On Jacobi Sum Hecke Characters Ramified only at 2

DESPINA T. PRAPADEVSSI

Department of Mathematics, Diablo Valley College, Pleasant Hill, California 94523

Communicated by K. A. Ribet

Received August 23, 1989; revised April 24, 1990

Let $K$ be the cyclotomic field of the $m$th roots of unity in some fixed algebraic closure of $\mathbb{Q}$. Weil has shown in [Jacobi sums as Großencharaktere, Trans. Amer. Math. Soc. 73 (1952), 487-495] that Jacobi sums induce Hecke characters on $K$ modulo $m^2$, or equivalently homomorphisms of the idele class group of $K$ into $K^*$. Given such a Hecke character $\rho$, we then obtain for every place $p$ of $K$ a continuous homomorphism $\rho_p$ (the local component of $\rho$ at $p$) from $(K_p)^*$ into $K^*$. When $p$ does not divide $m$, $\rho_p$ is completely determined. When $p$ divides $m$ the determination of $\rho_p$ is much more difficult. Coleman and McCallum in [Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. Reine Angew. Math. 385 (1988), 41-101] have given formulas and computed the conductors of the local components of $\rho$ at $p$ for $p|m$ and $m$ odd. Hasse, in [Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abh. Deut. Akad. Wiss. Berlin Kl. Math. Natur. 1954 4 (1955)] has computed the local component and the conductor when $m$ is prime, while in [C. Jensen, Über die Führer einer Klasse Hecke-Groessencharaktere, Math. Scand. 8 (1960), 81-96; D. Rohrlich, Jacobi sums and explicit reciprocity laws, Compositio Math. 60 (1986), 97-110; C.-G. Schmidt, Über die Führer von Gauss'schen Summen als Großencharaktere, J. Number Theory 12, No. 3 (1980), 283-310] the authors have given estimates and in some cases have determined the conductor of the local component. Here we deal with the case where $m = 2^n$ and we give an explicit formula for the local component in terms of Hilbert symbols, similar to the one in [R. Coleman and W. McCallum, Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. Reine Angew. Math. 385 (1988), 41-101]. In [D. Prapavessi, On the conductor of 2-adic Hilbert norm residue symbols, to appear in J. Algebra] we use this result to compute the conductor of $\rho$ when $m = 2^n$.

1. Introduction

Let $n$ be a positive integer, let $m = 2^n$, let $\mu_m$ be the group of the $m$th roots of unity in $\mathbb{Q}$, a fixed algebraic closure of $\mathbb{Q}$, and let $K = \mathbb{Q}(\mu_m)$. Let $O_K$ denote the ring of integers of $K$, $p$ a prime ideal of $O_K$, $F_p$ the residue field of $K$ at $p$, $q$ the order of $F_p$, and $K_p$ the completion of $K$ at $p$. Let $\lambda$ be the prime ideal above 2 in $K$ and let $I_m$ be the group of fractional ideals of $K$, coprime with $\lambda$. Let $N^m$ denote the norm from $K_\lambda$ to $\mathbb{Q}_2$. 0022-314X/91 $3.00

Copyright © 1991 by Academic Press, Inc.
All rights of reproduction in any form reserved.
For \( p \neq \lambda \), and for any \( x \in O_K, x \notin p \), let \((x/p)_m\) be the power residue symbol of \( K \); that is \((x/p)_m\) is the unique \( m \)th root of unity in \( K \) characterized by

\[
\left( \frac{x}{p} \right)_m \equiv x^{t_q - 1/m} \mod p.
\]

(For more details on the power residue symbol, see [1, ex. 1].)

Consequently, for any \( l \in \mathbb{Z}, (x/p)_m \) is a multiplicative character of \( F_p \). We denote by \( G_{l(m)}(p) \) the Gauss sum of \( F_p \) for this character, defined as follows:

Let \( p = \text{char } F_p \), let \( s_p \) be a fixed primitive \( p \)th root of 1 in \( \bar{Q} \), and let \( \text{Tr} \) denote the trace from \( F_p \) to the field with \( p \) elements. Let \( \psi_p : F_p \to \mu_p \) be the additive character of \( F_p \) given by \( \psi_p(x) = e^{\text{Tr}(x)} \). Then set

\[
G_{l(m)}(p) = -\sum_{x \in F_p} \left( \frac{x}{p} \right)_m^{l/m} \psi_p(x).
\]

Given any \( l \)-tuple of non-zero integers \( d = (d_i) \), \( i = 1 \to l \) such that \( \sum_i (d_i) = 0 \), we obtain a Hecke character \( \rho_{d}^{l(m)} \) over \( K \) modulo \( m^l \), by defining

\[
\rho_{d}^{l(m)}(p) = J_{d}^{(m)}(p),
\]

for prime ideals \( p \in \mathfrak{I}_m \), and extending multiplicatively to \( \mathfrak{I}_m \), where

\[
J_{d}^{(m)}(p) = \frac{1}{q} \prod_{i=1}^{l} G_{d_i}^{(m)}(p).
\]

Weil, in [11], has shown that \( \rho_{d}^{l(m)} \) is a Hecke character of weight 1 over \( K \) and is defined modulo \( m^2 \). That is, for \( s \in O_K, s \equiv 1 \mod m^2 \), if \( (s) \) denotes the principal ideal of \( O_K \) generated by \( s \) we have that

\[
\rho_{d}^{l(m)}((s)) = s^{\Phi_d},
\]

where \( \Phi_d \in \mathbb{Z}[\text{Gal}(K/Q)] \), is given by

\[
\Phi_d = \sum_{\sigma \in \mathbb{Z}} \left( \sum_{i=1}^{l} \left\lfloor \frac{d_it}{m} \right\rfloor - 1 \right) (\sigma_i)^{-1}.
\]

(Here \( \sum' \) denotes summation over indices prime to \( m \), and for \( r \in R \), \( [r] = r - [r] \) is the “fractional” part of \( r \), \( \{r\} \in [0, 1] \); \( \sigma_r \) is the automorphism of \( K \) over \( Q \) given by \( \zeta^{\sigma_r} = \zeta^r \) for \( \zeta \in \mu_m \).)

Let \( J_K \) denote the group of the finite idèles of \( K \). Then \( \rho_{d}^{l(m)} \) induces a unique continuous character \( \rho_{d}^{l(m)} \) on \( J_K \),

\[
\rho_{d}^{l(m)} : J_K \to K
\]
characterized by the following properties:

(i) \( \rho_d^{(m)}(x) = \rho_d^{(m)}((x)^i) \) if \( x \in J^i_K \)

(ii) \( \rho_d^{(m)}(x) = x^{p_d} \) if \( x \in K^* \subseteq J_K \).

For any finite prime \( p \) of \( K \), we let \( \rho_{d,p}^{(m)} \) be the continuous character \( K^*_p \rightarrow K \) obtained by restricting \( \rho_d^{(m)} \) to the \( p \)th component. We call it the local component at \( p \). When \( p \not= \lambda \), (ii) implies

\[
\rho_{d,\lambda}^{(m)}(x) = \frac{x^{p_d}}{\prod_{p \neq \lambda} (J_d^{(m)}(p))^{\text{ord}_p(x)}}. \tag{1.2}
\]

Let \( U_{\lambda} \) denote the group of units of \( \mathbf{Z}_2[[\mu_m]] \). Then as Weil [11] has shown, it is a consequence of Stickelberger's theorem on the prime decomposition of the Gauss sums, that \( \rho_{d,\lambda}^{(m)}(x) \in \mu_m \) for all \( x \in U_{\lambda} \cap K^* \), and by continuity, for all \( x \in U_{\lambda} \). Indeed we have

\[
(G_1^{(m)}(p))^m = p^{m\theta_m - i},
\]

where \( \theta_m \in \mathbf{Z}[\text{Gal}(K/Q)] \) is the Stickelberger element

\[
\theta_m = \sum_{t \equiv i \mod m} \left\{ \frac{t}{m} \right\} \sigma_i^{-1}. \tag{1.3}
\]

Since

\[
\sigma_{-1} \cdot \theta_m = \sum_{t \equiv i \mod m} \left\{ \frac{lt}{m} \right\} (\sigma_{-1})^{-1}, \tag{1.4}
\]

we obtain the prime decomposition of the Jacobi sums,

\[
(J_d^{(m)}(p)) = p^{\Phi_d}.
\]

(Observe that \( \Phi_d \) has integer coefficients since \( \sum_i d_i = 0 \).

Therefore for any ideal \( \eta \in I_m \), we have

\[
(\rho_d^{I_m}(\eta)) = \eta^{\Phi_d}.
\]

When \( \eta \) is a principal ideal \( \eta = (s) \), \( (\rho_d^{I_m}(s)) \cdot s^{-\Phi_d} \) is a unit of \( K \) all of whose conjugates have absolute value 1, and therefore it is a root of unity in \( K \). (For more details on this, see [11, 12].)

So to determine \( \rho_d^{(m)} \) completely, we need to determine \( \rho_{d,\lambda}^{(m)}(U_{\lambda}) \). The\(^1\) J^i_K denotes the subgroup of \( J_K \) consisting of the idèles with value 1 at the \( i \)th component and \((x)^i \in I_i \) is the fractional ideal of \( K \) associated with \( x \in J^i_K \).
really significant ones among these characters are those obtained from $d$ of length 3, since all the others can be expressed in terms of them. (When $d$ has length 2 the associated character is trivial, since $\rho^{(m)}_{a, b, c, r}(p) = (-1/p)^d q$.)

In this paper, we discuss exclusively Hecke characters of $K$ associated to $(a, b, c)$, with $a = 2'a', 1 \leq r \leq n - 1$, and $a', b, c$ odd. For $x \in U_\lambda$, we will express $\rho^{(m)}_{a, b, c, r}(x)$ in terms of the Hilbert symbol $(,)_m$. We briefly recall the definition of the Hilbert symbol,

$$(,)_m : K^*_\lambda \times K^*_\lambda \rightarrow \mu_m$$

$$(x, y)_m = \frac{(x^{1/m})^{\phi_\lambda(y)}}{x^{1/m}},$$

where $\phi_\lambda(y) \in \text{Gal}(K_\lambda(x^{1/m})/K_\lambda)$ denotes the image of $y$ under the Artin map associated with the Kummer extension $K_\lambda(x^{1/m})/K_\lambda$.

We are going to prove:

**Theorem 1.** Let $a, b, c, r, a'$ be as above. Let $w = 1 - 2\eta$, where $\eta$ is a generator of $\mu_4$. Then for $x \in U_\lambda$, we have

$$\rho^{(m)}_{a, b, c, r}(x) = (w^{-m/4}(1 - 4)^r a'^{a'b'b}c', x)_m,$$

where

$$s = \begin{cases} -2^{n-3} & \text{if } r \leq n - 3 \\ 2^{n-3} & \text{if } r = n - 2 \\ 0 & \text{if } r = n - 1 \text{ and } a' = 1 \text{ mod } 4 \\ 2^{n-2} & \text{if } r = n - 1 \text{ and } a' = 3 \text{ mod } 4. \end{cases}$$

(1.5)

The analogous formulas of the local components of $\rho^{(m)}_{a, b, c}$ at $p$ in the cases, where $p | m$ and $m$ is odd, as well as the computation of the conductors, were recently given by Coleman and McCallum in [3], using the special fibre of a stable model of the Fermat curve associated to $\rho^{(m)}_{a, b, c}$. Also Hasse, in [5], has computed the local component and the conductor of $\rho^{(m)}_{a, b, c}$ when $m$ is prime, while in [6], [9, 10], the authors have given estimates and have in special cases determined the conductor of the local component. Also as an application of the Anderson–Ihara theory, Anderson and Coleman have obtained the following result (cf. [4, Thm. 6.4]), which we will use in the proof of Theorem 1:

**Theorem 2.** Let $p \in \mathbb{Z}$ be prime, and let $p$ be the prime above $p$ in $\mathbb{Q}_p(\mu_p^n)$. Let $x \in (1 + p\mathbb{Z}_p[\mu_p^n])$, and suppose that $d = (d_i)_{i=1}^t$ is such that
ON JACOBI SUM HECKE CHARACTERS

165

Then if \( p \) is odd, or if \( p = 2 \) and \( N^m(x) \equiv 1 \mod 2^n + 2 \), we have

\[
\rho_{d, u}^{(m)}(x) = \left( \prod_{i=1}^{l} d_i^{d_i}, x \right)_m,
\]

where \(( , )_m\) is the Hilbert symbol.

The proof of Theorem 1 will be given in the following sequence: First observe that \( N^m \) maps \( U_\lambda \) onto \( 1 + 2^n \mathbb{Z}_2 \): Since \( U_\lambda / \mu_m = 1 + 2\lambda \mathbb{Z}_2[\mu_m] \), we have

\[ N^m(U_\lambda) = N^m(1 + 2\lambda \mathbb{Z}_2[\mu_m]) \subseteq 1 + 2^n \mathbb{Z}_2. \]

But also note that \( \mathbb{Z}_2^*/N^m(U_\lambda) \) has order equal to \( \mathbb{Q}_2^*/N^m(K_\lambda^*) \), which is \( 2^{n-1} \), (cf. [1, chap. VI, Sect. 2.6]), and therefore the inclusion above must be an equality. Hence the group of units \( U_\lambda \) modulo the group of units of norm \( \equiv 1 \mod 2^{n+2} \) is a cyclic group of order 4. In particular, since \( N^m(w) = 5^{2^n-2} \equiv 1 + 2^n \mod 2^{n+1} \), \( w \) is a generator of this quotient group. So given \( x \in U_\lambda \), there exists a unique \( t \in \{0, 1, 2, 3\} \) and a unique \( x_w \in U_\lambda \) with \( N^m(x_w) \equiv 1 \mod 2^{n+2} \), such that

\[ x = w^t \cdot x_w. \tag{1.6} \]

In Sections 2–5 we will show that

\[
\rho_{a, b, c, \lambda}^{(m)}(x_w) = (w^{-m/4}(1 - 4)^s a^a b^b c^c, x_w)_m \tag{1.7}
\]

with \( s \) as in (1.5). To prove (1.7), we will use the Hasse-Davenport relations for Gauss sums to express \( \rho_{a, b, c, \lambda}^{(m)} \) in terms of \( \rho_{1, 1, -2, \lambda}^{(4)} \) and of a tamely ramified character. Then we will evaluate the latter at \( x_w \) using Theorem 2. In Section 2 we reduce to the case where \( x_w \) is a generator of a principal prime ideal \( p \), prime to \( \lambda \). In Section 3 we compute a formula for \( \rho_{1, 1, -2, \lambda}^{(4)} \). In Section 4 we state and prove several lemmas which we use in Section 5 for the computation of \( \rho_{a, b, c, \lambda}^{(m)}(x_w) \). In Section 6, we will show that

\[
\rho_{a, b, c, \lambda}^{(m)}(w) = (w^{-m/4}(1 - 4)^s a^a b^b c^c, w)_m \tag{1.8}
\]

by showing that both sides of (1.8) equal \((-1)^{2^n-2} + 1\). From (1.7) and (1.8), using (1.6) and the bilinearity of the Hilbert symbol, Theorem 1 follows.

I thank Robert Coleman for suggesting the problem to me, for advising me on it, and for kindly discussing it with me during the course of my graduate studies at U. C. Berkeley.
2. SOME REDUCTION STEPS

In this section we will show that it suffices to prove the relation (1.7) of Section 1 for \( x_w \in K^* \), and \( x_w \) a generator of a principal prime ideal \( p \) of \( O_K \). (We identify \( K^* \) with its image in \( K^* \) under the natural inclusion.) This is a consequence of Proposition 3 given below:

**PROPOSITION 3.** Given \( x \in U_\lambda \), there exists a principal prime ideal \( p \) of \( O_K \), with generator \( \pi_x \in O_K \), such that \( \pi_x \equiv x \mod 2^{n+2} \).

**Proof of Proposition 3.** Let \( P_m \) denote the set of principal ideals of \( O_K \) coprime with \( \lambda \). Let \( P_{m,1} \subseteq P_m \) be the subset consisting of ideals generated by \( s \in O_K \), \( s \equiv 1 \mod 2^{n+2} \). Let \( L_K \) and \( H_K \) denote the class fields to \( I_m/P_{m,1} \) and \( I_m/P_m \), respectively. So \( H_K \) is the Hilbert class field to \( K \), and \( H_K \subseteq L_K \), with \( \text{Gal}(L_K/H_K) = P_m/P_{m,1} \). Let \( y \in O_K \) be determined by the congruence \( y \equiv x \mod 2^{n+2} \). By Tchebotarev's density theorem, there exists a prime \( p \) which maps to the same element of \( \text{Gal}(L_K/K) \) with \( (y) \) under the Artin map. Since \( (y) \) is principal, \( p \) actually maps into \( P \), therefore \( p \) is principal. Since then \( p \equiv (y) \mod P_{m,1} \), it follows that there is a generator \( \pi_x \) of \( p \), such that \( \pi_x \equiv y \mod 2^{n+2} \), and therefore \( \pi_x \equiv x \mod 2^{n+2} \) as claimed.

Given \( x \in U_\lambda \) with \( N_{m,1}(x_w) \equiv 1 \mod 2^{n+2} \), let \( \pi_{x_w} \) be as in Proposition 3. It follows that there is \( u \in U_\lambda \) such that \( x_w = \pi_x u^m \), since any unit in \( U_\lambda \) congruent to 1 mod \( 2^{n+2} \) is an \( m \)th power. (One way to see this is as follows: If \( u \equiv 1 \mod 2^{n+2} \mathbb{Z}_m \), there exists \( s \in \mathbb{Z}_m \) such that \( u = (1 - 4)^s \), and then we have that \( s \equiv 0 \mod m \).) Next observe that the Hecke character \( \rho_{a,b,c,\varepsilon}^{(m)} \) and the Hilbert symbol are trivial on \((U_\lambda)^m \). So both sides of (1.7) agree on \( x_w \) and \( \pi_{x_w} \). Also \( N^m \pi_{x_w} = 1 \mod 2^{n+2} \). So it suffices to prove (1.7) for \( \pi_{x_w} \).

For Sections 3 5, \( p \) denotes a fixed principal prime ideal of \( I_m \), \( x_w \in K^* \) is a generator of \( p \), and \( N^m(x_w) \equiv 1 \mod 2^{n+2} \). To simplify the notation we denote the Gauss sum \( G^{(m)}_l(p) \) by \( G_l \) and \( \Phi_{a,b,c} \) by \( \Phi \), unless needed otherwise.

3. THE COMPUTATION OF \( \rho_{1,1,-2,\varepsilon}^{(4)} \)

For this section only, \( K = \mathbb{Q}(\mu_4) \) and \( \lambda = (1 - t) \). Let \( w = (1 - 2t) \), as in the statement of Theorem 1. Note that

\[
\rho_{1,1,-2,\varepsilon}(t) = 1, \quad (3.0)
\]

since \( \Phi_{1,1,-2} = \sigma_1 \). We are going to prove:
PROPOSITION 4. For all $x \in U_2$, $\rho_{1,1,-2,\lambda}^{(4)}(x) = (-w, x)_4$.

Proof of Proposition 4.
We will first show that Proposition 4 holds for any $w \in K$, satisfying (a) and (b) below:

(a) $(w, i)_4 = 1$.
(b) $(w, 1 + \lambda^3 u)_4 = 1$ for all integers $u$ in $K$.

Then we will show that $w = 1 - 2I$ satisfies (a) and (b).

As it was shown in Section 2, we only need to prove Proposition 4 for $x$ a generator of a principal prime ideal $p \neq \lambda$. At first we are going to determine $\rho_{1,1,-2,\lambda}^{(4)}$ for $p \in K^*$ such that:

(i) $\pi$ is a generator of a prime $p$ of $K$, $p \neq \lambda$.
(ii) $\pi \equiv 1 \mod \lambda^3$.

Given any principal prime ideal $p \neq \lambda$ of $K$, such a generator always exists; for, the equivalence classes of $1, i, -1, -i$ are distinct modulo $\lambda^3$ and so given a generator of $p \neq \lambda$ we can multiply it by the appropriate root of unity to obtain $\pi$ satisfying (i) and (ii). For such $\pi$ we are going to prove

$$\rho_{1,1,-2,\lambda}^{(4)}(\pi) = (-1, \pi)_4.$$  

By (1.2) and since $\Phi_{1,1,-2} = \sigma_1$, we have

$$\rho_{1,1,-2,\lambda}^{(4)}(\pi) = \frac{\pi}{J_{1,1,-2}^{(4)}(p)}.  \tag{3.1}$$

By definition,

$$J_{1,1,-2}^{(4)}(p) = -\sum_{x \in \mathcal{F}_p \setminus \{0, 1, \frac{1}{2}\}} \left(\frac{x}{p}\right)_4 \left(\frac{1-x}{p}\right)_4$$

$$= -\left(\frac{1/2}{p}\right)_4^{-2} \sum_{x \in \mathcal{S}} \left(\frac{x}{p}\right)_4 \left(\frac{1-x}{p}\right)_4, \tag{3.2}$$

where $\mathcal{S}$ is a subset of $\mathcal{F}_p - \{0, 1, \frac{1}{2}\}$ containing exactly one element of each pair $(x, 1-x)$. Since $\# \mathcal{S} = (q-3)/2$, then $\# \mathcal{S} \equiv 1 \mod 2$. Since any element of $\mu_4$ is $\equiv 1 \mod \lambda$ we have that $(x/p)_4 ((1-x)/p)_4 \equiv 1 \mod \lambda$, and since $\# \mathcal{S} \equiv 1 \mod 2$,

$$\sum_{x \in \mathcal{S}} \left(\frac{x}{p}\right)_4 \left(\frac{1-x}{p}\right)_4 \equiv 1 \mod \lambda.$$
Also, from the quadratic reciprocity law, we have that \((\frac{1}{2}\mathbf{p})^{2} = (-1)^{(q^2 - 1)/8}\) and therefore (3.2) gives

\[ J_{1, 1, -2}(\mathbf{p}) \equiv (-1)^{(q^2 - 1)/8} + 2 \mod \lambda^3. \tag{3.3} \]

By (3.3) and since \(\pi \equiv 1 \mod \lambda^3\) we conclude

\[ \rho_{1, 1, -2, \varepsilon}(\pi) \equiv \begin{cases} 1 & \text{mod } \lambda^3 \quad \text{if } q \equiv 1 \mod 8 \\ 1 + 2 & \text{mod } \lambda^3 \quad \text{if } q \equiv -3 \mod 8 \end{cases} \]

and since \(\rho_{1, 1, -2, \varepsilon}(\pi) \in \mu_4\), it suffices to determine it modulo \(\lambda^3\). That is we have

\[ \rho_{1, 1, -2, \varepsilon}(\pi) = \begin{cases} 1 & \text{mod } \lambda^3 \quad \text{if } N^4\mathbf{p} \equiv 1 \mod 8 \\ -1 & \text{mod } \lambda^3 \quad \text{if } N^4\mathbf{p} \equiv 5 \mod 8 \end{cases} \]

\[ \equiv (-1)^{(N^4\mathbf{p} - 1)/4} = \left(\frac{-1}{\mathbf{p}}\right)_4 = (-1, \pi)_4. \tag{3.4} \]

Given any \(x \in K^*, x\) a generator at \(\mathbf{p} \neq \lambda\) we have that \(x = t^* \cdot \pi\), where \(t\) is an integer mod 4 and \(\pi \equiv 1 \mod \lambda^3\). So if \(w\) satisfies (a) and (b), by (3.4) and (3.0), we have

\[ \rho_{1, 1, -2, \varepsilon}(x) = (\rho_{1, 1, -2, \varepsilon}(t))^4 \rho_{1, 1, -2, \varepsilon}(\pi) = t^4 \cdot (-1, \pi)_4 = (w, t)^4 \cdot (-1, \pi)_4 \]

\[ = (w, t)^4 \cdot (-1, t)^4 \cdot (w, \pi)_4 \cdot (-1, \pi)_4 = (-w, x)_4. \]

The last equality follows from the bilinearity of the norm residue symbol. We also used the observation that \((-1, t)_4 = 1\) which is easy to see since \((-1, t)_4 = (-1, t)^4 \cdot (t^3, t)_4\) and \((-1, t)_4 = 1\). So \((-1, t)_4 = (t, t)_4^2\) and \((-1, t)_4 = (t, t)_4^3\), therefore \((t, t)_4 = 1\) and hence \((-1, t)_4 = 1\).

It remains to prove that \(w = 1 - 2i\) satisfies (a) and (b), for which we will use some relations between the power and the norm residue symbols (cf. [1, ex. 2]). A direct computation gives (a),

\[ (w, t)_4 = \left(\frac{1}{w}\right)_4 = t^{(N^4w - 1)/4} = t^1 - t. \]

To prove (b) observe first that

\[ (w, 1 + 2(1 - i))_4 = \left(\frac{w}{1 + 2(1 - i)}\right)_4^{-1} \left(\frac{1 + 2(1 - i)}{w}\right)_4 \]

\[ = (-i)^{-1} (-i) = 1, \]
and that since \((1 + 2(1 - i))^t = -1 + 6i \mod 2^t\), we have

\[
(w, (1 + 2(1 - i))^t)_4 = \left( \frac{w}{-1 + 6i} \right)_4 \left( \frac{-1 + 6i}{w} \right)_4
\]

\[
= (-1)^{-1} (-1) = 1.
\]

Then for any \(\beta = 1 + \lambda^2 u\), where \(u\) is an integer in \(K\), set \(\beta = \{1 + 2(1 - i)^k\}^k\) with \(k = \log(1 + \lambda^2 u)/\log(1 + 2(1 - i))\), where \(\log\) denotes the Iwasawa logarithm (cf. [7, Chap. 4, Sect. 3]). So \(k \in \mathbb{Z}_2[i]^*\). Then if \(\{k_n\}\) denotes a sequence in \(\mathbb{Z}[i]\) converging to \(k\), with \(k_n = a_n + ib_n\), \(a_n, b_n \in \mathbb{Z}\), the sequence \(\{1 + 2(1 - i)^{k_n}\}\) converges to \(\beta\). From the linearity of the symbol it follows that

\[
(w, \{1 + 2(1 - i)^{k_n}\})_4 = \left(\{w, 1 + 2(1 - i)\}_4\right)^{a_n} \left(\{w, -1 + 6i\}_4\right)^{b_n} = 1.
\]

From the continuity of the symbol we have that \((w, \beta) = 1\). This completes the proof of (b) and hence Proposition 4.

### 4. Five Lemmas

In this section we are going to state and prove five lemmas that we will need in the computation of \(\rho_{a,b,c,d}(x_w)\) which is given in Section 5. The first three (Lemmas 5, 6, and 7), will be used to express the Gauss sum \(G_a\) in \(J_{a,b,c,d}(p)\) in terms of Gauss sums of odd powers of the power residue symbol. We will need two Hasse-Davenport relations:

The first relates the Gauss sums \(G(\chi)\) arising from the characters \(\chi\) of \(F_p^*\) of order \(l\) and an arbitrary character \(\psi\) of \(F_p^*\) (cf. [7, Chap. II, Thm. 10.1]),

\[
\prod_{\chi = 1} G(\chi \psi) = \psi(1^l) G(\psi') \prod_{\chi = 1} G(\chi). \tag{4.1}
\]

The second relates Gauss sums of finite extensions of finite fields (cf. 7, Chap. I, Thm. 5.1)]. Let \(E/F\) be such an extension, and let \(\chi\) be a character of \(F^*\), \(G^F(\chi)\) the Gauss sum corresponding to \(\chi\). Then

\[
G^F(\chi \circ N_{E/F}^E) = (G^F(\chi))^{[E:F]}, \tag{4.2}
\]

where \(N_{E/F}^E\) is the norm for \(E/F\).

**Lemma 5.** With \(m, a, c, a', r\), as in the statement of Theorem 1 and \(q = N^m p\) we have

\[
G_a = \left( \frac{2^r}{p} \right)^a q^{-\frac{1}{2} \left( \frac{2^r - 1}{m} \right)} \prod_{k=1}^{2^r - 1} \frac{1}{G_{a' + km/2^r} G_{a' - km/2^r}} \frac{1}{G_a G_{a' - m/2}}.
\]
Proof of Lemmas 5. Since \( a = 2'a' \), the character \((x/p)^a_m\) of \( F^*_p \) is the \( 2' \)th power of \((x/p)^a_m\). We apply (4.1) with \( \psi(x) = (x/p)^a_m \) and \( l = 2' \), and we obtain

\[
G_a = \left( \frac{2'}{p} \right)_m \frac{1}{\prod_{r' = 0(m)} G_{a' + r'}} \prod_{r' = 0(m)} G_r.
\]

Observe now that the denominator is the product of \( G_0 \), \( G_{m/2} \), and \( 2' - 1 \) pairs of Gauss sums of conjugate characters. Since \( G_0 = 1 \), \( G_{m/2} = G_{-m/2} \), and \( G_r G_{-r'} = (-1/p)_m q \), the denominator equals \( q^{2' - 1} G_{-m/2} \). (\( t \) is even for all terms in the product, so \((-1/p)_m = 1\).)

**Lemma 6.** Let \( x \) be a uniformizer at a prime ideal \( p \neq \lambda \) in \( K \) and let \( q = N^m p \). Let \( N^m_4 \) denote the norm for \( K/Q(\mu_4) \) and \( w = 1 - 2t \). Then we have

\[
G_{m/4} G_{m/4} G_{-m/2} = q N^m_4(x)(-w)^{-m/4}, x)_m.
\]

Proof of Lemma 6. Let \( p_4 = p \cap Q(\mu_4) \) denote the prime ideal lying under \( p \) in \( Q(\mu_4) \). Let \( F_{p_4} \) be the residue field at \( p_4 \) and \( p = \text{char} F_4 = \text{char} F_{p_4} \). Let \( q_4 = N^4_4 \) be the order of \( F_{p_4} \) and let \( f \) denote the degree of the extension \( F_p/F_{p_4} \), that is \( (q_4)^f = q \). To prove Lemma 6, we will show that

\[
G_{m/4} G_{m/4} G_{-m/2} = (G_1^{(4)} G_1^{(4)} G_{-2}^{(4)})^f,
\]

(4.6.1)

where \( G_1^{(4)} \) is the Gauss sum associated with the character \((x/p)_4^{(1)}\) of \( F_{p_4}^* \), and then we will use Proposition 4 of Section 3. Indeed, observe that

\[
\left( \frac{x}{p} \right)_m^{m/4} = \left( \frac{N_{p_4}^4(x)}{p_4} \right)_4.
\]

Then using (4.2), we have that \( G_{m/2} = (G_1^{(4)})^f \), and similarly \( G_{-m/2} = (G_{-2}^{(4)})^f \). So (4.6.1) follows. Recall now that \( x \) is a uniformizer at \( p \). Using (1.2) and since \( \text{ord}_{p_4}(N_4^m(x)) = f \), we have that

\[
\rho_{1,1,-2,4}(N_4^m(x)) = \frac{(q_4)^f N_4^m(x)}{G_{m/4} G_{m/4} G_{-m/2}} = \frac{q \cdot N_4^m(x)}{G_{m/4} G_{m/4} G_{-m/2}},
\]

(4.6.2)

and using Proposition 4 of Section 3, we also have

\[
\rho_{1,1,-2,4}(N_4^m(x)) = (-w, N_4^m(x))_4 = ((-w)^{-m/4}, x)_m,
\]

(4.6.3)

where the last equality follows from the norm restriction of the Artin map.
for the corresponding extensions. Equating (4.6.2) and (4.6.3), completes the proof of Lemma 6.

**Lemma 7.** Let $m = 2^n$, $n \geq 3$ and $q = N^m p$. Then

$$
(G_{m/4})^2 = q^{1-m/4} \left( \prod_{k=1}^{m/8-1} G_{1+4k} G_{1-4k} \right)^2 G_1 G_{1+m/2} G_{1-m/2}.
$$

**Proof of Lemma 7.** As a special case of Lemma 5 with $a = m/4 = 2^{n-2}$ we obtain

$$
G_{m/4} = \left( \frac{2^n - 2}{p} \right)_{m/4} \frac{1}{q^{n-3}} \left( \prod_{k=1}^{m/8-1} G_{1+4k} G_{1-4k} \right) G_1 G_{1+m/2}. \tag{4.7.1}
$$

We square both sides of (4.7.1) and we use the relations $G_{1+m/2} = G_{1-m/2}$ and $(G_{-m/2})^2 = q$. Also observe that for $n \geq 3$, we have

$$
\left( \frac{2}{p} \right)^{m/2} = \left( i \left( \frac{1-i}{2} \right)^{m/2} \right)_{m/2} = \left( \frac{i}{p} \right)_{m/2} = 1,
$$

since $i$ is a square. Lemma 7 now follows.

Next, we need some computations in the group ring of $\mathrm{Gal}(K/Q)$. Let $\theta_m$ be as in (1.3). For $n \geq 3$ and $l \in \mathbb{Z}$, with $\text{ord}_l(l) = r$, $1 \leq r < n$, we define $\tilde{\omega}_l \in \mathbb{Z}[\mathrm{Gal}(K/Q)]$ by

$$
\tilde{\omega}_l = \sum_{k=-2^{r-1}+1}^{2^{r-1}} \sigma_{-(l-km)/2^r}.
$$

We have:

**Lemma 8.** Let $n \geq 3$, and let $\tilde{\omega} \in \mathbb{Z}[\mathrm{Gal}(K/Q)]$ be given by

$$
\tilde{\omega} = \sigma_\omega - \tilde{\omega}_a - 2\tilde{\omega}_{m/4}.
$$

Let $\Phi = \tilde{\omega} \theta_m$. Then we have that $\Phi = \sum_{t=1}^m \alpha_t \sigma_{-1}^{-1}$, where

$$
\alpha_t = \begin{cases} 
-2^{r-1} - m/4 + 1 & \text{if } t = 1 \mod 4 \\
-2^{r-1} - m/4 & \text{if } t = 3 \mod 4.
\end{cases} \tag{4.8.1}
$$

**Proof of Lemma 8.** The proof results from the following claim:

$$
\tilde{\omega}_l \cdot \theta_m = \sum_{t=1}^m \left( \left\{ \frac{lt}{m} \right\} + 2^{r-1} - \frac{1}{2} \right) \sigma_{-t}^{-1} \tag{4.8.2}
$$
Let us assume (4.8.2) at first. Then using (1.4), we obtain
\[
\tilde{\Phi} = \sum_{t=1}^{m} \left( \frac{at}{m} \right) \sigma^{-1} - \sum_{t=1}^{m} \left( \frac{at}{m} + 2^{r-1} - \frac{1}{2} \right) \sigma^{-1}_t
\]
\[-2 \sum_{t=1}^{m} \left( \left\lfloor \frac{t}{4} \right\rfloor + 2^{r-3} - \frac{1}{2} \right) \sigma^{-1}_t = \sum_{t=1}^{m} \alpha_t \sigma^{-1}_t
\]
with \( \alpha_t \) as in (4.8.1).

It remains to prove (4.8.2). Let \( l' = l/2^r \). Using (1.4) we have
\[
\tilde{\omega}_{l'} \cdot \tilde{\theta}_m = \sum_{t=1}^{m} \left( \sum_{k=1}^{2^r} \left\{ \left( \frac{l'}{m} + \frac{k}{2^r} \right) t \right\} \right) \sigma^{-1}_t
\]
We will show that for any \( t \in (\mathbb{Z}/m\mathbb{Z})^* \), we have
\[
\sum_{k=1}^{2^r} \left\{ \left( \frac{l'}{m} + \frac{k}{2^r} \right) t \right\} = \frac{l't}{m} + 2^{r-1} - \frac{1}{2}
\]
Fix \( t \in (\mathbb{Z}/m\mathbb{Z})^* \). Define \( s \in (\mathbb{Z}/2^r\mathbb{Z})^* \), by \( s = t \mod 2^r \). Then
\[
\sum_{k=1}^{2^r} \left\{ \left( \frac{l'}{m} + \frac{k}{2^r} \right) t \right\} = \sum_{k=1}^{2^r} \left\{ \frac{l't}{m} + \frac{ks}{2^r} \right\} = \sum_{k=1}^{2^r} \left\{ \frac{l't}{m} + \frac{k}{2^r} \right\} \tag{4.8.3}
\]
since multiplication by \( s \) gives a permutation of the elements of \((\mathbb{Z}/2^r\mathbb{Z})^*\).

Let now \( j \in \mathbb{Z}, 0 \leq j < 2^r \), be defined by the inequality
\[
\frac{j}{2^r} \leq \left\{ \frac{l't}{m} \right\} < \frac{j+1}{2^r} \tag{4.8.4}
\]
Then we have
\[
\left\{ \frac{l't}{m} + \frac{k}{2^r} \right\} = \left\{ \frac{l't}{m} + \frac{k}{2^r} \right\} \quad \text{if} \quad 1 \leq k \leq 2^r - (j+1) \tag{4.8.4}
\]
\[
\left\{ \frac{l't}{m} + \frac{k}{2^r} \right\} = \left\{ \frac{l't}{m} + \frac{k}{2^r} \right\} + 2^{r-1} - \frac{1}{2} - j \quad \text{if} \quad 2^r - j \leq k \leq 2^r.
\]
It follows that
\[
\sum_{k=1}^{2^r} \left\{ \frac{l't}{m} + \frac{k}{2^r} \right\} = 2^r \left\{ \frac{l't}{m} \right\} + 2^{r-1} - \frac{1}{2} - j \tag{4.8.5}
\]
Also note that since \( l = 2^r l' \), and \( j/2^r \leq \left\{ l't/m \right\} < (j+1)/2^r \), we have
\[
\frac{j}{2^r} \leq \left\{ \frac{l't}{m} \right\} < \frac{j+1}{2^r}
\]
hence
\[
\left\{ \frac{lt}{m} \right\} = \left\{ \frac{2^r l'}{l} \right\} = 2^r \left\{ \frac{l'}{m} \right\} - j.
\]

This, with (4.8.5) and (4.8.3) completes the proof of (4.8.2), and hence of Lemma 8.

Now let \( \log \) denote the Iwasawa logarithm (cf. [7, Chap. 4, Sect. 3]). For units of \( \mathbb{Z}_2 \) the logarithm has a power series expansion given by
\[
\log(1 + x) = \sum_{t=1}^{\infty} (-1)^{t-1} \frac{x^t}{t}.
\]

This series converges in \( \mathbb{Q}_2 \) provided that \( \text{ord}_2(x) > 1 \). Let \( A \) be given by
\[
A = \prod_{k=1}^{2^{r-1}-1} \left( 1 + \frac{km}{a} \right)^{a' + km/2^r} \cdot \left( 1 - \frac{km}{a} \right)^{a' - km/2^r}
\]
where \( a = 2^r a' \), with \( a' \) odd and \( 2 \leq r \leq n - 1 \). Then the series for \( \log A \) converges. In Section 5, we will use the following lemma:

**Lemma 9.** Let \( m = 2^n, n \geq 3 \). Then we have
\[
\log A = \frac{(-1)^{2^n-r-1}}{a'} 2^{2^r - r - 2^{r-1} - 1} \mod 2^{n+2}.
\]

*Proof of Lemma 9.* We will distinguish two cases, as \( r \leq n - 2 \) or \( r = n - 1 \). In the first case the series for \( \log(1 + km/a) \) already converges in \( \mathbb{Q}_2 \) while when \( r = n - 1 \) the series for \( \log((1 + km/a)^2) \) converges.

**Case (i).** \( r \leq n - 2 \).

To simplify the notation, let
\[
C = \prod_{k=1}^{2^{r-1}-1} \left( 1 + \frac{km}{a} \right)^{1 + km/a} \cdot \left( 1 - \frac{km}{a} \right)^{1 - km/a},
\]
so that
\[
\log A = \log(C^a) = a' \log C.
\]

Using (4.9.1) we find
\[
\log C = \sum_{t=1}^{\infty} \frac{1}{t(2t-1)} \frac{m^{2r} 2^{r-1} - 1}{a^{2t}} \sum_{k=1}^{2^r} k^{2t}.
\]
Since we only need to compute $\log C \mod 2^{n+2}$, we need to determine those terms from the above infinite sum, for which

$$
(2n - 2r) t - \text{ord}_2 t + \text{ord}_2 \left( \sum_{k=1}^{2^{r-1}-1} k^{2t} \right) < n + 2. \tag{4.9.2}
$$

Now observe that

$$
\text{ord}_2 \left( \sum_{k=1}^{2^{r-1}-1} k^{2t} \right) \geq (r - 2), \tag{4.9.3}
$$

which follows, for instance from the well-known identity

$$
(2t + 1) \sum_{k=1}^{2^{r-1}-1} k^{2t} = \sum_{l=0}^{2t} \binom{2t + 1}{l} B_l (2^r - 1)^{2t + 1 - l},
$$

where $B_l$ is the $l$th Bernoulli number, (so $\text{ord}_2 B_l \geq -1$).

Using (4.9.3), we find that (4.9.2) is only satisfied for $t = 1$. Therefore,

$$
\log C \mod 2^{n+2} = \frac{m^2 2^{r-1} (2^{r-1} - 1)(2^r - 1)}{6} \mod 2^{n+2}.
$$

Since $r \leq n - 2$, and $r \geq 2$, it follows that $\frac{1}{3} 2^{n-r-2}(2^r - 1) \equiv 2^{2n-r-2} \mod 2^{n+2}$, and so we have

$$
\log A = a' \log C \mod 2^{n+2} = \frac{2^{2n-r-2}}{a'} (2^{r-1} - 1) \mod 2^{n+2}.
$$

Case (ii) $r = n - 1$.

In this case, we have

$$
\log A = \log D + \log E,
$$

where

$$
D = \prod_{k=1}^{2n-2-1} \left( 1 - \frac{4k^2}{a'^2} \right) ^{a'},
$$

and

$$
E = \prod_{k=1}^{2^{r-2}-1} \left( 1 + 4 \left( \frac{k^2 + a'k}{a'^2} \right) \right)^{k} \left( 1 + 4 \left( \frac{k^2 - a'k}{a'^2} \right) \right) ^{-k}.
$$
From (4.9.3), we have \( \text{ord}_{2}(\sum_{k=1}^{2^{n-2}-1} k^{2^{t}}) \geq n - 3 \) for all \( t \), and so we find

\[
\log D \equiv -a' \sum_{t=1}^{2} \left( \frac{4^{t}}{td'2^{t}} \sum_{k=1}^{2^{n-2}-1} k^{2^{t}} \right) \mod 2^{n+2}
\]

\[
\equiv \frac{1}{a'} (2^{n-1} + 2^{n+1} - 2^{2n-3} - 2^{2n-2}) + \frac{1}{a'} (-2^{n}) \mod 2^{n+2}. \tag{4.9.4}
\]

A similar computation yields

\[
\log E = \sum_{k=1}^{2^{n-2}-1} \left( k \sum_{t=1}^{\infty} (-1)^{t+1} \frac{(k^{2} + a'k)^{2t} 4^{t}}{a'^{2t}t} \right)
\]

\[
= \sum_{k=1}^{2^{n-2}-1} \left( k \sum_{t=1}^{\infty} (-1)^{t+1} \frac{(k^{2} - a'k)^{2t} 4^{t}}{a'^{2t}t} \right)
\]

\[
= \sum_{k=1}^{2^{n-2}-1} \left( \frac{2^{3}k^{2}a'}{a'^{2}} - \frac{2^{5}k^{4}}{a'^{3}} \right) \mod 2^{n+2}
\]

\[
\equiv \frac{-2^{n}}{a'} (1 - 2^{n-1} - 2^{n-2}) \mod 2^{n+2}. \tag{4.9.5}
\]

Then using (4.9.4) and (4.9.5), we have

\[
\log A \equiv \frac{1}{a'} (2^{n-1} - 2^{2n-3}) \mod 2^{n+2},
\]

as claimed.

5. The Computation of \( \rho_{a,b,c,\lambda}^{(m)}(x_{w}) \)

As we showed in Section 2, it suffices to establish formula (1.7) for \( x_{w} \in K^{*} \), \( x_{w} \) a generator at a principal prime ideal \( p \neq \lambda \). By analogy with the results of Coleman–McCallum (cf. [3]), and Anderson–Coleman (cf. [4]), we would expect to express \( \rho_{a,b,c,\lambda}^{(m)}(x_{w}) \) as

\[
\rho_{a,b,c,\lambda}^{(m)}(x_{w}) = \varepsilon(x_{w}) \cdot (a^{a'b^{b}c^{c}}, x_{w})_{m}, \tag{5.1}
\]

where \( \varepsilon(x_{w}) \) is a correction term. In this section, we will establish (5.1) and we will show that

\[
\varepsilon(x_{w}) = (w^{-m'4}(1 - 4)^{t'}, x_{w})_{m}, \tag{5.2}
\]

with \( s \) as in (1.5). Our proof will follow the steps (1) through (5), described below:
Using Lemmas 5, 6, and 7 of Section 4, we find \( d = (d_i) \), with \( d_i \) odd \( \sum d_i = 0 \), such that
\[
G_a G_b G_c = A_\alpha(p) \prod_{d_i} G_{d_i},
\]
(5.3)
where \( A_\alpha(p) \) depends only on \( r \) and \( p \).

More precisely, we first substitute \( G_a \) as given by Lemma 5, we multiply the resulting expression by \((G_{m/4})^2 (G_{m/4})^{-2}\), and we then substitute \((G_{m/4} G_{m/4} G_{-m/2})^{-1}\) as given by Lemma 6. In the case where \( n > 2 \), we also use Lemma 7 to substitute \((G_{m/4})^2\). So we obtain
\[
A_\alpha(p) = \left( \frac{2^r}{p} \right)^\alpha \frac{((-w)^{m/4}, x_w)_m}{N_{m/4}(x_w) q^{2^{-1} + m/4 - 1}},
\]
(5.4)
and that
\[
\prod_{i} G_{d_i} = \begin{cases} 
G_a^2 G_b G_c & \text{if } n = 2 \\
\left( \prod_{k=1}^{2^{r-1} - 1} G_{a' - km/2} G_{a' - km/2} \right) G_a^2 G_b G_{a' - m/2} \\
\times \left( \prod_{k=1}^{m/8 - 1} G_{1 + 4k} G_{1 - 4k} \right)^2 G_1^2 G_1 + m/2 G_1 - m/2 G_b G_c & \text{if } n \geq 3.
\end{cases}
\]
(5.5)
Let \( d = (d_i) \) be determined by (5.5).

(2) Since \( \sum d_i = 0 \), \( d \) induces a Hecke character \( \rho_{d,a}^{(m)} \) on \( K \). Since all the \( d_i \) are odd, and \( N^m(x_w) \equiv 1 \mod 2^{n+2} \), we use Theorem 2 of Section 1 to obtain
\[
\rho_{d,a}^{(m)}(x_w) = \left( \prod d_i^{d_i}, x_w \right)_m,
\]
which together with (1.2) gives that
\[
\frac{1}{q} \prod_i G_d = x_w^{\Phi_d} \left( \prod_i d_i^{d_i}, x_w \right)_m^{-1},
\]
(5.6)
with \( \Phi_d \) as in (1.1). Note that using (1.2), (5.3) and (5.6) we have
\[
\rho_{a,b,c,a}^{(m)}(x_w) = \frac{x_w^{\Phi}}{1/q A_\alpha(p) \prod_i G_{d_i}} = \frac{x_w^{\Phi}}{1/q A_\alpha(p)} \left( \prod_i d_i^{d_i}, x_w \right)_m.
\]
(5.7)
(3) We compute $x_w^\Phi - \Phi_d$. When $n = 2$, a direct computation gives $\Phi - \Phi_d = -\sigma_3 - 2\sigma_1$, while when $n \geq 3$, $\Phi - \Phi_d = \tilde{\Phi}$, with $\tilde{\Phi}$ as defined in Lemma 8. In either case, we have

$$x_w^\Phi - \Phi_d = q^{-2^{r-1} - m/4} x_w^{-\sum_{i=3}^{3|d|} (\sigma_{i})^{-1}} = q^{-2^{r-1} - m/4 + 1} \frac{1}{N_d^m(x_w)}; \quad (5.8)$$

since $N_d^m(x_w) = N_d^m(p)$, and $\text{Gal}(K/\mathbb{Q}(\mu_4)) = \{\sigma; i \equiv 1 \mod 4\}$.

(4) We compute the ratio $R$, given by

$$R = \frac{2^a \prod_i d_i^{a_i}}{a^b b^c c^e}. \quad (5.9)$$

A direct computation gives

$$R = \begin{cases} 
\left(1 - \frac{2}{a'}\right)^{a - 2} (a')^{-2} & \text{if } n = 2 \\
\left(\prod_{k=1}^{2^{r-1} - 1} \frac{(1 + (km/a'))^{a' + km/2'} (1 - (m/2a'))^{-m/2}}{\prod_{k=1}^{m/8 - 1} (1 + 4k)^2 + 8k}
\times \prod_{k=1}^{m/8 - 1} (1 - 4k)^{-2 + 8k}
\right) & \text{if } n \geq 3.
\end{cases} \quad (5.10)$$

Using (5.8) and (5.9), together with the relation $(2'/p)_m^{-1} = (2', x_w)_m$, (cf. [1, ex. 2]), (5.7) gives

$$\rho_{a,b,c,d}(x_w) = ((-w)^{-m/4}, x_w)_m (R, x_w)_m (a^b b^c c^e, x_w)_m. \quad (5.11)$$

(5) It remains to simplify (5.11). We will show

$$((-1)^{m/4} R, x_w)_m = ((1 - 4)^s, x_w)_m, \quad (5.12)$$

with $s$ as in (1.5), which proves (5.2). Recall that any unit which is congruent to $1 \mod 2^n + 2$ is a $2^n$th power. So we only need to do arithmetic mod $2^n + 2$.

When $n = 2$, a direct computation gives that

$$(-1)^{m/4} R \mod 2^4 \equiv \begin{cases} 
1 \mod 2^4 & \text{if } a' \equiv 1 \mod 4 \\
1 \mod (1 - 4)^3 \mod 2^4 & \text{if } a' \equiv 3 \mod 4.
\end{cases}$$

Since $((1 - 4)^3, x_w)_m = ((1 - 4), x_w)_m$, (5.12) follows.
From here on, we assume that \( n \geq 3 \). Since \( R \equiv 1 \mod 4 \), there exists \( f \in \mathbb{Z}_2[x] \) such that

\[
R = (1 - 4)^f, \tag{5.13}
\]

that is \( f = (1/\log(1 - 4)) \log R \). Observe also that \((1 - 4)^{2^n - 1}, x_w)_{m} = ((1 - 4), N^m(x_w))_2 = 1\), since the extension \( \mathbb{Q}_2(\sqrt{-3}) \) is unramified over \( \mathbb{Q}_2 \). Since \(((1 - 4)^{m/4} R, x_w)_m = ((1 - 4)^f, x_w)_m\), we therefore only need to compute \( f \mod 2^{n-1} \). We will show that \( f \mod 2^{n-1} = s \), as given by (1.5). Since \( \text{ord}_2 \log(1 - 4) = 2 \), we need to compute \( \log R \mod 2^{n+1} \). By Lemma 9 we have

\[
\log \left( \prod_{k=1}^{2^{r-1}-1} \left( 1 + \frac{km}{a} \right)^{u^r + km/2^r} \left( 1 - \frac{km}{a} \right)^{-u^r - km/2^r} \right) \\
\equiv \frac{(-1)^{2^{r-1}-1}}{a'} 2^{2n-r-2}(2^r-1-1) \mod 2^{n+2}. \tag{5.14}
\]

We also apply Lemma 9 for \( a = m/4 \) and then square both sides, to obtain

\[
\log \left( \prod_{k=1}^{m/8-1} (1 + 4k)^{1+4k} (1 - 4k)^{1-4k} \right)^2 \equiv 0 \mod 2^{n+1}. \tag{5.15}
\]

Next, we compute directly \( \log(1 + m/2)^{1+m/2} (1 - m/2)^{1-m/2} \mod 2^{n+1} \),

\[
\log \left( 1 + \frac{m}{2} \right)^{1+m/2} \left( 1 - \frac{m}{2} \right)^{1-m/2} \\
= \left( 1 + \frac{m}{2} \right) \left( \frac{m}{2} - \frac{1}{2} \cdot \frac{m^2}{4} \right) + \left( 1 - \frac{m}{2} \right) \left( -\frac{m}{2} - \frac{1}{2} \cdot \frac{m^2}{4} \right) \mod 2^{n+1} \\
\equiv \frac{m^2}{4} \mod 2^{n+1} \equiv 0 \mod 2^{n+1}. \tag{5.16}
\]

Similar computations give

\[
\log \left( 1 - \frac{m}{2a'} \right)^{u^r-m/2} \equiv -2^{n-1} + \frac{2^{2n-3}}{a'} \mod 2^{n+1}, \tag{5.17}
\]

and that

\[
\log (a'^2)^{m/4} \equiv 0 \mod 2^{n+1}. \tag{5.18}
\]

Adding together (5.14), (5.15), (5.16), (5.17), and (5.18), we obtain

\[
\log R \equiv \frac{(1)^{2^{n-r-1}}}{a'} 2^{2n-r-2}(2^r-1-1) - 2^{n-1} + \frac{2^{2n-3}}{a'} \mod 2^{n+1}. \tag{5.19}
\]
From the relations
\[ \text{ord}_2(2^{2n-r-2}) \geq n-1, \]
\[ \text{ord}_2(2^{2n-3}) \geq n, \]

\[ \frac{2^{2n-3}}{a^r} \equiv 2^{2n-3} \mod 2^{n+1} \text{ (because \text{ord}_2(2^{2n-3}) \geq n)}, \]

and

\[ \frac{1}{\log(1 - 4)} = \frac{1}{2^2} (1 + 2^2 u), \quad u \in \mathbb{Z}_2, \]

we have that \( f \) of (5.13) satisfies \( f \equiv s \mod 2^{n-1} \), with \( s \) as in (1.5). (Note that the case \( r < n - 3 \) only applies for \( n \geq 4 \), and then we have that \( 2^{2n-3} \equiv 0 \mod 2^{n+1} \).) This completes the proof of (5.1).

6. The Computation of \( \rho^{(m)}_{n,b,c}(w) \) in \( \mathbb{Q}(\mu_m) \)

Let \( w = 1 - 2i \), let \( n, r, a, b, c \) be as in the statement of Theorem 1. In this section, we are going to prove the following proposition:

**Proposition 10.** For \( n \geq 2 \), \( 1 \leq r \leq -1 \), we have that

\[ \rho^{(m)}_{a,b,c}(w) = (-1)^{2^{n-2} + 1} = (w^{m/4}(1 - 4)^a a^a b^b c^c, w)_m. \]

**Proof of Proposition 10.** We will first show that \( \rho^{(m)}_{n,b,c}(w) = (-1)^{2^{n-2} + 1} \). Note that by (1.2) we have that

\[ \prod_{p|w} (J^{(m)}_{a,b,c}(p))^{\text{ord}_p(w)} \in \mu_m. \]

We will compute \( w^{\Phi_{a,b,c}} \) and \( \prod_{p|w} (J^{(m)}_{a,b,c}(p))^{\text{ord}_p(w)} \) separately. Observe that all the \( m \)th roots of unity map into distinct classes in \( \mathbb{Z}/(2) \). (To see this, consider for instance the binomial expansion for \( \pm \zeta^t = \pm (1 - \lambda)^t \), for \( t = 1, ..., 2^{n-1} \), and recall that \( 2 \equiv \lambda^2 \mod 2^{n-1} \).) It suffices therefore to perform all computations \( \mod 2\lambda \), since \( \rho^{(m)}_{a,b,c}(w) \in \mu_m \).

At first, let us compute \( w^{\Phi_{a,b,c}} \). We will prove the following lemma:

**Lemma 11.** With notation as above, we have

\[ w^{\Phi_{a,b,c}} = \begin{cases} -1 \mod 2\lambda & \text{if } n = 2 \\ 1 \mod 2\lambda & \text{if } n \geq 3. \end{cases} \]
Proof of Lemma 11. Since \( w \in \mathbb{Q}_2(t) \), we have

\[ \Psi_j = \sum_{t=1, t \equiv j \mod 4}^{m'} \left( \left\{ \frac{at}{m} \right\} + \left\{ \frac{bt}{m} \right\} + \left\{ \frac{ct}{m} \right\} - 1 \right). \]

Since \( 1 - 2t \equiv -1 \mod 2^\lambda \), and \( 1 + 2t \equiv -1 \mod 2^\lambda \), it follows that

\[ w^{\Phi_{a,b,c}} \equiv (-1)^{\Psi_1 + \Psi_3} \mod 2^\lambda. \] (6.2)

We will now compute \( \Psi_1 + \Psi_3 \). For \( l \in \mathbb{Z} \), odd, observe

\[ \sum_{t=1}^{m'} \left\{ \frac{lt}{m} \right\} = \sum_{k=0}^{2^{n-1}-1} \frac{1 + 2k}{2^n} = \frac{1}{2^n} \left( 2^{n-1} + 2 \sum_{k=0}^{2^{n-1}-1} k \right) = \frac{m}{4}. \] (6.3)

Also note that if \( r = n - 1 \), \( \sum_{t=1}^{m'} \left\{ \frac{at}{m} \right\} = \sum_{t=1}^{m'} \frac{1}{2} = m/4 \), while if \( r \leq n - 2 \), we have (using also (6.3)), that

\[ \sum_{t=1}^{m'} \left\{ \frac{at}{m} \right\} = 2^r \sum_{t=1}^{2^{n-r}} \left\{ \frac{a't}{2^{n-r}} \right\} = 2^r \cdot (2^{n-r} - 2) = \frac{m}{4}. \]

Therefore we obtain

\[ \Psi_1 + \Psi_3 = 3 \cdot \frac{m}{4} - \frac{m}{2} = \frac{m}{4}, \]

which, with (6.2) gives Lemma 11.

Next, we will compute \( \prod_{w \mid w} (J_{a,b,c}^{(m)}(p))^{ord_{p}(w)} \). The ideal \( (w) \) is prime in \( \mathbb{Z}[t] \) and lies over the ideal \( (5) \) of \( \mathbb{Z} \). Since \( (\mathbb{Z}/m\mathbb{Z})^* \) has order \( 2^{n-1} \) and \( 5^{2^{n-j}} \equiv 1 + 2^{n-j+2} \mod 2^{n-j+3} \) for \( n \geq 2 \), it follows that 5 has inertia degree \( 2^{n-2} \) in \( \mathbb{Q}(\mu_m) \). So 5 splits into two principal primes \((1 - 2t)\) and \((1 + 2t)\) in \( \mathbb{Q}(\mu_4) \), each of which remains inert in \( \mathbb{Q}(\mu_m) \). Therefore

\[ \prod_{w} (J_{a,b,c}^{(m)}(p))^{ord_{p}(w)} = J_{a,b,c}^{(m)}(\delta_n), \] (6.4)

where \( \delta_n \) denotes the prime ideal above \( (w) \) in \( \mathbb{Q}(\mu_m) \). We will prove the following lemma:

**Lemma 12.** Let \( \lambda_n = (1 - \zeta_n) \), where \( \zeta_n \) is a primitive \( 2^n \)th root of 1. For any triple \( a, b, c \) as in the statement of Theorem 1 we have

\[ J_{a,b,c}^{(m)}(\delta_n) = -1 \mod 2\lambda_n. \]
Proof of Lemma 12. We need to fix some notation. For $k \geq 2$, let $F_{\delta_k}$ denote the finite field $\mathbb{Z}[\mu_k]/\delta_k$. (So $F_{\delta_k}$ has $5^{2k-2}$ elements.) Let $S_k = F_{\delta_k} - F_{\delta_{k-1}}$, and let $R_k \in \mathbb{Z}[\mu_m]$ for $k = 3, \ldots, n$ be defined by $R_k = \sum_{x \in S_k} (x/\delta_n)^c_m ((1-x)/\delta_n)_m$. Then we have

$$J^{(m)}_{a,b,c}(\delta_n) = - \sum_{k=3}^n R_k - \sum_{x \in F_{\delta_k}, x \neq 0,1} \left( \frac{x}{\delta_n/\delta_n} \right)_m \left( \frac{1-x}{\delta_n/\delta_n} \right)^c_m.$$ 

We will prove the lemma by first showing that

$$J^{(m)}_{a,b,c}(\delta_n) = \sum_{x \in F_{\delta_k}, x \neq 0,1} \left( \frac{x}{\delta_n/\delta_n} \right)_m \left( \frac{1-x}{\delta_n/\delta_n} \right)^c_m \mod 2\lambda_k,$$ 

and then computing the above three terms directly. To prove (6.5), we will show that $R_k \equiv 0 \mod 2\lambda_k$, for $3 \leq k \leq n$. We will work with two disjoint sets, $A_k$ and $B_k$, whose union is $S_k$, and we will show that

$$\sum_{x \in A_k} \left( \frac{x}{\delta_n/\delta_n} \right)_m \left( \frac{1-x}{\delta_n/\delta_n} \right)^c_m \equiv 0 \mod 2\lambda_k,$$ 

and that

$$\sum_{x \in B_k} \left( \frac{x}{\delta_n/\delta_n} \right)_m \left( \frac{1-x}{\delta_n/\delta_n} \right)^c_m \equiv 0 \mod 2\lambda_k.$$ 

Set $A_k = \{x \in S_k | x^{5^{2k-3}} = 1 - x\}$. Since $5^{2k-3} \equiv 1 + 2k^{-1} \mod 2k$, the roots of the polynomial $x^{5^{2k-3}} + x - 1 \mod \delta_k$ are given by $a_{\delta_k} + 3$, where $a \in F_{\delta_{k-1}}, a \neq 0$. In particular

$$\# A_k = 5^{2k-3} - 1 \equiv 2^{k-1} \mod 2k \equiv 0 \mod 4.$$ 

Also set $B_k = S_k - A_k$. Now we need the following observations:

1. If $x \in S_k$, then $1-x \in S_k$ and $x^{5^{2k-3}} \in S_k$.

2. If $x \in S_k$, then $(x/\delta_n)_m \in \mu_k$. (For if $g$ is a generator of $F_{\delta_k}^*$, $g^u$ generates $F_{\delta_k}^*$, where $u = (5^{2k-2} - 1)/(5^{2k-2} - 1) \equiv 2n^{-k} \mod 2^{n-k+1}$. But then $(g^u/\delta_n)_m \in (\mu_m)^{2^{n-k-1}}$.)

3. If $x \in S_k$, then $(x^{5^{2k-3}}/\delta_n)_m = \pm (x/\delta_n)_m$. (This follows from (2), since $5^{2k-3} \equiv 1 + 2^{k-1} \mod 2k$.)

4. If $x \in S_k$, then $x$ and $x^{5^{2k-3}}$ are distinct, and we have that

$$\left( \frac{x}{\delta_n/\delta_n} \right)_m \left( \frac{1-x}{\delta_n/\delta_n} \right)^c_m = \pm \left( \frac{x^{5^{2k-3}}}{\delta_n/\delta_n} \right)_m \left( \frac{1-x^{5^{2k-3}}}{\delta_n/\delta_n} \right)^c_m.$$
where the sign in the above relation equals \((x(1-x)/\delta_n)^{\frac{k}{2}}\). (This follows
from (3), and the relation \((1-x)^{\frac{k}{2}} = 1 - x^{\frac{k}{2}} \mod \delta_n\).

We will now show (6.6). Let \(A_k\) be a subset of \(A_k\) containing exactly one
element from each pair \((x, 1-x)\). Then we have using (3) that

\[
\sum_{x \in A_k} \left( \frac{x}{\delta_n} \right)^b \left( \frac{1-x}{\delta_n} \right)^c = \sum_{x \in \overline{A}_k} \pm 2 \left( \frac{x}{\delta_n} \right)^{h+c}. \tag{6.8}
\]

From (2), we have that \((x/\delta_n)^{h+c} \equiv 2 \mod 2\lambda_k\). Since \# \overline{A}_k = \frac{1}{2} \# A_k \equiv 0 \mod 2\), it follows that

\[
\sum_{x \in \overline{A}_k} \pm 2 \left( \frac{x}{\delta_n} \right)^{h+c} \equiv 0 \mod 2\lambda_k
\]

which with (6.8), completes the proof of (6.6).

Next, we will prove (6.7). For \(x \in B_k\), we have that \(x, 1-x, x^{5k-3}, 1-x^{5k-3}\)
are all distinct. Let \(B_k\) be a subset of \(B_k\) containing exactly one
element from each 4-tuple \((x, 1-x, x^{5k-3}, 1-x^{5k-3})\). For any \(x \in B_k\), let \(b_x\)
be defined by

\[
b_x = \left( \frac{x}{\delta_n} \right)^b \left( \frac{1-x}{\delta_n} \right)^c + \left( \frac{x^{5k-3}}{\delta_n} \right)^b \left( \frac{1-x^{5k-3}}{\delta_n} \right)^c
\]

\[+ \left( \frac{1-x}{\delta_n} \right)^b \left( \frac{x}{\delta_n} \right)^c + \left( \frac{x^{5k-3}}{\delta_n} \right)^b \left( \frac{1-x^{5k-3}}{\delta_n} \right)^c.
\]

We will show that

\[
b_x \equiv \mod 2\lambda_k, \tag{6.9}
\]

from which (6.7) follows, since \(\sum_{x \in B_k} \left( x/\delta_n \right)^{h^b} \left( (1-x)/\delta_n \right)^{c} = \sum_{x \in B_k} b_x\).

Using (4), we find that either \(b_x = 0\) (if the sign in (4) is “−”), or else that

\[
b_x = 2\zeta_k^i + 2\zeta_k^j \quad \text{for some} \quad i, j \mod k
\]

\[
\equiv 0 \mod 2\lambda_k
\]

which completes the proof of (6.5). Since \(2 \equiv -1 \mod \delta_n\), it follows from a
direct computation that

\[
J_{a,b,c}(\delta_n) \equiv \begin{cases} t^b + t^c \mod 2\lambda_n & \text{if } n \geq 3 \\ -t^b - t^c \mod 2\lambda_n & \text{if } n = 2 \\ -1 \mod 2\lambda_n, \end{cases}
\]
which completes the proof of Lemma 12. This, with Lemma 11 and (6.4) imply that \( \rho^{(m)}_{a,b,c}(w) = (1)^{2n-2} + 1 \). To complete the proof of Proposition 10, it remains to show that

\[
(w^{-m/4}(1-4)^r a^ab^bc^c, w)_m = (-1)^{2n-2} + 1. \tag{6.10}
\]

For this we need the observations (5) through (8) below, which follow from the properties of the Hilbert norm residue symbol (cf. [1, ex. 2]):

1. \((-1, w)_m = -1\). (It follows from a direct computation.)
2. \((w, w)_m = -1\). (It follows from the linearity of the symbol, since \((-1, w)_m = -1\), and \((-w, w)_m = 1\).)
3. \((2, w)_m = \pm i\), because \(N^m(w) = 1 + 2^n \mod 2^{n+1}\), and \(2 \equiv -i \mod(w)\).
4. \((1 - 4, w)_m = 1\) because the conductor of the character \((1 - 4, x)_m\) is \(2\) (cf. [8, Prop. 6]).

Observe that (6.10) follows directly from (6) and (8) above, together with the following lemma:

**Lemma 13.** With \(a, b, c\) as in the statement of Theorem 1, we have

\[
(a^ab^bc^c, w)_m = -1.
\]

**Proof of Lemma 13.** Note that \(a^ab^bc^c = 2^a a^ab^bc^c\). From (7), we have

\[
(2^a, w)_m = (\pm 1)^{ra} = \begin{cases} 1 & \text{if } r \geq 2 \\ -1 & \text{if } r = 1. \end{cases} \tag{6.11}
\]

Next, note that for some \(l \in \mathbb{Z}_2\), we have

\[
a^ab^bc^c = \begin{cases} -(1-4)^l & \text{if } r \geq 2 \\ (1-4)^l & \text{if } r = 1. \end{cases} \tag{6.12}
\]

(To see this, observe that \(a^ab^bc^c = a^a(bc)^b c^c - b\), and since \(a\), and \(c - b\) are even, we have \(a^ab^bc^c \equiv 1 \mod 4\), so \(a^ab^bc^c \equiv bc \mod 4\). Since \(a + b + c = 0\), we have that when \(r = 1\), \(b \equiv c \mod 4\), while for \(r \geq 2\), \(b \not\equiv c \mod 4\).)

Using (5) and (8), (6.12) together with the bilinearity and the continuity of the symbol, give

\[
(a^ab^bc^c, w)_m = \begin{cases} -1 & \text{if } r \geq 2 \\ 1 & \text{if } r = 1. \end{cases}
\]

which with (6.11) completes the proof of Lemma 13.
REFERENCES

2. C. CHEVALLEY, La théorie du corps de classes, Ann. of Math. (2) 41 (1940), 394–418.