the quadratic Gauss sum.

5. The global root number

For the remainder of this paper the setting is the same as in the introduction: K is the cyclotomic field of p^n-th roots of unity, F is the maximal totally real subfield of K, and χ is the unitary Jacobi-sum Hecke character determined by the triple (a, b, c), where $a + b + c = 0$, $\gcd(a, b, c, p) = 1$, and $p^n \nmid a, b, c$. We write $\mathfrak{p}$ for the prime ideal of K above p, and $\kappa_{\mathfrak{p}}$ and $\chi_{\mathfrak{p}}$ for the local components of κ and χ at $\mathfrak{p}$. The conductor $\mathfrak{f}(\chi)$ of χ has the form

$$\mathfrak{f}(\chi) = \mathfrak{p}^f,$$

with $f = f(\chi_{\mathfrak{p}})$, and if $f > 1$ then f is even.

When $f > 1$, we define an invertible residue class l modulo p by the condition

$$\chi_{\mathfrak{p}}(1 + \pi_K^{f-1}) = e^{2\pi i l/p}, \tag{19}$$

where $\pi_K = \zeta - \zeta^{-1}$ and $\zeta = e^{2\pi i/p^n}$ (recall that an embedding of K into $\mathbf{C}$ was fixed in the introduction).

Given a residue class x modulo p^n, let $\langle x \rangle_{p^n}$ or simply $\langle x \rangle$ denote the least nonnegative representative for x modulo p^n. Let H denote the set of $h \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ which satisfy

$$\langle ah^{-1} \rangle + \langle bh^{-1} \rangle + \langle ch^{-1} \rangle = p^n.$$

Then H is a set of representatives for the distinct cosets of $\{\pm 1\}$ in $(\mathbf{Z}/p^n\mathbf{Z})^\times$, because $\langle -x \rangle = p^n - \langle x \rangle$ provided x is nonzero (mod p^n). Let k be the number of elements h of H satisfying $1 \le \langle h \rangle \le (p^n - 1)/2$.

PROPOSITION 3.

$$W(\chi) = \begin{cases} (-1)^k \left(\dfrac{l}{p}\right)\left(\dfrac{-1}{p}\right)^{(n+f/2)}, & \text{if } f > 1, \\ \left(\dfrac{2}{p}\right), & \text{if } f = 1. \end{cases}$$

Proof. Formula (7) of §2 is applicable in the case at hand, because the condition that χ agree with κ on the ideles of F is satisfied. Indeed, this condition is equivalent to the condition that χ be equivariant with respect to complex conjugation ([6], Prop. 1), and the latter condition can be verified directly from the formula defining the Jacobi sum. Now according to Props. 11 and 12 of [6], we have $W(\kappa_v, \chi_v) = 1$ if v is either an infinite place of F or a finite place where χ_v is unramified. Therefore (7) gives $W(\chi) = W(\kappa_{\mathfrak{p}}, \chi_{\mathfrak{p}})$.

If $f = 1$, then the stated formula follows at once from Prop. 2.

If $f > 1$, then Prop. 2 gives

$$W(\chi) = \left(\frac{-2l}{p}\right)\chi_{\mathfrak{p}}(\pi_K^{f-1}) i^{\delta}, \tag{20}$$

with δ as in (14). Since χ is a Hecke character unramified outside $\mathfrak{p}$ and infinity, we have

$$\chi_{\mathfrak{p}}(\pi_K) = \prod_{v \in \infty} \chi_v^{-1}(\pi_K), \tag{21}$$

where ∞ denotes the set of infinite places of F. On the other hand, Stickelberger's theorem implies that for $z \in K$,

$$\prod_{v \in \infty} \chi_v^{-1}(z) = \prod_{h \in H} \frac{z^{\sigma_h}}{|z^{\sigma_h}|} \tag{22}$$

([8], formula (9)), where σ_h is the automorphism of K sending ζ to ζ^h. Combining (21) and (22), we see that

$$\chi_{\mathfrak{p}}(\pi_K) = \prod_{h \in H} i \operatorname{sign}(\sin 2\pi h/p^n) = i^g(-1)^{g-k}, \tag{23}$$

where $g = (p-1)p^{n-1}/2$ is the cardinality of H. Now substitute (23) in (20). We obtain

$$\begin{aligned} W(\chi) &= \left(\frac{-2l}{p}\right) i^{g(f-1)+\delta}(-1)^{g-k} \\ &= \left(\frac{-2l}{p}\right)\left(\frac{-1}{p}\right)^{f/2} i^{\delta-g}(-1)^{g-k}. \end{aligned}$$

Considering separately the four possibilities for the residue class of p modulo 8, one checks that this last expression coincides with the stated formula.

It remains to make the quantities $(-1)^k$, f, and (l/p) more explicit. First we consider $(-1)^k$.

6. Gauss's lemma

We begin with a convenient formulation.

LEMMA. *Let N be an integer ≥ 3, let σ be a permutation of $(\mathbf{Z}/N\mathbf{Z})^\times$ satisfying the identity $\sigma(-x) = -\sigma(x)$, and let I be a set of representatives for the distinct cosets of $\{\pm 1\}$ in $(\mathbf{Z}/N\mathbf{Z})^\times$. Write J for the complement of I in $(\mathbf{Z}/N\mathbf{Z})^\times$. Then*

$$\operatorname{sign}(\sigma) = (-1)^{|\sigma(I) \cap J|}.$$

Proof. For each $j \in \sigma(I) \cap J$, let τ_j be the transposition which interchanges j and $-j$, and let τ be the product of the τ_j. Then $\tau \circ \sigma(I) = I$ and $\tau \circ \sigma(-x) = -\tau \circ \sigma(x)$. It follows that $\tau \circ \sigma$ is an even permutation, whence $\operatorname{sign}(\sigma) = \operatorname{sign}(\tau)$.

We apply the lemma as follows: Let $\langle x \rangle = \langle x \rangle_N$ denote the least nonnegative residue of x modulo N. Since

$$\sum_{i\in I}\langle i\rangle = \sum_{i\in I}\langle \sigma(i)\rangle - \sum_{j\in\sigma(I)\cap J}\langle j\rangle + \sum_{j\in\sigma(I)\cap J}\langle -j\rangle,$$

and $\langle -j\rangle = N - \langle j\rangle$, we have

$$\sum_{i\in I}\langle \sigma(i)\rangle \equiv \sum_{i\in I}\langle i\rangle + N|\sigma(I) \cap J| \pmod 2.$$

Hence if N is odd, then

$$(-1)^{\sum_{i\in I}\langle \sigma(i)\rangle} = \operatorname{sign}(\sigma)(-1)^{\sum_{i\in I}\langle i\rangle}. \tag{24}$$

Now take $N = p^w$ with $w \geq 1$, let ν be an integer prime to p, and suppose that σ is the permutation $\sigma(x) = \nu x^{-1}$. Let I be the set of $i \in (\mathbf{Z}/p^w\mathbf{Z})^\times$ satisfying $1 \leq \langle i \rangle \leq (p^w - 1)/2$. Then

$$\sum_{i\in I}\langle i\rangle = \frac{(p^{2w-1}+1)(p-1)}{8},$$

so that

$$(-1)^{\sum_{i\in I}\langle i\rangle} = \left(\frac{2}{p}\right). \tag{25}$$

On the other hand, σ is the composition of two permutations of $(\mathbf{Z}/p^w\mathbf{Z})^\times$: the inversion map $x \mapsto x^{-1}$ and the translation $x \mapsto \nu x$. The former, being the product of $(p^{w-1}(p-1)/2) - 1$ transpositions, has sign $-(-1/p)$, while the latter has sign equal to the determinant of the regular representation of $(\mathbf{Z}/p^w\mathbf{Z})^\times$ at ν, namely (ν/p). (Write the regular representation as a direct sum of Dirichlet characters.) It follows that

$$\operatorname{sign}(\sigma) = -\left(\frac{-\nu}{p}\right). \tag{26}$$

Together, (24), (25), and (26) give

$$(-1)^{\sum_{i\in I}\langle \nu i^{-1}\rangle} = -\left(\frac{-2\nu}{p}\right). \tag{27}$$

More generally, suppose that $\nu = p^{\upsilon}\nu'$, where $\upsilon = \upsilon_p(\nu) < w$. Write $\langle x\rangle' = \langle x\rangle_{p^{w-\upsilon}}$ for the least nonnegative residue of x modulo $p^{w-\upsilon}$ and I' for the subset of $(\mathbf{Z}/p^{w-\upsilon}\mathbf{Z})^{\times}$ consisting of all i such that $1 \leq \langle i\rangle' \leq (p^{w-\upsilon} - 1)/2$. Then

$$\sum_{i\in I}\langle \nu i^{-1}\rangle = p^{\upsilon}\sum_{i\in I}\langle \nu' i^{-1}\rangle'. \tag{28}$$

Since

$$\frac{p^{w}-1}{2} = \frac{p^{\upsilon}-1}{2}p^{w-\upsilon} + \frac{p^{w-\upsilon}-1}{2},$$

the right-hand side of (28) is

$$p^{\upsilon}\frac{p^{\upsilon}-1}{2}\sum_{x\in(\mathbf{Z}/p^{w-\upsilon}\mathbf{Z})^{\times}}\langle x\rangle' + p^{\upsilon}\sum_{i\in I'}\langle \nu' i^{-1}\rangle',$$

or in other words

$$p^{\upsilon}\frac{p^{\upsilon}-1}{2}\,\frac{p^{2(w-\upsilon)-1}(p-1)}{2} + p^{\upsilon}\sum_{i\in I'}\langle \nu' i^{-1}\rangle'.$$

Therefore (28) gives

$$(-1)^{\sum_{i\in I}\langle \nu i^{-1}\rangle} = \left(\frac{-1}{p}\right)^{\upsilon}(-1)^{\sum_{i\in I'}\langle \nu' i^{-1}\rangle'}.$$

Applying (27) with I replaced by I', we conclude that

$$(-1)^{\sum_{i\in I}\langle \nu i^{-1}\rangle} = -\left(\frac{2\nu'}{p}\right)\left(\frac{-1}{p}\right)^{\upsilon+1}. \tag{29}$$

Now take $w = n$, so that I is the set of $i \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ such that $1 \le \langle i \rangle \le (p^n - 1)/2$. The integer k defined in §5 is the cardinality of $H \cap I$, with H as in §5. Equivalently, k is the number of elements $i \in I$ such that

$$\langle ai^{-1} \rangle + \langle bi^{-1} \rangle + \langle ci^{-1} \rangle = p^n. \tag{30}$$

PROPOSITION 4.

$$(-1)^k = -\left(\frac{2a'b'c'}{p}\right)\left(\frac{-1}{p}\right)^{v_p(abc)+1}$$

Proof. We have

$$k = \sum_{i \in I}\left(2 - \frac{\langle ai^{-1} \rangle + \langle bi^{-1} \rangle + \langle ci^{-1} \rangle}{p^n}\right),$$

the summand being 1 or 0 according as i does or does not satisfy (30). Hence the proposition follows from (29).

7. The conductor

Next we come to the formula for f:

PROPOSITION 5 (Coleman and McCallum). (1) *Suppose that $p \nmid abc$. Put*

$$u = v_p\left((a^a b^b c^c)^{p-1} - 1\right).$$

Then

$$f = \begin{cases} 2p^{n-u}, & \text{if } u \le n, \\ 1, & \text{if } u > n. \end{cases}$$

(2) *Suppose that $p | abc$. Put*

$$u = v_p(abc).$$

Then

$$f = \begin{cases} 2p^{n-u}, & \text{if } u \not\equiv 1 \pmod{p}, \\ (p+1)p^{n-u-1}, & \text{if } u \equiv 1 \pmod{p}. \end{cases}$$

The basic reference for these assertions is Cor. 6.1.1 of [1], but we add the following remarks:

—Under our hypotheses, the parameter t of [1] is simply $v_p(abc)$. Hence the condition $t = v_p((a, b, c, m))$ in [1] is equivalent to our condition $p \nmid abc$.

—In the statement of Cor. 6.1.1, the definition of u in the case $t > v_p((a, b, c, m))$ is incorrect. The correct definition is that $u = t = v_p(s) + 1$ (notation as in [1]).

—Under our hypotheses, if $p|abc$ then $u \leq n - 1$.

—Finally, if $p = 3$ and $3|abc$ then Cor. 6.1.1 is not immediately applicable because of a restriction in the hypothesis of Theorem 5.3. Nevertheless, the proof of Cor. 6.1.1 goes through if we appeal to Theorem 7.2 in place of Theorem 5.3. In applying Theorem 7.2 we need only observe that if $v_3(abc) = n - 1$, then the conductor of the Hilbert symbol $(a^a b^b c^c(1 + x3^n), *)_{3^n}$ (where $x \in \mathbf{Z}^\times$) coincides with that of $(a^a b^b c^c, *)_{3^n}$. Indeed, the conductor-exponent of $(1 + 3^n, *)_{3^n}$ is 2 by Theorem 6.1, while $2p^{n-u} > 2$ and $(p + 1)p^{n-u-1} > 2$ even for $p = 3$ and $u = n - 1$.

8. Coleman's explicit reciprocity law

Recall that for $f > 1$ we have defined an invertible residue class l modulo p by the requirement

$$\chi_{\mathfrak{p}}\left(1 + \pi_K^{f-1}\right) = e^{2\pi i l/p},$$

where $\pi_K = \zeta - \zeta^{-1}$ and $\zeta = e^{2\pi i/p^n}$.

Proposition 6. *Assume that $f > 1$.*

(1) *If $p \nmid abc$ put*

$$u = v_p\left(\left(a^a b^b c^c\right)^{p-1} - 1\right) \quad \textit{and} \quad d = \frac{\left(a^b b^b c^c\right)^{p-1} - 1}{p^u}.$$

Then

$$l \equiv 2d \pmod{p}.$$

(2) *If $p|abc$ put $u = v_p(abc)$ and*

$$d = \begin{cases} \dfrac{v_p(a^a b^b c^c)}{u}(1 - u), & \textit{if } u \not\equiv 1 \pmod{p}, \\ -v_p(a^a b^b c^c), & \textit{if } u \equiv 1 \pmod{p}. \end{cases}$$

Then $d' = d/p^u$ and

$$l \equiv \begin{cases} 2d' \pmod{p}, & \textit{if } u \not\equiv 1 \pmod{p}, \\ -2d' \pmod{p}, & \textit{if } u \equiv 1 \pmod{p}. \end{cases}$$

Proof. For $1 \leq m \leq n$ put

$$\zeta_m = \zeta^{p^{n-m}}$$

and

$$\pi_m = 1 - \zeta_m.$$

In particular, $\zeta_n = \zeta$ and $\pi_n = 1 - \zeta$. Hence $\pi_K = -(1 + \zeta^{-1})\pi_n$, so that

$$\pi_K^{f-1} \equiv (-2)^{f-1}\pi_n^{f-1} \pmod{\mathfrak{p}^f}.$$

Equivalently,

$$\pi_K^{f-1} \equiv -2\pi_n^{f-1} \pmod{\mathfrak{p}^f},$$

because $f \equiv 2 \pmod{p-1}$ in all cases where $f > 1$ (see Prop. 5). Therefore

$$\chi_{\mathfrak{p}}\left(1 + \pi_n^{f-1}\right)^{-2} = e^{2\pi i l/p}. \tag{31}$$

By Theorems 5.3 and 7.2 of [1], the left-hand side of (31) is $(a^a b^b c^c, 1 + \pi_n^{f-1})_{p^n}^{-2}$. Hence if we write

$$a^b b^b c^c = \epsilon p^r (1-p)^s \tag{32}$$

with $r \in \mathbf{Z}$, ε, $s \in \mathbf{Z}_p$, and $\varepsilon^{p-1} = 1$, then (31) becomes

$$\left(p^r(1-p)^s, 1 + \pi_n^{f-1}\right)_{p^n}^{-2} = e^{2\pi i l/p}. \tag{33}$$

By assumption, $f > 1$. Hence either $f = 2$ or $f > 2$. We consider these two cases separately. If $f = 2$ then by Prop. 5, $p \nmid abc$ and $u = n$, whence $r = 0$ and $sp \equiv dp^n \pmod{p^{n+1}}$. Thus (33) becomes

$$\left((1-p)^{dp^{n-1}}, 1 + \pi_n\right)_{p^n}^{-2} = e^{2\pi i l/p}. \tag{34}$$

On the other hand,

$$\left((1-p)^{p^{n-1}}, 1 + \pi_n\right)_{p^n} = \left(1 - p, 2^{p^{n-1}} - \zeta_1\right)_p = e^{-2\pi i/p} \tag{35}$$

by one of the explicit reciprocity laws of Artin-Hasse. Comparing (34) and (35) we find $l \equiv 2d \pmod{p}$, as claimed.

Henceforth we suppose that $f > 2$. To prepare for the use of Coleman's explicit reciprocity law, let $g_1, g_2 \in \mathbf{Z}_p[[x]]$ be the power series defined on p.

90 of [1], so that

$$g_1(\pi_n) = p,$$

and

$$g_2(\pi_n) = 1 - p.$$

Put

$$g_0 = \begin{cases} g_1^r g_2^s, & \text{if } v_p(s) + 1 = v_p(r), \\ g_2^s, & \text{if } v_p(s) + 1 < v_p(r). \end{cases} \tag{36}$$

The two cases indicated are the only possible ones, because $v_p(s) + 1 \leq v_p(r)$ always. (See the proof of Cor. 6.1.1 of [1]. If $p \nmid abc$ then we follow the convention that $v_p(0) = \infty$.) In both cases,

$$\left(g_0(\pi_n), 1 + \pi_n^{f-1}\right)_{p^n} = \left(p^r(1-p)^s, 1 + \pi_n^{f-1}\right)_{p^n}$$

and the conductor-exponent of $(g_0(\pi_n), *)_{p^n}$ is f ([1], Theorem 6.1).

Now let us apply Coleman's reciprocity law as stated on p. 89 of [1]: we have

$$\left(p^r(1-p)^s, 1 + \pi_n^{f-1}\right)_{p^n} = \left(g_0(\pi_n), 1 + \pi_n^{f-1}\right)_{p^n} = \zeta^{-w} \tag{37}$$

with

$$w = \int_n x^{f-1} \frac{Dg_0}{g_0}(x)\, dx, \tag{38}$$

where the integral and the operator D are as in [1]. In the preceding formula we have written x^{f-1} where a literal quotation of [1] would require

$$\log(1 + x^{f-1}) - \frac{1}{p}\log\left(1 + \left(1 - (1-x)^p\right)^{f-1}\right).$$

To justify the replacement, recall that for $m \geq 2$ the map

$$\Lambda(h) = \log h - \frac{1}{p}\log h\left(1 - (1-x)^p\right)$$

defines an isomorphism

$$\Lambda : 1 + x^m \mathbf{Z}_p[[x]] \to x^m \mathbf{Z}_p[[x]]$$

([1], p. 89). Therefore

$$\Lambda(1+x^{f-1}) \equiv (1-p^{f-2})x^{f-1} \mod \Lambda\bigl(1+x^f\mathbf{Z}_p[[x]]\bigr).$$

Since $(g_0(\pi_n), *)_{p^n}$ has conductor-exponent f, a literal application of Coleman's reciprocity law gives

$$\bigl(g_0(\pi_n), 1+\pi_n^{f-1}\bigr)_{p^n} = \zeta^{-(1-p^{f-2})w}$$

with w as in (38). But since the left-hand side is *a priori* a p-th root of unity, the factor $1-p^{f-2}$ on the right is extraneous, and (37) follows.

Given nonzero elements α and β of a p-adic field, write $\alpha \sim \beta$ if $\alpha-\beta$ has a strictly larger valuation than either α or β. We denote by $[\alpha]$ an arbitrary member of the equivalence class of α under $\sim$. Let T_m denote the trace from $\mathbf{Q}_p(\zeta_m)$ to $\mathbf{Q}_p$, and let us henceforth take

$$m = n - u + 1, \tag{39}$$

so that under our assumptions $m \geq 2$. We claim that for $h(x) \in x^{f-1}\mathbf{Z}_p[[x]]$,

$$\int_n h\frac{Dg_0}{g_0} \equiv p^{-n}T_m\left(h(\pi_m)\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \quad (\text{mod } p^n). \tag{40}$$

To justify this claim, we consider three cases. First suppose that $v_p(s)+1 < v_p(r)$. Then $g_0 = g_2^s$, and Cor. 6.7.1 of [1] shows that the hypotheses of Cor. 6.3.1 of [1] are satisfied with $g = g_0$, $j = m$, and $k_j = f$. Therefore (40) follows from the last displayed formula in the proof of Cor. 6.3.1, because the term $Dg/g(\pi_j)$ appearing in that formula can be replaced by any element of its equivalence class.

Next suppose that $v_p(s)+1 = v_p(r)$ and that $u \not\equiv 1 \pmod p$. Then $(p^r, *)_{p^n}$ and $((1-p)^s, *)_{p^n}$ have the same conductor-exponent as $(p^r(1-p)^s, *)_{p^n}$, namely f. Appealing to Cors. 6.5.1 and 6.7.1 and to the displayed formula mentioned above, we deduce that (40) holds with g_0 replaced by either g_1^r or g_2^s. Hence (40) holds for g_0 itself by linearity.

Finally, suppose that $v_p(s)+1 = v_p(r)$ but that $u \equiv 1 \pmod p$. The analogue of Cors. 6.5.1 and 6.7.1 in this case, while not stated explicitly in [1], is that

$$v_{\pi_i}\bigl(p^{2n-i}\pi_1\bigr) - v_{\pi i}\left(\frac{Dg_0}{g_0}(\pi_i)\right) = p^{i-2}\bigl(p(1+(p-1)(m-i))+1\bigr) \tag{41}$$

and that the right-hand side attains its maximum solely when $i = n - u + 1$.

(Here v_{π_i} denotes order at π_i, and the verification of (41) requires Lemmas 6.5 and 6.7 of [1].) Granting these facts, we deduce (40) as before.

Now let us combine (38) and (40). We obtain the congruence

$$w \equiv p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \pmod{p^n}.$$

On the other hand, a comparison of (33) and (37) shows that

$$2w \equiv lp^{n-1} \pmod{p^n}.$$

Together, the preceding two congruences give

$$2p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \equiv lp^{n-1} \pmod{p^n},$$

so that the following lemma will complete the proof:

Lemma. (1) *If $p \nmid abc$, then*

$$p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \equiv dp^{n-1} \pmod{p^n}.$$

(2) *If $p \mid abc$, then*

$$p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \equiv \begin{cases} dp^{n-u-1} \pmod{p^n}, & \text{if } u \not\equiv 1 \pmod{p}, \\ -dp^{n-u-1} \pmod{p^n}, & \text{if } u \equiv 1 \pmod{p}. \end{cases}$$

Proof. We prove the lemma in three steps.

Step 1. $\pi_m^{p^{m-1}}/\pi_1 \equiv \pi_m^{p^{m-2}}/\pi_2 \equiv 1 \pmod{\pi_m}$

Proof. We have

$$\pi_1 = \prod_\nu (1 - \zeta_m^\nu),$$

where ν runs over integers mod p^m which are congruent to 1 mod p. Therefore

$$\pi_1/\pi_m^{p^{m-1}} = \prod_\nu (1 + \zeta_m + \cdots + \zeta_m^{\nu-1}).$$

It follows that

$$\pi_1/\pi_m^{p^{m-1}} \equiv \prod_\nu \nu \equiv 1 \pmod{\pi_m},$$

which is one of the desired congruences. The other follows by a similar argument.

Step 2. $T_m(\pi_1/\pi_m) \equiv -p^{m-1} \pmod{p^m}$

Proof. We have

$$\pi_1/\pi_m = \left(1 - \zeta_m^{p^{m-1}}\right)\big/(1-\zeta_m) = 1 + \zeta_m + \cdots + \zeta_m^{p^{m-1}-1},$$

and each term in the sum but the first is a root of unity of order divisible by p^2. Hence all terms but the first have trace 0, and

$$T_m(\pi_1/\pi_m) = (p-1)p^{m-1}.$$

Step 3. *Proof of the lemma.* (1) Suppose first that $p \nmid abc$. In this case $f = 2p^{m-1}$ (Prop. 5, formula (39)), and we may take $[Dg_0/g_0(\pi_m)] = -sp^n/\pi_1$ by Lemma 6.7 of [1]. (Note that there is a sign error in the statement of Lemma 6.7, which arises in the course of the calculation at the bottom of p. 93 of [1]: $D([p^n])$ is $-p^n(1-x)^{p^n}$, not $p^n(1-x)^{p^n}$.) Thus

(42)
$$p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) = -sp^mT_m\left(\left(\pi_1p^{-m}\right)\left(\pi_m^{-1}\right)\left(\pi_m^{p^{m-1}}/\pi_1\right)^2\right).$$

But π_1p^{-m} generates the inverse of the different ideal of $\mathbf{Q}_p(\zeta_m)$. Hence Step 1 gives

$$p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \equiv -sT_m(\pi_1/\pi_m) \pmod{sp^m}. \tag{43}$$

Then Step 2 gives

$$p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \equiv sp^{m-1} \pmod{sp^m}. \tag{44}$$

This is the desired congruence, because $s \equiv dp^{u-1} \pmod{p^u}$ (immediate from (32)) and $m = n - u + 1$ (formula (39)).

(2) Now suppose that $p|abc$, and assume to begin with that $u \not\equiv 1 \pmod p$. Then $f = 2p^{m-1}$, and Lemmas 6.5 and 6.7 of [1] show that we may take

$$[Dg_0/g_0(\pi_m)] = -(s - r/p)p^n/\pi_1.$$

(We again note a sign error: in the fourth line on p. 91, $D[a]$ should be $-a(1-x)^a$, not $a(1-x)^a$.) This choice of $[Dg_0/g_0(\pi_m)]$ is valid even if $g_0 = g_2^s$, for then $v_p(r/p) > v_p(s)$. Thus formulas (42), (43), and (44) still hold with s replaced by $s - r/p$ (note that r/p is an integer). Now the last paragraph in the proof of Cor. 6.1.1 of [1] shows that $v_p(s - r/p) = u - 1$ and that $s - r/p \equiv d/p \pmod{p^u}$. From these assertions we obtain the desired congruence, because $n - m - u = -1$.

Next we assume that $u \equiv 1 \pmod{p}$. Then $f = (p+1)p^{m-2}$, and Lemmas 6.5 and 6.7 (corrected as above) permit us to take $[Dg_0/g_0(\pi_m)] = -sp^n/\pi_2$. The analogue of (42) is therefore

$$\begin{aligned} p^{-n}T_m\left(\pi_m^{f-1}\left[\frac{Dg_0}{g_0}(\pi_m)\right]\right) \\ = -sp^mT_m\Big((\pi_1 p^{-m})(\pi_m^{-1})\big(\pi_m^{p^{m-1}}/\pi_1\big)\big(\pi_m^{p^{m-2}}/\pi_2\big)\Big), \end{aligned}$$

and (43) and (44) hold without change. Now the last paragraph in the proof of Cor. 6.1.1 shows that $v_p(s) = u - 1$ and also that $s \equiv r/p \pmod{p^u}$. Since $r = v_p(a^a b^b c^c) = -d$, the desired congruence follows as before.

The proof of the lemma yields the "more nearly uniform" definition of d' mentioned in the introduction. In all cases treated by the lemma, we see that d' is uniquely determined modulo p by the condition

$$Dg_0/g_0(\pi_m) \sim (-1)^{\xi} d' p^{*}/\pi_{\xi},$$

where $*$ is an integer $(= n + u - 1)$ and $\xi = 1$ if $p \nmid abc$ or $u \not\equiv 1 \pmod{p}$ and $\xi = 2$ otherwise.

9. Proof of the theorem

This is just a matter of substituting the formulas for $(-1)^k$, f, and (l/p) given by Props. 4, 5, and 6 respectively into the expression for $W(\chi)$ given by Prop. 3. We draw the reader's attention to the following points:

—The condition "$f = 1$" is equivalent to "$p \nmid abc$ and $u > n$".

—If $p \nmid abc$ and $u \leq n$, or if $p \mid abc$ and $u \not\equiv 1 \pmod{p}$, then $f/2$ is odd.

—If $p \mid abc$ and $u \equiv 1 \pmod{p}$, then $f/2$ is even or odd according as $p \equiv 3 \pmod{4}$ or $p \equiv 1 \pmod{4}$. Thus in both cases,

$$\left(\frac{-1}{p}\right)^{f/2} = 1.$$

We conclude with a remark pertaining to the formula for $W(\chi)$ obtained in [3] in the case $n = 1$. While the earlier formula may appear to be different from ours, the reader can verify that the two formulas are consistent by applying Gauss's Lemma and an identity of Lerch (see [4], p. 64, or [5], p. 474). In the special case of the triple $(a, b, c) = (1, 1, -2)$, the verification is in effect already carried out in [3] (p. 218).

References

1. R. Coleman and W. McCallum, *Stable reduction of Fermat curves and Jacobi sum Hecke characters*, J. Reine Angew. Math., vol. 385 (1988), pp. 41–101.
2. P. Deligne, "Les constantes des équations fonctionelles des fonctions *L*" in *Modular Functions of One Variable, II*, Lecture Notes in Math., vol. 349, Springer-Verlag, New York, 1973.
3. B.H. Gross and D.E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math., vol. 44 (1978), pp. 201–224.
4. H. Hasse, *Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus*, Abhand. der Deut. Akad. der Wissen. zu Berlin, 1955.
5. M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1} - 1)/p = q(a)$, *Math. Ann.*, vol. 60 (1905), pp. 471–490.
6. D.E. Rohrlich, *Root numbers of Hecke L-functions of CM fields*, Amer. J. Math., vol. 104 (1982), pp. 517–543.
7. ______, *Jacobi sums and explicit reciprocity laws*, Compositio Math., vol. 60 (1986), pp. 97–114.
8. A. Weil, *Jacobi sums as Grössencharaktere*, Trans. Amer. Math. Soc., vol. 73 (1952), pp. 487–495.

Boston University
Boston, Massachusetts