TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 353, Number 11, Pages 4429–4445
S 0002-9947(01)02823-9
Article electronically published on June 27, 2001

GAUSS SUMS AND KLOOSTERMAN SUMS OVER RESIDUE RINGS OF ALGEBRAIC INTEGERS

RONALD EVANS

ABSTRACT. Let $\mathcal{O}$ denote the ring of integers of an algebraic number field of degree m which is totally and tamely ramified at the prime p. Write $\zeta_q = \exp(2\pi i/q)$, where $q = p^r$. We evaluate the twisted Kloosterman sum

$$\sum_{\alpha \in (\mathcal{O}/q\mathcal{O})^*} \chi(N(\alpha))\zeta_q^{T(\alpha)+z/N(\alpha)},$$

where T and N denote trace and norm, and where χ is a Dirichlet character (mod q). This extends results of Salié for $m = 1$ and of Yangbo Ye for prime m dividing $p - 1$. Our method is based upon our evaluation of the Gauss sum

$$\sum_{\alpha \in (\mathcal{O}/q\mathcal{O})^*} \chi(N(\alpha))\zeta_q^{T(\alpha)},$$

which extends results of Mauclaire for $m = 1$.

1. Introduction

Let E be a field of degree m over $\mathbb{Q}$, and let $\mathcal{O}_E$ denote the ring of integers in E. Suppose that p is a prime and $\mathfrak{P} \subset \mathcal{O}_E$ is a prime ideal such that

$$p\mathcal{O}_E = \mathfrak{P}^m, \quad p \not| \, m, \tag{1.1}$$

that is, p is totally and tamely ramified in E. For

$$q = p^r, \quad r \geq 1, \tag{1.2}$$

consider the finite quotient rings

$$R_q = \mathbb{Z}/q\mathbb{Z}, \quad \mathcal{O}_q = \mathcal{O}_E/q\mathcal{O}_E, \tag{1.3}$$

which have cardinalities q and q^m, respectively. For $\alpha \in \mathcal{O}_E$ viewed as an element of $\mathcal{O}_q$, write $N(\alpha)$ and $T(\alpha)$ to denote the norm and trace of α from $\mathcal{O}_q$ to R_q. For any positive integer n, set

$$\zeta_n = \exp(2\pi i/n). \tag{1.4}$$

For Dirichlet characters χ, η (mod q) and $z \in R_q^*$, define the Gauss sum

$$G(\chi) = G_m(\chi) = \sum_{\alpha \in \mathcal{O}_q^*} \chi(N(\alpha))\zeta_q^{T(\alpha)} \tag{1.5}$$

and the (twisted) Kloosterman sum

$$K(\eta, z) = K_m(\eta, z) = \sum_{\alpha \in \mathcal{O}_q^*} \eta(N(\alpha))\zeta_q^{T(\alpha)+z/N(\alpha)}. \tag{1.6}$$

Received by the editors November 17, 1999 and, in revised form, January 4, 2001.
2000 *Mathematics Subject Classification.* Primary 11L05, 11T24.

In the case that η is the trivial character, write $\eta = 1$ and set

$$K(z) = K(1, z).$$

The sums in (1.5) - (1.6) are well-defined, since the summands would be unchanged if a multiple of q were added to α.

Mauclaire [9], [10], [2, Theorem 1.6.4, p. 40], Odoni [12], [2, Theorem 1.6.2, p. 33], and Funakura [6], [2, Theorem 1.6.3, p. 37] explicitly evaluated the Gauss sums $G_1(\chi)$ for all $r \geq 2$. In §2 (Theorem 2.2), we extend Mauclaire's results by evaluating the Gauss sums $G_m(\chi)$ for *all* m.

Salié [13] evaluated the Kloosterman sums $K_1(1, z)$ for all $r \geq 2$. Ye [16] evaluated the Kloosterman sums $K_m(1, z)$ in terms of a twisted hyper-Kloosterman sum over R_q^*, in the case that m is prime, $m|(p-1)$, and $E/\mathbb{Q}$ is cyclic; see (3.1). In §3 (Theorem 3.2), we apply Theorem 2.2 to extend Ye's result in the case $r \geq 2$ by evaluating $K_m(\eta, z)$ for all m (where m need not be a prime nor a divisor of $p-1$). Our evaluations are in terms of twisted hyper-Kloosterman sums over R_q^* which in turn have been explicitly evaluated in [5]. In Theorem 3.3, we extend Ye's result in the case $r = 1$ by evaluating $K_m(1, z)$ for all (not necessarily prime) m dividing $p-1$.

In contrast with Ye's determination, we do not require results from local class field theory. Our proof requires only relatively basic results from local and global algebraic number theory.

Ye [18] has pointed out that the results of [16] can be generalized to cyclic extensions E of composite degree m over $\mathbb{Q}$, by applying repeated liftings of prime degree as in Arthur and Clozel [1, Eq. (6.7), p. 60]. For work related to [16] where the prime p is unramified in E, see Ye [17]. We note that in both [16] and [17], E is assumed to be cyclic over $\mathbb{Q}$, whereas in this paper, there is no such restriction.

In §4 (Theorem 4.1), we give a general product formula for the Gauss sums $G_m(\chi)$, which reduces in the case $m = r = 1$ to the famous Davenport-Hasse product formula [3], [2, Theorem 11.3.5, p. 355] for Gauss sums (mod p) given in (3.16).

2. Evaluation of Gauss sums $G_m(\chi)$

In the case $m = 1$, the Gauss sum $G_m(\chi)$ over $\mathcal{O}_q^*$ reduces to the familiar Gauss sum $G_1(\chi)$ over R_q^* defined by

$$G_1(\chi) = \sum_{a \in R_q^*} \chi(a) \zeta_q^a. \tag{2.1}$$

No explicit evaluation of $G_1(\chi)$ is known for general χ in the case $r = 1$ (i.e., $q = p$), but for $r \geq 2$, $G_1(\chi)$ can be evaluated as follows. We have

$$G_1(\chi) = 0 \quad \text{if } \chi \text{ is nonprimitive}, \quad r \geq 2 \tag{2.2}$$

(see [2, Eqs. (1.6.4)–(1.6.5)]). If $r \geq 2$ and χ is primitive, then

$$G_1(\chi) = \begin{cases} \sqrt{q}\,\zeta_q, & \text{if } r \text{ is even,} \\ \sqrt{q}\,\zeta_q\zeta_8^{1-p}, & \text{if } p > 2 \text{ and } r \geq 3 \text{ is odd,} \\ \sqrt{q}\,\zeta_q\zeta_8, & \text{if } p = 2 \text{ and } r \geq 5 \text{ is odd,} \\ \sqrt{q}\,\zeta_q\zeta_8^{-\chi(-1)}, & \text{if } p = 2 \text{ and } r = 3, \end{cases} \tag{2.3}$$

provided that $\nu(\chi) = 1$, where $\nu = \nu(\chi)$ is defined for $r \geq 2$ by

$$\chi(1 + p^s) = \zeta_{p^s}^{-\nu}, \quad \text{for even } r = 2s \geq 2, \tag{2.4}$$

$$\chi(5) = (-1)^\nu, \quad \text{for } q = 8 \text{ (i.e., } p = 2,\ r = 3), \tag{2.5}$$

and

$$\chi(1 + p^s + \frac{1}{2}p^{2s}) = \zeta_{p^{s+1}}^{-\nu}, \quad \text{for odd } r = 2s + 1 \geq 3, \quad q \neq 8. \tag{2.6}$$

(In (2.6) and in the sequel, $\frac{1}{2} (\mathrm{mod}\, p)$ is interpreted as $(p + 1)/2 \pmod{p}$ when $p > 2$.)

The evaluation of $G_1(\chi)$ in (2.3) was proved by Mauclaire [9], [10]. For a shortened proof, see [2, Theorem 1.6.4, p. 40] (where "inner sum on y" should be corrected to read "inner sum on x" in [2, p. 41]).

For $r \geq 2$, the assertion that χ is primitive is equivalent to the assertion that p does not divide $\nu(\chi)$. When $r \geq 2$ and $\nu(\chi) = 1$, the (primitive) character χ is said to be *normalized*. When $r \geq 2$ and χ is primitive but not necessarily normalized, we can evaluate $G_1(\chi)$ in terms of a normalized Gauss sum in (2.3), as follows. First write

$$\chi = \xi^\nu, \tag{2.7}$$

where ξ is a normalized character (mod q), and $\nu = \nu(\chi)$ is chosen relatively prime to $q(p - 1)$. Then

$$G_1(\chi) = G_1(\xi^\nu) = \chi(\nu)\sigma_\nu(G_1(\xi)), \tag{2.8}$$

where $\sigma_\nu \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q(p-1)})/\mathbb{Q})$ is defined by $\sigma_\nu(\zeta_{q(p-1)}) = \zeta_{q(p-1)}^\nu$. Since $G_1(\xi)$ is evaluated in (2.3), we see that (2.8) yields an evaluation of $G_1(\chi)$ for any primitive character χ, when $r \geq 2$.

In Theorem 2.2 below, we extend the evaluations of $G_1(\chi)$ given above by evaluating the Gauss sums $G_m(\chi)$ for *all* m. We begin with a lemma which gives a useful representation of the elements of $\mathcal{O}_q$. While its proof is p-adic, the lemma allows us to prove our main results in the language of global rather than local rings.

Lemma 2.1. *There exists $\tau \in \mathcal{O}_E$ of degree m over $\mathbb{Q}$ such that*

$$\tau^m \equiv pu \pmod{q\mathcal{O}_E} \quad \textit{for some integer } u \not\equiv 0 \pmod{p}, \tag{2.9}$$

$$\mathrm{Tr}_{E/\mathbb{Q}}(\tau^i) \equiv 0 \pmod{q} \quad (1 \leq i \leq m - 1), \tag{2.10}$$

and

$$\mathcal{O}_q = \left\{ \sum_{i=0}^{m-1} \alpha_i \tau^i : \alpha_i \in R_q \right\}. \tag{2.11}$$

Moreover, the m conjugates of τ over $\mathbb{Q}$ have the form $\tau\zeta_m^i + q\beta_i$, $1 \le i \le m$, where the β_i are algebraic integers.

Proof. Choose any $\omega \in \mathcal{O}_E$ with $\mathfrak{P} \| \omega$, i.e., $\omega \in \mathfrak{P} - \mathfrak{P}^2$. Then the irreducible polynomial of ω over $\mathbb{Q}$ is p-Eisensteinian of degree m, and $E = \mathbb{Q}(\omega)$. We also have [11, Theorem 5.5, p. 217] $E_{\mathfrak{P}} = \mathbb{Q}_p(\omega)$ and $[E_{\mathfrak{P}} : \mathbb{Q}_p] = m$, where $E_{\mathfrak{P}}$ is the $\mathfrak{P}$-adic completion of E, and $\mathbb{Q}_p$ denotes the p-adic rationals. Let $\mathbb{Z}_p$ denote the p-adic integers. By [8, Ex. 13-14, pp. 74, 140] (cf. [15, pp. 324–325]), there exists an element $\pi \in E_{\mathfrak{P}}$ such that

$$E_{\mathfrak{P}} = \mathbb{Q}_p(\pi), \quad \mathcal{O}_{E_{\mathfrak{P}}} = \mathbb{Z}_p(\pi), \tag{2.12}$$

$$\pi^m = p\mu, \quad \text{for some } \mu \in \mathbb{Z}_p^*, \tag{2.13}$$

$$\pi \mathcal{O}_{E_{\mathfrak{P}}} = \mathfrak{P} \mathcal{O}_{E_{\mathfrak{P}}}, \tag{2.14}$$

and

$$\pi - \omega \in \mathfrak{P}^2 \mathcal{O}_{E_{\mathfrak{P}}}. \tag{2.15}$$

Since $X^m - p\mu$ is the irreducible polynomial of π over $\mathbb{Q}_p$, the m conjugates of π over $\mathbb{Q}_p$ are $\pi\delta^j$ $(0 \le j \le m-1)$, where δ is a primitive m-th root of unity in a field extension of $\mathbb{Q}_p$. Thus

$$\mathrm{Tr}_{E_{\mathfrak{P}}/\mathbb{Q}_p}(\pi^i) = 0, \qquad 1 \le i \le m-1, \tag{2.16}$$

where Tr denotes the trace. By (2.12)–(2.13), every $\alpha \in \mathcal{O}_E$ can be π-adically represented in the form

$$\alpha = \sum_{i=0}^{m-1} a_i \pi^i, \qquad a_i \in \mathbb{Z}_p. \tag{2.17}$$

We can find $\tau \in \mathcal{O}_E$ such that

$$\tau \equiv \pi (\mathrm{mod}\ q\mathcal{O}_{E_{\mathfrak{P}}}), \tag{2.18}$$

by reducing (mod q) an appropriate linear combination of $\omega, \omega^2, \ldots, \omega^{m-1}$ over $\mathbb{Z}_p$. Then τ has degree m over $\mathbb{Q}$, by the same argument we used to show that ω has degree m over $\mathbb{Q}$. By (2.13) and (2.18), we see that (2.9) holds for some integer u with $u \equiv \mu$ (mod $q\mathbb{Z}_p$). By (2.16), (2.18) and the fact that

$$\mathrm{Tr}_{E_{\mathfrak{P}}/\mathbb{Q}_p}(\tau^i) = \mathrm{Tr}_{E/\mathbb{Q}}(\tau^i)$$

[11, Corollary, p. 266], we see that (2.10) holds. Equality (2.11) follows easily from (2.17) - (2.18). The last assertion of the lemma results from applying the m different $\mathbb{Q}_p$-embeddings of $E_{\mathfrak{P}}$ to both sides of (2.18). □

We now evaluate the Gauss sums $G(\chi) = G_m(\chi)$ over $\mathcal{O}_q^*$ in terms of the Gauss sums $G_1(\chi)$ over R_q^* discussed at the beginning of this section.

Theorem 2.2. *If $r = 1$, then*

$$G(\chi) = p^{m-1}\overline{\chi}^m(m)G_1(\chi^m). \tag{2.19}$$

If $r \geq 2$ and χ is nonprimitive, then $G(\chi) = 0$. If $r \geq 2$ and χ is primitive, then, with $\nu(\chi)$ defined by (2.4) – (2.6),

$$G(\chi) = \begin{cases} G_1(\chi)^m p^{(m-1)/2}\left(\frac{p}{m}\right)^r, & \text{if } 2 \nmid m, \\ G_1(\chi)^m p^{(m-1)/2}\zeta_8^{(1-p)(1-m)}\left(\frac{-Dp^{1-m}}{p}\right)^{r+1}\left(\frac{m\nu(\chi)}{p}\right), & \text{if } 2|m, \end{cases} \tag{2.20}$$

where D is the discriminant of the number field E, and where $G_1(\chi)$ is explicitly given by (2.8).

Remark. If $2|m$, then $p > 2$ by (1.1). Moreover, $p^{m-1}\|D$ by [11, Theorem 4.8, p. 166]. Hence the Legendre symbols in (2.20) make sense. For a formulation of (2.20) in the case $2|m$ in which $\nu(\chi)$ does not appear, see (2.45).

Proof. For $\alpha \in \mathcal{O}_q$, write

$$\alpha = \sum_{i=0}^{m-1} \alpha_i\tau^i, \qquad \alpha_i \in R_q, \tag{2.21}$$

as in (2.11). First suppose that $r = 1$, so that $q = p$. Recall the definitions of T and N below (1.3). By Lemma 2.1, $T(\alpha) = m\alpha_0$ and $N(\alpha) = \alpha_0^m$, since $q = p$. Thus

$$G(\chi) = \sum_{\alpha_0,\ldots,\alpha_{m-1}\in R_p} \chi(\alpha_0^m)\zeta_p^{m\alpha_0} = p^{m-1}\sum_{a\in R_p}\chi^m(a)\zeta_p^{ma} = p^{m-1}\overline{\chi}^m(m)G_1(\chi^m),$$

which proves (2.19).

Suppose now that $r \geq 2$. If χ is nonprimitive, then $G(\chi) = 0$ by an argument analogous to that proving (2.2). Next assume that χ is primitive. If $m = 1$, then (2.20) follows from the definition (2.1) of $G_1(\chi)$. Hence assume that $m > 1$.

We first prove (2.20) when χ is normalized. There are three cases.

Case 1: $\nu(\chi) = 1,\ r = 2s,\ s \geq 1$.

The elements $\alpha \in \mathcal{O}_q^*$ may be written

$$\alpha = z + zwp^s \qquad (z \in \mathcal{O}_{p^s}^*,\ w \in \mathcal{O}_{p^s}),$$

so

$$G(\chi) = \sum_{z\in\mathcal{O}_{p^s}^*}\chi(N(z))\zeta_q^{T(z)}\sum_{w\in\mathcal{O}_{p^s}}\chi(N(1+wp^s))\zeta_{p^s}^{T(zw)}.$$

Since

$$N(1+wp^s) = 1 + T(w)p^s \equiv (1+p^s)^{T(w)} \pmod{q},$$

it follows from the normalization (2.4) that

$$G(\chi) = \sum_z \chi(N(z))\zeta_q^{T(z)}\sum_w \zeta_{p^s}^{T(w(z-1))}.$$

Using Lemma 2.1, one sees that the inner sum $\sum_w$ vanishes unless $z \equiv 1 \pmod{\tau p^{s-1}}$, in which case

$$\sum_w = \mathrm{Card}(\mathcal{O}_{p^s}) = p^{sm} = (\sqrt{q})^m.$$

Thus, writing $z = 1 + xp^{s-1}$ with

$$x := \sum_{i=1}^{m-1} x_i \tau^i \in \mathcal{O}_p \qquad (x_1, \ldots, x_{m-1} \in R_p),$$

we have

$$G(\chi) = (\sqrt{q}\zeta_q)^m \sum_{x_1,\ldots,x_{m-1} \in R_p} \chi(N(1 + xp^{s-1})). \tag{2.22}$$

Write $N(1 + xp^{s-1})$ as a product of m conjugates and expand. One sees, using Lemma 2.1, that

$$N(1 + xp^{s-1}) = 1 - p^{2s-1} \left\{ \frac{mu}{2} \sum_{i=1}^{m-1} x_i x_{m-i} + f(x_1, \ldots, x_{m-1}) \right\}, \tag{2.23}$$

where $f(x_1, \ldots, x_{m-1})$ is a $\mathbb{Z}$-linear combination of monomials $x_{i_1} \ldots x_{i_n}$ with $3 \le n \le m$, $i_1 + \cdots + i_n = m$. If $m = 2$, f is interpreted as 0. (Note that each coefficient in f is divisible by p^{s-1}, so the term f could have been omitted from (2.23) were it not for the pesky case $s = 1$.) Since

$$N(1 + xp^{s-1}) = (1 + p^s)^{-p^{s-1}\left\{ \frac{mu}{2} \sum_{i=1}^{m-1} x_i x_{m-i} + f(x_1, \ldots, x_{m-1}) \right\}},$$

the normalization (2.4) gives

$$\chi(N(1 + xp^{s-1})) = \zeta_p^{\frac{mu}{2} \sum_{i=1}^{m-1} x_i x_{m-i} + f(x_1, \ldots, x_{m-1})}.$$

Therefore, by (2.22) and (2.3),

$$G_1(\chi)^{-m} G(\chi) = \sum_{x_1,\ldots,x_{m-1} \in R_p} \zeta_p^{\frac{mu}{2} \sum_{i=1}^{m-1} x_i x_{m-i} + f(x_1, \ldots, x_{m-1})}. \tag{2.24}$$

Now, x_{m-1} does not actually appear in the polynomial $f(x_1, \ldots, x_{m-1})$ and so unless $x_1 = 0$, the sum on x_{m-1} in (2.24) vanishes when $m > 2$. Therefore we may set $x_1 = 0$ in the summands of (2.24) when $m > 2$. Further, x_{m-2} does not appear in the polynomial $f(0, x_2, \ldots, x_{m-1})$, and so unless $x_2 = 0$, the sum on x_{m-2} vanishes when $m > 4$. Continuing in this way, we see that one may set

$$x_1 = x_2 = \cdots = x_{[(m-1)/2]} = 0$$

in the summands of (2.24). With this substitution, all terms of the polynomial f vanish, and so (2.24) becomes

$$G_1(\chi)^{-m} G(\chi) = \begin{cases} p^{(m-1)/2}, & \text{if } 2 \nmid m, \\ p^{(m-2)/2} \sum_{y=0}^{p-1} \zeta_p^{muy^2/2}, & \text{if } 2 | m, \end{cases} \tag{2.25}$$

where we've written y for the variable $x_{m/2}$. This proves (2.20) for odd m. Assume now that $2|m$. Then

$$\sum_{y=0}^{p-1} \zeta_p^{muy^2/2} = \sqrt{p} \left(\frac{mu}{p} \right) \zeta_8^{(1-p)(1-m)} \left(\frac{-1}{p} \right)^{m/2} \tag{2.26}$$

(see [2, Theorem 1.5.2, p. 26]). In view of (2.25) - (2.26), it remains to prove that

$$\left(\frac{u}{p}\right) = \left(\frac{-1}{p}\right)^{m/2}\left(\frac{-Dp^{1-m}}{p}\right). \tag{2.27}$$

By Lemma 2.1,

$$N_{E/\mathbb{Q}}(\tau) \equiv -pu \pmod{q},$$

so by (2.18), $N := N_{E_{\mathfrak{P}}/\mathbb{Q}_p}(\pi)$ satifies

$$\left(\frac{u}{p}\right) = \left(\frac{-N/p}{p}\right).$$

By (2.15),

$$N_{E/\mathbb{Q}}(\omega)/p \equiv N/p \pmod{p\mathbb{Z}_p},$$

and so

$$\left(\frac{u}{p}\right) = \left(\frac{-N/p}{p}\right) = \left(\frac{-(N_{E/\mathbb{Q}}(\omega)/p)^{m-1}}{p}\right), \tag{2.28}$$

where the last equality uses the fact that m is even. Let $g(x) \in \mathbb{Z}[x]$ denote the (p-Eisensteinian) irreducible polynomial of ω over $\mathbb{Q}$, discussed near the beginning of the proof of Lemma 2.1. Since

$$g'(\omega) \equiv m\omega^{m-1} \pmod{p\mathcal{O}_E}$$

and m is even, (2.28) yields

$$\left(\frac{u}{p}\right) = \left(\frac{-N_{E/\mathbb{Q}}(g'(\omega))p^{1-m}}{p}\right). \tag{2.29}$$

By a well-known formula for the discriminant of the basis $1, \omega, \dots, \omega^{m-1}$ for E [11, Prop. 2.4, p. 53], the "numerator" on the right side of (2.29) may be replaced by $(-1)^{(m+2)/2}Dp^{1-m}$. This proves (2.27) and completes the proof of (2.20) in Case 1.

Case 2: $\nu(\chi) = 1,\ r = 2s+1,\ s \geq 1,\ q \neq 8.$

In this case, $s > 1$ when $p = 2$. The elements $\alpha \in \mathcal{O}_q^*$ may be written

$$\alpha = z + zwp^s \qquad \left(z \in \mathcal{O}_{p^s}^*, w \in \mathcal{O}_{p^{s+1}}\right),$$

so

$$G(\chi) = \sum_{z\in\mathcal{O}_{p^s}^*} \chi(N(z))\zeta_q^{T(z)} \sum_{w\in\mathcal{O}_{p^{s+1}}} \chi(N(1+wp^s))\zeta_{p^{s+1}}^{T(zw)}.$$

Observe that

$$N(1+wp^s) = 1 + p^sT(w) + \frac{1}{2}p^{2s}(T(w)^2 - T(w^2)),$$

so since $s > 1$ when $p = 2$,

$$N(1+wp^s) = (1 + p^s + \frac{1}{2}p^{2s})^{T(w-p^sw^2/2)}.$$

It thus follows from the normalization (2.6) that

$$G(\chi) = \sum_{z\in\mathcal{O}_{p^s}^*} \chi(N(z))\zeta_q^{T(z)}S(z), \tag{2.30}$$

where

$$S(z)=\sum_{w\in\mathcal{O}_{p^{s+1}}}\zeta_{p^{s+1}}^{T(zw+p^sw^2/2-w)}.$$

Writing

$$w=x+yp^s \qquad (x\in\mathcal{O}_{p^s}, y\in\mathcal{O}_p),$$

we have

$$S(z)=\sum_x \zeta_{p^{s+1}}^{T(x(z-1)+x^2p^s/2)}\sum_y \zeta_p^{T(y(z-1))}.$$

The inner sum $\sum_y$ vanishes unless $z\equiv 1 \pmod{\tau}$, in which case $\sum_y = p^m$. Thus set

$$z=1+\sum_{i=1}^{m-1} z_i\tau^i, \qquad z_i\in R_{p^s}. \tag{2.31}$$

Writing

$$x=a+bp \qquad (a\in\mathcal{O}_p, b\in\mathcal{O}_{p^{s-1}}),$$

we have

$$S(z)=p^m\sum_a \zeta_p^{T(a^2/2)}\zeta_{p^{s+1}}^{T(a(z-1))}U(z), \tag{2.32}$$

where

$$U(z)=\sum_{b\in\mathcal{O}_{p^{s-1}}}\zeta_{p^s}^{T(b(z-1))}.$$

Writing

$$b=\sum_{i=0}^{m-1} b_i\tau^i, \qquad b_i\in R_{p^{s-1}},$$

we have, by (2.31) and Lemma 2.1,

$$U(z)=\sum_{b_0,\dots,b_{m-1}}\zeta_{p^s}^{mpu\sum_{i=1}^{m-1} z_ib_{m-i}}=\sum_{b_0,\dots,b_{m-1}}\zeta_{p^{s-1}}^{mu\sum_{i=1}^{m-1} z_ib_{m-i}}.$$

Therefore $U(z)$ vanishes unless p^{s-1} divides each of $z_1,z_2,\dots,z_{m-1}$, in which case $U(z)=p^{m(s-1)}$. Thus, with

$$z=1+p^{s-1}\sum_{i=1}^{m-1} q_i\tau^i, \qquad q_i\in R_p,$$

(2.32) becomes

$$S(z)=p^{sm}\sum_{a\in\mathcal{O}_p}\zeta_p^{T(a^2/2)}\zeta_{p^2}^{T(a\sum_{i=1}^{m-1} q_i\tau^i)}.$$

Writing

$$a=\sum_{i=0}^{m-1} a_i\tau^i, \qquad a_i\in R_p,$$

we obtain

$$S(z) = p^{sm} \sum_{a_0,\dots,a_{m-1}} \zeta_p^{ma_0^2/2+mu\sum_{i=1}^{m-1} a_{m-i}q_i}.$$

Thus $S(z)$ vanishes unless $q_1 = \cdots = q_{m-1} = 0$, i.e., $S(z)$ vanishes unless $z = 1$. Since

$$S(1) = p^{sm+(m-1)} \sum_{d\in R_p} \zeta_p^{md^2/2},$$

(2.30) yields

$$\begin{aligned} G(\chi) &= \zeta_q^m p^{m(s+1/2)} p^{m/2-1} \sum_{d\in R_p} \zeta_p^{md^2/2} \\ &= (\zeta_q\sqrt{q})^m p^{m/2-1} \sum_{d\in R_p} \zeta_p^{md^2/2}. \end{aligned} \tag{2.33}$$

By (2.3),

$$(\sqrt{q}\zeta_q)^m = \begin{cases} G_1(\chi)^m \zeta_8^{-m(1-p)}, & \text{if } p > 2, \\ G_1(\chi)^m \zeta_8^{-m}, & \text{if } p = 2. \end{cases} \tag{2.34}$$

By [2, Theorem 1.5.2, p. 26],

$$\sum_{d\in R_p} \zeta_p^{md^2/2} = \begin{cases} \sqrt{p}\left(\frac{m}{p}\right)\zeta_8^{1-p}, & \text{if } p > 2, \\ 1 + i^m = \sqrt{p}\left(\frac{p}{m}\right)\zeta_8^m, & \text{if } p = 2. \end{cases} \tag{2.35}$$

When p and m are odd, the law of quadratic reciprocity gives

$$\left(\frac{p}{m}\right) = \left(\frac{m}{p}\right)\zeta_8^{(1-p)(1-m)}. \tag{2.36}$$

Combining (2.33) - (2.36), we complete the proof of (2.20) in Case 2.

Case 3: $\nu(\chi) = 1,\ q = 8$.

The elements $\alpha \in \mathcal{O}_8^*$ can be written

$$\alpha = a + 2ab \qquad (a \in \mathcal{O}_2^*,\ b \in \mathcal{O}_4),$$

so

$$G(\chi) = \sum_{a\in\mathcal{O}_2^*} \chi(N(a))\zeta_8^{T(a)} \sum_{b\in\mathcal{O}_4} \chi(N(1+2b))\zeta_4^{T(ab)}. \tag{2.37}$$

Observe that

$$N(1+2b) = 1 + 2T(b) + 2(T(b)^2 - T(b^2)). \tag{2.38}$$

Write

$$a = 1 + \sum_{i=1}^{m-1} a_i\tau^i, \qquad a_i \in R_2,$$

and

$$b = \sum_{i=0}^{m-1} b_i\tau^i, \qquad b_i \in R_4.$$

We have $T(b) = mb_0$, and, since m is odd, $T(b)^2 = m^2 b_0^2 = b_0^2$. Also,

$$T(b^2) = T(b_0^2) + T(2u \sum_{i=1}^{m-1} b_i b_{m-i}).$$

Since m is odd, $\sum b_i b_{m-i}$ is even, so

$$2T(b^2) = 2T(b_0^2) = 2mb_0^2.$$

Thus (2.38) becomes

$$N(1+2b) = 1 + 2mb_0 + 2b_0^2 - 2mb_0^2. \tag{2.39}$$

Now,

$$T(ab) = mb_0 + 2mu \sum_{i=1}^{m-1} a_i b_{m-i}. \tag{2.40}$$

By (2.39) - (2.40), we see that (2.37) becomes

$$\begin{aligned} G(\chi) = \sum_{a \in \mathcal{O}_2^*} \chi(N(a)) \zeta_8^{T(a)} \sum_{b_0 \in R_4} \chi(1 + 2mb_0 + 2b_0^2(1-m)) \zeta_4^{mb_0} \\ \times \sum_{b_1,\ldots,b_{m-1} \in R_4} (-1)^{\sum_{i=1}^{m-1} a_i b_{m-i}}. \end{aligned} \tag{2.41}$$

The inner sum on $b_1, \ldots, b_{m-1}$ vanishes unless $a_1, \ldots, a_{m-1}$ are all even, in which case $a = 1$ and this inner sum equals 4^{m-1}. Thus (2.41) becomes

$$\begin{aligned} G(\chi) &= \zeta_8^m 4^{m-1} \sum_{b_0 \in R_4} \chi(1 + 2mb_0 + 2b_0^2(1-m)) \zeta_4^{mb_0} \\ &= \zeta_8^m 4^{m-1} \left\{1 + \chi(3)\zeta_4^m + \chi(5)\zeta_4^{2m} + \chi(7)\zeta_4^{3m}\right\}. \end{aligned}$$

Since $\chi(5) = -1$ by (2.5),

$$\begin{aligned} G(\chi) &= \zeta_8^m 4^{m-1} \{1 - \chi(-1)\zeta_4^m + 1 - \chi(-1)\zeta_4^m\} \\ &= \zeta_8^m 2^{2m-1} \{1 - \chi(-1)\zeta_4^m\} \\ &= \left(\sqrt{8}\zeta_8^{1-\chi(-1)}\right)^m 2^{(m-1)/2} \left(\frac{2}{m}\right) \\ &= G_1(\chi)^m 2^{(m-1)/2} \left(\frac{2}{m}\right), \end{aligned}$$

where the last equality follows from (2.3). This proves (2.20) in Case 3, which completes the proof of (2.20) for normalized χ.

We now drop the assumption that χ is normalized, and consider the general situation where χ is given by (2.7). For brevity, we rewrite (2.20) in the normalized case as

$$G(\xi) = G_1(\xi)^m A(m), \tag{2.42}$$

where

$$A(m) = \begin{cases} \left(\frac{p}{m}\right)^r p^{(m-1)/2}, & \text{if } 2 \nmid m, \\ \zeta_8^{(1-p)(1-m)} \left(\frac{m}{p}\right) \left(\frac{-Dp^{1-m}}{p}\right)^{r+1} p^{(m-1)/2}, & \text{if } 2 | m. \end{cases} \tag{2.43}$$

Applying the automorphism σ_ν to both sides of (2.42), we have, by (2.7) and (2.8),

$$G(\chi) = G_1(\chi)^m \sigma_\nu(A(m)).$$

To prove (2.20), it remains to show that

$$\sigma_\nu(A(m)) = \begin{cases} A(m), & \text{if } 2 \nmid m, \\ \left(\frac{\nu}{p}\right) A(m), & \text{if } 2|m. \end{cases} \tag{2.44}$$

If $2 \nmid m$, (2.44) follows because $A(m) \in \mathbb{Z}$. Now suppose that $2|m$ (so that $p > 2$). Then $A(m) = n\sqrt{p}i^{(p-1)^2/4}$ for some $n \in \mathbb{Z}$. Now (2.44) follows since

$$\sqrt{p}i^{(p-1)^2/4} = \sum_{x=0}^{p-1} \zeta_p^{x^2}$$

(see [2, Theorem 1.2.4, p. 15]) and

$$\sigma_\nu\left(\sum_{x=0}^{p-1} \zeta_p^{x^2}\right) = \left(\frac{\nu}{p}\right)\sum_{x=0}^{p-1} \zeta_p^{x^2}.$$

□

We remark that in the case $2|m$, (2.20) can also be written

(2.45)

$$G(\chi) = G_1(\chi)^{m-1} G_1(\chi\phi) p^{(m-1)/2} \zeta_8^{(1-p)(1-m)} \left(\frac{-Dp^{1-m}}{p}\right)^{r+1} \left(\frac{m}{p}\right), \text{ if } r \geq 2,$$

where ϕ is the Legendre symbol, viz., $\phi(x) = \left(\frac{x}{p}\right)$. To see this, write $\chi = \xi^\nu$ as in (2.7). In view of (2.4) - (2.6), $\nu(\xi\phi) = 1$, so $G_1(\xi\phi) = G_1(\xi)$ by (2.3); then, applying σ_ν to both sides of this equality, we obtain, by (2.8),

$$G_1(\chi\phi) = \left(\frac{\nu(\chi)}{p}\right) G_1(\chi), \quad \text{if } \ r \geq 2. \tag{2.46}$$

3. Evaluation of Kloosterman sums $K(\eta, z)$

In the case that $E/\mathbb{Q}$ is cyclic, p is an odd prime, and m is a prime dividing $(p-1)$, Ye [16, Theorem 1] gave essentially the following evaluation of the Kloosterman sum $K(z)$ (defined below (1.6)):

$$K(z) = p^{(m-1)/2} \left(\frac{m}{p}\right) \left(\frac{-Dp^{1-m}}{p}\right)^{(m+1)(r+1)} \zeta_8^{(1-p)(1-m)} H(z), \quad z \in R_q^*, \tag{3.1}$$

where $H(z)$ is the twisted hyper-Kloosterman sum defined by

$$H(z) = \sum_{x_1,\ldots,x_m \in R_q^*} \psi(x_2 x_3^2 \cdots x_m^{m-1}) \zeta_q^{x_1+\cdots+x_m+z/(x_1\cdots x_m)} \tag{3.2}$$

for any character ψ (mod p) of order m. (Note that H does not depend on the choice of ψ.) Our formulation (3.1) does not quite agree with the statement in [16, Theorem 1]. This is because when $m = 2$, the factor $\eta(p)$ in [16, Theorem 1, p. 1159] should be corrected to read $\eta(p)^{a+1}$, which turns out to equal $\left(\frac{-D/p}{p}\right)^{r+1}$ in our notation.

For $z \in R_q^*$ and any characters $A, B \pmod q$, define another twisted hyper-Kloosterman sum $J(A,B,z)$ by

$$J(A,B,z) = \sum_{y_1,\ldots,y_m \in R_q^*} A(y_1)B(y_1 \cdots y_m)\zeta_q^{y_1+\cdots+y_m+z/(y_1\cdots y_m)}. \tag{3.3}$$

In (3.11) below, we give a formula for $H(z)$ in terms of the sum $J(A,B,z)$ which is valid for $r \geq 2$. The sums $H(z)$ and $J(A,B,z)$ are special cases of the general twisted hyper-Kloosterman sum

$$K(A_1,\ldots,A_m,z) := \sum_{x_1,\ldots,x_m \in R_q^*} A_1(x_1)\cdots A_m(x_m)\zeta_q^{x_1+\cdots+x_m+z/(x_1\cdots x_m)},$$

which has been evaluated for $r \geq 2$ by Evans [5]. In the case $r = 1$, the sum $K(A_1,\ldots,A_m,z)$ (as well as its analogue over general finite fields) was estimated by Katz [7, pp. 48–49]. When the characters $A_1,\ldots,A_m$ are all trivial, the sum $K(A_1,\ldots,A_m,z)$ reduces to the familiar hyper-Kloosterman sum $J(1,1,z)$, evaluated for $r \geq 2$ by Smith [14]. (Some errors in Smith's formulations [14, Theorem 5] are corrected in [5].)

Using the Davenport-Hasse product formula (3.14), one can evaluate a sum related to $H(z)$ in the case $r = 1$, namely

$$\sum_{x_2,\ldots,x_m \in R_p^*} \psi(x_2x_3^2\cdots x_m^{m-1})\zeta_p^{x_2+\cdots+x_m+z/(x_2\cdots x_m)};$$

see Duke [4], Katz [7, p. 85] for evaluations of this sum and its analogue over finite fields.

The following lemma expresses the Kloosterman sums $K(\eta,z), J(A,B,z)$, and $H(z)$ in terms of Gauss sums $G(\chi)$; cf. Katz [7, p. 47].

Lemma 3.1. *Let $z \in R_q^*$ and let A, B, η be characters* $\pmod q$. *Then*

$$K(\eta,z) = \frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(z)G_1(\chi)G(\chi\eta) \tag{3.4}$$

(*where χ runs through the $\varphi(q)$ characters* $\pmod q$) *and*

$$J(A,B,z) = \frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(z)G_1(\chi)G_1(\chi AB)G_1(\chi B)^{m-1}. \tag{3.5}$$

Also, if ψ is a character of order m (in which case $m|(p-1)$), then

$$H(z) = \frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(z)G_1(\chi)\prod_{j=0}^{m-1}G_1(\chi\psi^j). \tag{3.6}$$

Proof. For $c \in R_q^*$,

$$\frac{1}{\varphi(q)}\sum_{\chi}\chi(c) = \begin{cases}1, & \text{if } c = 1,\\ 0, & \text{if } c \neq 1.\end{cases}$$

Hence,

$$\begin{aligned}\frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(z)G_1(\chi)G(\chi\eta)\\ &= \frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(z)\sum_{y\in R_q^*}\chi(y)\zeta_q^y\sum_{\alpha\in\mathcal{O}_q^*}\chi(N(\alpha))\eta(N(\alpha))\zeta_q^{T(\alpha)}\\ &= \sum_{\alpha\in\mathcal{O}_q^*}\eta(N(\alpha))\zeta_q^{T(\alpha)+z/N(\alpha)} = K(\eta,z).\end{aligned}$$

This proves (3.4). The proofs of (3.5) and (3.6) are completely analogous. □

Theorem 3.2 below extends Ye's evaluation (3.1) of $K(1,z)$ for $r\geq 2$ by showing that for any odd prime p, (3.1) holds for all (not necessarily prime) values of m dividing $p-1$. More generally, for $r\geq 2$ and any prime $p\geq 2$, Theorem 3.2 gives an evaluation of $K(\eta,z)$ for all m (not necessarily prime or a divisor of $p-1$), in terms of the sum J defined in (3.3). For evaluations of J, see [14], [5].

The case $r=1$ will be considered in Theorem 3.3.

Theorem 3.2. *Let $r\geq 2$ and $z\in R_q^*$. Let η be any character* (mod q) *and let ϕ denote the Legendre symbol, viz., $\phi(x)=\left(\frac{x}{p}\right)$. Then*

$$K(\eta,z)=p^{(m-1)/2}\left(\frac{p}{m}\right)^r J(1,\eta,z),\quad \text{if } 2\nmid m, \tag{3.7}$$

and

$$K(\eta,z)=p^{(m-1)/2}\left(\frac{m}{p}\right)\left(\frac{-Dp^{1-m}}{p}\right)^{r+1}\zeta_8^{(1-p)(1-m)}J(\phi,\eta,z),\quad \text{if } 2|m, \tag{3.8}$$

where $J(A,B,z)$ is defined by (3.3). *Moreover, for every odd prime p and every m dividing* $(p-1)$, (3.1) *holds.*

Proof. If m is odd, then by (3.4) and (2.20),

$$\begin{aligned}K(\eta,z) &= p^{(m-1)/2}\left(\frac{p}{m}\right)^r\frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(z)G_1(\chi)G_1(\chi\eta)^m\\ &= p^{(m-1)/2}\left(\frac{p}{m}\right)^r J(1,\eta,z),\end{aligned}$$

where the last equality follows from (3.5) with $A=1, B=\eta$. This proves (3.7).

If m is even, then by (3.4) and (2.45),

$$\begin{aligned}K(\eta,z) &= p^{(m-1)/2}\left(\frac{-Dp^{1-m}}{p}\right)^{r+1}\left(\frac{m}{p}\right)\zeta_8^{(1-p)(1-m)}\frac{1}{\varphi(q)}\\ &\times\sum_{\chi}\overline{\chi}(z)G_1(\chi)G_1(\chi\eta\phi)G_1(\chi\eta)^{m-1}.\end{aligned}$$

By (3.5) with $A=\phi, B=\eta$, this proves (3.8).

Next let p be an odd prime $\equiv 1 \pmod m$. It remains to prove (3.1).

Let ψ be a character (mod p) of order m and write $\chi=\xi^\nu$ as in (2.7). In view of (2.4) - (2.6), $\nu(\xi\psi^i)=1$ for all i, so that by (2.3), $G_1(\xi\psi^i)=G_1(\xi)$ for all i. Thus

$$\prod_{i=0}^{m-1}G_1(\xi\psi^i)=G_1(\xi)^m. \tag{3.9}$$

Since $\nu = \nu(\chi)$ is relatively prime to $p-1$, it follows that ν is relatively prime to m. Hence, applying σ_ν to both sides of (3.9), we obtain, by (2.8),

$$\prod_{i=0}^{m-1} G_1(\chi\psi^i) = \left(\frac{\nu}{p}\right)^{m-1} G_1(\chi)^m.$$

Thus, by (2.46),

$$\prod_{i=0}^{m-1} G_1(\chi\psi^i) = \begin{cases} G_1(\chi)^m, & \text{if } 2 \not| \, m, \\ G_1(\chi)^{m-1} G_1(\chi\phi), & \text{if } 2|m. \end{cases} \tag{3.10}$$

Putting (3.10) in (3.6) and then using (3.5), we see that for $r \geq 2$,

$$H(z) = \begin{cases} J(1,1,z), & \text{if } 2 \not| \, m, \\ J(\phi,1,z), & \text{if } 2|m. \end{cases} \tag{3.11}$$

Set $\eta = 1$ in (3.7) - (3.8) and make the substitution (3.11). Then using (2.36) for odd m and noting that $\left(\frac{p}{m}\right) = 1$ (since $p \equiv 1 \pmod{m}$), we obtain (3.1). □

For the remainder of this section, let $r = 1$. Then

$$K(\eta, z) = \sum_{\alpha \in \mathcal{O}_p^*} \eta(N(\alpha)) \zeta_p^{T(\alpha)+z/N(\alpha)}.$$

By (2.11), we can write

$$\alpha = a + a_1\tau + \cdots + a_{m-1}\tau^{m-1} \qquad (a \in R_p^*, \ a_i \in R_p).$$

Then $N(\alpha) = a^m$ and $T(\alpha) = ma$, so that

$$K(\eta, z) = p^{m-1} \sum_{a=1}^{p-1} \eta^m(a) \zeta_p^{ma+z/a^m}, \quad \text{when } \ r = 1. \tag{3.12}$$

In Theorem 3.3 below, we extend Ye's result (3.1) for $r = 1$ by showing that for any odd prime p, (3.1) holds for *all* m dividing $p-1$.

We will need the product formula of Davenport-Hasse [2, Theorem 11.3.5, p. 355] for the Gauss sums

$$\gamma(\chi) := \sum_{a=1}^{p-1} \chi(a) \zeta_p^a, \tag{3.13}$$

namely,

$$\overline{\chi}^m(m)\gamma(\chi^m) = \prod_{j=0}^{m-1} \gamma(\chi\psi^j) / \prod_{j=1}^{m-1} \gamma(\psi^j), \tag{3.14}$$

where ψ is a character (mod p) of order m (so that $m|(p-1)$). Note that $\gamma(\chi)$ is the Gauss sum $G_1(\chi)$ in the case $r = 1$. It is not difficult to show that for $p > 2$,

$$\prod_{j=1}^{m-1} \gamma(\psi^j) = p^{(m-1)/2} \left(\frac{m}{p}\right) \zeta_8^{(1-p)(m-1)}; \tag{3.15}$$

see [2, p. 352]. Substituting (3.15) into (3.14), we obtain the following version of the Davenport-Hasse formula, when $p > 2,\ m|(p-1)$:

$$\overline{\chi}^m(m)\gamma(\chi^m)p^{(m-1)/2}\left(\frac{m}{p}\right)\zeta_8^{(1-p)(m-1)} = \prod_{j=0}^{m-1}\gamma(\chi\psi^j). \tag{3.16}$$

Theorem 3.3. *Let $r = 1$ and $z \in R_p^*$, where p is an odd prime. Then* (3.1) *holds for every m dividing $(p-1)$.*

Proof. Let ψ be a character (mod p) of order m. Since by (2.19),

$$G(\chi) = p^{m-1}\overline{\chi}^m(m)\gamma(\chi^m),$$

if follows from (3.16) that

$$G(\chi) = p^{(m-1)/2}\left(\frac{m}{p}\right)\zeta_8^{(1-p)(1-m)}\prod_{j=0}^{m-1}\gamma(\chi\psi^j). \tag{3.17}$$

Substituting (3.17) into (3.4) with $\eta = 1$, we obtain

$$K(z) = p^{(m-1)/2}\left(\frac{m}{p}\right)\zeta_8^{(1-p)(1-m)}H(z), \tag{3.18}$$

by (3.6). This completes the proof, as (3.18) is the same as (3.1) in the case $r = 1$. ☐

4. A product formula for Gauss sums $G(\chi)$

In Theorem 4.1 below, we give a product formula for the Gauss sums $G(\chi)$, which in the case $m = r = 1$ reduces to the Davenport-Hasse product formula (3.16).

Theorem 4.1. *Let p be an odd prime and let ψ be a character* (mod p) *of order ℓ* (*so that $\ell|(p-1)$*). *Let χ be any character* (mod q). *Then if $r \geq 2$,*

$$\overline{\chi}^{\ell m}(\ell)G(\chi^\ell)p^{(\ell-1)(rm+m-1)/2}C(\chi) = \prod_{j=0}^{\ell-1}G(\chi\psi^j), \tag{4.1}$$

where $C(\chi) \in \{\pm 1, \pm i\}$ is defined by

(4.2)

$$C(\chi) := \begin{cases} \left(\frac{\nu(\chi)}{p}\right)^{\ell-1}, & \text{if } 2\not| m,\ 2|r, \\ \zeta_8^{(1-p)(\ell-1)}\left(\frac{\ell}{p}\right)\left(\frac{m}{p}\right)^{\ell-1}\left(\frac{\nu(\chi)}{p}\right)^{(\ell-1)(m-1)}, & \text{if } 2\not| r, \\ \zeta_8^{(1-p)(1-m)(\ell-1)}\left(\frac{\ell}{p}\right)\left(\frac{m}{p}\right)^{\ell-1}\left(\frac{-Dp^{1-m}}{p}\right)^{\ell-1}\left(\frac{\nu(\chi)}{p}\right)^{\ell-1}, & \text{if } 2|m,\ 2|r, \end{cases}$$

with $\nu(\chi)$ defined by (2.4) *and* (2.6). *If in the case $r = 1$, we define the* (*previously undefined*) *expression $\nu(\chi)$ by setting $\nu(\chi) = 1$, then* (4.1) *also holds when $r = 1$, provided that $(m, \ell) = 1$.*

Proof. We first consider the case $r \geq 2$. If χ is nonprimitive, then both sides of (4.1) vanish by Theorem 2.2. Assume therefore that χ is primitive.

First suppose that χ is normalized, i.e., $\nu(\chi) = 1$. In this case $\chi\psi^j$ is normalized, i.e., $\nu(\chi\psi^j) = 1$, for each j. Hence by (2.20) and (2.3),

$$G(\chi) = G(\chi\psi^j), \qquad \text{for all } j. \tag{4.3}$$

Choose b relatively prime to $q(p-1)$ such that $b \equiv \ell \pmod{q}$, and define c by $bc \equiv 1 \pmod{q(p-1)}$. We claim that

$$\sum_{\alpha \in \mathcal{O}_q^*} \chi^b(N(\alpha))\zeta_q^{T(\alpha b)} = \sum_{\alpha \in \mathcal{O}_q^*} \chi^\ell(N(\alpha))\zeta_q^{T(\alpha \ell)}. \tag{4.4}$$

To verify (4.4), apply σ_c to both sides to obtain $G(\chi)$ on the left and $G(\chi^{c\ell})$ on the right; then note that $\nu(\chi) = \nu(\chi^{c\ell}) = 1$, so that $G(\chi) = G(\chi^{c\ell})$ by (2.20) and (2.3).

We can rewrite (4.4) as

$$\sigma_b G(\chi) = \overline{\chi}^{\ell m}(\ell) G(\chi^\ell). \tag{4.5}$$

In view of (4.3) and (4.5), the proposed equality (4.1) is equivalent to

$$\sigma_b(G(\chi)) p^{(\ell-1)(rm+m-1)/2} C(\chi) = G(\chi)^\ell. \tag{4.6}$$

By (2.42) and by (2.44) with $\nu = b$, the left side of (4.6) equals

$$\sigma_b(G_1(\chi)^m) \left(\frac{\ell}{p}\right)^{m+1} A(m) p^{(\ell-1)(rm+m-1)/2} C(\chi),$$

while the right side of (4.6) equals

$$G_1(\chi)^{m\ell} A(m)^\ell.$$

Thus (4.6) (and hence (4.1)) is equivalent to

$$C(\chi) = A(m)^{\ell-1} \left(\frac{\ell}{p}\right)^{m+1} p^{(1-\ell)(rm+m-1)/2} G_1(\chi)^{m\ell} / \sigma_b(G_1(\chi)^m). \tag{4.7}$$

Substitute the value of $G_1(\chi)$ given by (2.3) into (4.7) to see, after a tedious calculation, that (4.7) is equivalent to (4.2) when $\nu(\chi) = 1$. This completes the proof of (4.1) for $r \geq 2$ when $\nu(\chi) = 1$. To prove (4.1) for $r \geq 2$ and general $\nu(\chi)$, first write down (4.1) with ξ in place of χ (in the notation of (2.7)). Then, applying σ_ν to both sides, we obtain (4.1). This completes the proof of the theorem in the case $r \geq 2$.

Now let $r = 1$ and assume that $(m, \ell) = 1$. It remains to prove

$$\overline{\chi}^{\ell m}(\ell) G(\chi^\ell) p^{(\ell-1)(m-1/2)} C = \prod_{j=0}^{\ell-1} G(\chi\psi^j), \tag{4.8}$$

where

$$C = \zeta_8^{(1-p)(\ell-1)} \left(\frac{\ell}{p}\right) \left(\frac{m}{p}\right)^{\ell-1}. \tag{4.9}$$

Since, by (2.19),

$$G(\chi) = \overline{\chi}^m(m) p^{m-1} \gamma(\chi^m)$$

for every character $\chi \pmod{p}$, we have in particular,

$$G(\chi\psi^j) = \overline{\chi}^m(m) \overline{\psi}(m)^{mj} p^{m-1} \gamma(\chi^m \psi^{mj}) \tag{4.10}$$

for all j, and

$$\overline{\chi}^{\ell m}(\ell) G(\chi^\ell) = \overline{\chi}^{\ell m}(m\ell) p^{m-1} \gamma(\chi^{m\ell}). \tag{4.11}$$

Because $(m, \ell) = 1$, it follows that ψ^{mj} runs through the same characters as ψ^j does when j runs through $0, 1, 2, \ldots, \ell - 1$. Thus, by (4.10),

$$\prod_{j=0}^{\ell-1} G(\chi\psi^j) = \overline{\chi}^{m\ell}(m) p^{\ell(m-1)} \left(\frac{m}{p}\right)^{\ell-1} \prod_{j=0}^{\ell-1} \gamma(\chi^m \psi^j). \tag{4.12}$$

By (3.16) with $m = \ell$,

$$\prod_{j=0}^{\ell-1} \gamma(\chi^m \psi^j) = \overline{\chi}^{m\ell}(\ell) p^{(\ell-1)/2} \gamma(\chi^{m\ell}) \left(\frac{\ell}{p}\right) \zeta_8^{(1-p)(\ell-1)}. \tag{4.13}$$

Multiplying (4.13) by (4.12) and then dividing the resulting equality by (4.11), we obtain (4.8). □

References

[1] J. Arthur and L. Clozel, *Simple Algebras, Base Change, and the Advanced Theory of the Trace Formula*, Annals of Math. Studies, No. 120, Princeton University Press, Princeton, 1989. MR **90m:**22041

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, N.Y., 1998. MR **99d:**11092

[3] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172**(1934), 151-182.

[4] W. Duke, *On multiple Salié sums*, Proc. Amer. Math. Soc. **114**(1992), 623-625. MR **92f:**11113

[5] R. J. Evans, *Twisted hyper-Kloosterman sums over finite rings of integers*, Proceedings of the Millennial Conference on Number Theory, University of Illinois (May 21-26, 2000), A K Peters, Natick, MA, to appear in 2001.

[6] T. Funakura, *A generalization of the Chowla-Mordell theorem on Gaussian sums*, Bull. London Math. Soc. **24**(1992), 424-430. MR **93e:**11094

[7] N. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Annals of Math. Studies, No. 116, Princeton University Press, Princeton, 1988. MR **91a:**11028

[8] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, N. Y., 1977. MR **57:**5964

[9] J.-L. Mauclaire, *Sommes de Gauss modulo p^α I*, Proc. Jap. Acad. Ser. A **59**(1983), 109-112. MR **85f:**11062a

[10] J.-L. Mauclaire, *Sommes de Gauss modulo p^α II*, Proc. Jap. Acad. Ser. A **59**(1983), 161-163. MR **85f:**11062a

[11] W. Narkiewicz, *Elementary and Analytic Theory of Numbers*, Springer-Verlag, Berlin and PWN-Polish Scientific Publishers, Warsaw, 1990. MR **91h:**11107

[12] R. Odoni, *On Gauss sums* (mod p^n), $n \geq 2$, Bull. London Math. Soc. **5**(1973), 325-327. MR **48:**6020

[13] H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$*, Math. Z. **34**(1932), 91-109.

[14] R. Smith, *On n-dimensional Kloosterman sums*, J. Number Theory 11 (1979), 324-343. MR **80i:**11052

[15] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Springer-Verlag, N. Y., 1997. MR **97h:**11130

[16] Y. Ye, *A hyper-Kloosterman sum identity*, Science in China (Series A) **41**(1998), 1158-1162. MR **99m:**11094

[17] Y. Ye, *The lifting of an exponential sum to a cyclic algebraic number field of prime degree*, Trans. Amer. Math. Soc. **350**(1998), 5003-5015. MR **99b:**11092

[18] Y. Ye, Personal communication, November, 1999.

Department of Mathematics, University of California at San Diego, La Jolla, California 92093-0112

E-mail address: revans@ucsd.edu