THE LIFTING OF AN EXPONENTIAL SUM
TO A CYCLIC ALGEBRAIC NUMBER FIELD
OF PRIME DEGREE

YANGBO YE

ABSTRACT. Let E be a cyclic algebraic number field of prime degree. We prove
an identity which lifts an exponential sum similar to the Kloosterman sum to
an exponential sum taken over certain algebraic integers in E.

1. INTRODUCTION

Based on the relative trace formula for $GL(2)$ (Ye [13] and Jacquet and Ye [8])
and inspired by early work of Zagier [15], Ye [14] established a lifting identity for
Kloosterman sums. Let $E = \mathbb{Q}(\sqrt{\tau})$ be a quadratic field with a square-free integer
τ, and let c be a positive odd integer with $(c, \tau) = 1$. Assume that for any prime
factor p of c we have $\left(\frac{\tau}{p}\right) = -1$. Then for any nonzero integers m and n with
$(m, c) = (n, c) = 1$ we have

$$(1) \qquad \sum_{\substack{1 \leq x \leq c, \\ (x, c) = 1}} e^{2\pi i (xm + \bar{x}n)/c} = (-1)^{\Omega(c)} \sum_{\substack{1 \leq a \leq c,\, 1 \leq b \leq c, \\ a^2 - \tau b^2 \equiv mn \,(\mathrm{mod}\, c)}} e^{4\pi i a/c}$$

where $\bar{x}$ is the inverse of x modulo c. Here $\Omega(c)$ is the number of prime factors of
c counting multiplicity. Note that the exponential sum on the right side of (1) is
actually a sum taken over some algebraic integers in $E = \mathbb{Q}(\sqrt{\tau})$.

In this paper we will prove a similar identity which lifts an exponential sum to
a cyclic algebraic number field of prime degree. The main results are given in the
following theorem.

Theorem 1. *Let E be a cyclic algebraic number field of an odd prime degree ℓ
with an integral basis $\{1, \omega_1, \ldots, \omega_{\ell-1}\}$. Let m be a positive integer such that every
prime factor p of m is unramified (inert or splitting) in E and larger than ℓ. Assume
that $p^2 | m$ for any prime factor p of m. Then for any integer b relatively prime to*

m we have

$$\sum_{\substack{x \bmod m, \\ (x,m)=1}} e^{2\pi i (x - \bar{b}\, (\overline{\ell+1})^{\ell+1} x^{\ell+1})/m}$$

$$(2) \qquad = m^{1-\ell/2} \prod_{\substack{p|m \text{ to an} \\ \text{odd power}}} \left(\frac{2b(\ell+1)}{p}\right) \varepsilon_p^{-\ell}$$

$$\cdot \sum_{\substack{x_0,\dots,x_{\ell-1} \bmod m, \\ \mathrm{N}_{E/\mathbb{Q}}(x_0+x_1\omega_1+\cdots+x_{\ell-1}\omega_{\ell-1})\equiv b \,(\bmod\, m)}} e^{2\pi i \mathrm{tr}_{E/\mathbb{Q}}(x_0+x_1\omega_1+\cdots+x_{\ell-1}\omega_{\ell-1})/m},$$

where $\bar{b}$ and $\overline{\ell+1}$ are inverses of b and $\ell+1$ modulo m, respectively. Here as usual $\varepsilon_p = 1$ if $p \equiv 1 \,(\mathrm{mod}\, 4)$ and $\varepsilon_p = i$ if $p \equiv 3 \,(\mathrm{mod}\, 4)$.

Note that the assumptions in Theorem 1 exclude only finitely many primes from being prime factors of m. We can rewrite the product in (2) using the Jacobi symbol

$$\left(\frac{2b(\ell+1)}{m}\right) \cdot \prod_{\substack{p|m \text{ to an} \\ \text{odd power}}} \varepsilon_p^{-\ell}.$$

Also note that it is necessary to have the assumption that m is divisible by the square of every prime dividing it: the identity (2) does not hold otherwise. This assumption seems to be related to the phenomena that exponential sums "trivialize" when $p^2|m$ for every $p|m$. It would be interesting to see if an identity of this kind holds without this assumption.

As an example let us take the cyclic cubic field E generated by a root θ of the polynomial $P(x) = x^3 - 3x - 1$ (cf. Cohen [1]). Then the conjugates of θ are $\sigma(\theta) = -2 - \theta + \theta^2$ and $\sigma^2(\theta) = 2 - \theta^2$; $\{1, \theta, \sigma(\theta)\}$ is an integral basis with the trace map $\mathrm{tr}_{E/\mathbb{Q}}(x_0 + x_1\theta + x_2\sigma(\theta)) = 3x_0$ and the norm map

$$\mathrm{N}_{E/\mathbb{Q}}(x_0 + x_1\theta + x_2\sigma(\theta))$$
$$= x_0^3 + x_1^3 + x_2^3 - 3x_0x_1^2 - 3x_0x_2^2 + 3x_1^2x_2 - 6x_1x_2^2 - 3x_0x_1x_2.$$

Then for any positive integer m which satisfies $(m,6)=1$ and $p^2|m$ for any $p|m$ we have

$$\sum_{\substack{x \bmod m, \\ (x,m)=1}} e^{2\pi i (x - \overline{4^4 b}\, x^4)/m}$$

$$= m^{-1/2} \prod_{\substack{p|m \text{ to an} \\ \text{odd power}}} \left(\frac{2b}{p}\right) \varepsilon_p \cdot \sum_{\substack{x_0,x_1,x_2 \bmod m, \\ \mathrm{N}_{E/\mathbb{Q}}(x_0+x_1\theta+x_2\sigma(\theta))\equiv b \,(\bmod\, m)}} e^{6\pi i x_0/m}$$

when $(b,m)=1$.

The work is inspired by an identity of exponential sums over the finite field $\mathbf{F}_q$ with $q = p^a \equiv 1 \,(\mathrm{mod}\, 3)$ which is proved by Duke and Iwaniec [3] and Mao and

Rallis [11]. When $q = p \equiv 1 \pmod 3$ this identity is

$$(3) \qquad \sum_{1 \le x \le p} e^{2\pi i(x + ax^3)/p} = \sum_{\substack{1 \le x \le p, \\ (x,p)=1}} \varphi(x\bar{a}) e^{2\pi i(x - \overline{3^3 ax})/p},$$

where a is a number relatively prime to p, $\bar{a}$ is the inverse of a modulo p, and φ is a multiplicative character of order three. Indeed, comparing the left side of (3) with (2), we see that it is essentially an exponential sum corresponding to a quadratic field. The right side of (3) confirms this observation because apart from the cubic character φ it is a Kloosterman sum related to the same quadratic field via (1).

According to [13] and [14], the identity (1) plays a crucial role in the fundamental lemma of the relative trace formula for $GL(2)$ between distributions over a ground algebraic number field and its quadratic extension. This relative trace formula was used to give a new proof of the quadratic base change for $GL(2)$ (see remarks in Jacquet [6]). On the other hand, according to [11] the identity (3) is equivalent to the fundamental lemma of a relative trace formula between distributions on $SL(2)$ and its threefold cover $\widetilde{SL}^3(2)$, where $SL(2) \times \widetilde{SL}^3(2)$ is embedded in a group of type G_2. This relative trace formula might be used to deduce a correspondence between automorphic forms on $SL(2)$ and $\widetilde{SL}^3(2)$. Based on the same consideration, the identity in Theorem 1 or an improved version might be used to establish a relative trace formula which could be applied to the study of the correspondence between automorphic forms on $GL(2)$ over the ground field and its cyclic extensions.

Besides its potential applications to automorphic forms, the identity (2) certainly has significance on its own right. Comparing it with (1), we can see the role played by the exponential sum on the left side of (2) is similar to that of the Kloosterman sum. This indicates that the Kloosterman sum and the expression on the left side of (3) are basically exponential sums related to quadratic number fields, while the sum on the left side of (2) is related to a cyclic number field of degree ℓ.

In the following sections we will see that the proof of (2) is partly based on the Davenport–Hasse formulas for Gauss sums of a new type. Indeed, this approach was first used by Katz [9], who established certain identities for Kloosterman sums using a Davenport–Hasse relation based on a power map $x \mapsto x^N$. The Kloosterman sums in his identities are similar to some of our local exponential sums over a p-adic field which splits in E (see the proof of Theorem 3).

The author would like to thank the referees for their helpful suggestions.

2. The Davenport–Hasse relation

Let χ be a multiplicative character modulo a prime p. The Gauss sum is

$$\tau(\chi) = \sum_{\substack{n \bmod p, \\ (n,p)=1}} \chi(n) e^{2\pi in/p}.$$

If φ is a multiplicative character of order n modulo p, then a Davenport–Hasse formula for Gauss sums is (Davenport and Hasse [2])

$$\tau(\chi^n)\tau(\varphi) \cdots \tau(\varphi^{n-1}) = \chi^n(n)\tau(\chi)\tau(\chi\varphi) \cdots \tau(\chi\varphi^{n-1}).$$

This formula has been actively reexamined recently by many authors (e.g. Kubert and Lichtenbaum [10], Greene and Stanton [4], and Duke and Iwaniec [3]), but the

discussions are mainly centered on the case of finite fields. To study this relationship over the p-adic field $\mathbb{Q}_p$, we use the local ε-factor (see e.g. Tate [12])

$$\varepsilon(\chi, \psi_p; dx) \quad = \quad 1 \qquad\qquad\qquad \text{if } \chi \text{ is unramified;}$$

$$= \int_{p^{-a}R_p^\times} \chi^{-1}(x)\psi_p(x)\, dx \qquad \begin{array}{l}\text{if } \chi \text{ is ramified with conductor} \\ \text{exponent equal to } a,\end{array}$$

where the measure dx on $\mathbb{Q}_p$ is normalized by $\mathrm{vol}(R_p) = 1$. Here we have chosen an additive character $\psi = \psi_{\mathbb{R}} \prod_{p<\infty} \psi_p$ on the adele ring $\mathbb{Q}_A$ trivial on $\mathbb{Q}$ with $\psi_{\mathbb{R}}(x) = e^{2\pi i x}$ and the order of the local character ψ_p being zero for any $p < \infty$. If χ is a ramified character on $\mathbb{Q}_p^\times$ with conductor exponent $a(\chi)$ equal to 1, we have

$$\tau(\chi) = \chi(p)\bar\varepsilon(\chi, \psi_p; dx).$$

Let φ be a ramified character on $\mathbb{Q}_p^\times$ with $\varphi^n = 1$ such that the conductor exponents $a(\chi) = a(\chi\varphi) = \cdots = a(\chi\varphi^{n-1}) = 1$. Then the Davenport–Hasse formula takes the form

$$\varepsilon(\chi^n, \psi_p; dx)\varepsilon(\varphi, \psi_p; dx)\cdots\varepsilon(\varphi^{n-1}, \psi_p; dx)$$
$$= \bar\chi^n(n)\varepsilon(\chi, \psi_p; dx)\varepsilon(\chi\varphi, \psi_p; dx)\cdots\varepsilon(\chi\varphi^{n-1}, \psi_p; dx).$$

What we need in this article is a formula of Davenport–Hasse type with an unramified character φ. Note that when φ is unramified we have

$$\varepsilon(\varphi, \psi_p; dx) = \cdots = \varepsilon(\varphi^{n-1}, \psi_p; dx) = 1$$

and $\varepsilon(\chi\varphi, \psi_p; dx) = \varphi(q)\varepsilon(\chi, \psi_p; dx)$. Also note that the conditions $a(\chi) = a(\chi\varphi) = \cdots = a(\chi\varphi^{n-1})$ hold automatically in this case.

Theorem 2. *Let p be a prime greater than n and let χ be a ramified character with conductor exponent $a(\chi) = a > 1$. Set $q = p^a$. Then*

$$(4) \quad \varepsilon(\chi^n, \psi_p; dx) \prod_{1<j\leq n} \int_{p^{[a/2]}R_p} \chi\left(1 + \frac{j-1}{2j}y_j^2\right) dy_j = \bar\chi^n(n)q^{1-n}\left(\varepsilon(\chi, \psi_p; dx)\right)^n.$$

If a is even, then the above can be simplified:

$$\varepsilon(\chi^n, \psi_p; dx) = \bar\chi^n(n)q^{(1-n)/2}\left(\varepsilon(\chi, \psi_p; dx)\right)^n.$$

We note the similarity between this identity and another Davenport–Hasse formula ([2], (0.8)):

$$(5) \qquad\qquad\qquad \tau\left(\chi \circ \mathrm{N}_{K/k}\right) = \left(\tau(\chi)\right)^n,$$

where K is a finite extension of degree n of the finite field k of $q = p^a$ elements and $\mathrm{N}_{K/k}$ is the norm map from K to k. Over the p-adic field $\mathbb{Q}_p$, (5) takes the form

$$(6) \qquad \begin{aligned}\lambda_{E_p/\mathbb{Q}_p}(\psi_p)&\varepsilon\left(\chi \circ \mathrm{N}_{E_p/\mathbb{Q}_p}, \psi_p \circ \mathrm{tr}_{E_p/\mathbb{Q}_p}; d\beta\right) \\ &= \varepsilon(\chi, \psi_p; dx)\varepsilon(\chi\eta_p, \psi_p; dx)\cdots\varepsilon(\chi\eta_p^{\ell-1}, \psi_p; dx),\end{aligned}$$

where E_p is a cyclic extension of $\mathbb{Q}_p$ of prime degree ℓ, η_p is a nontrivial multiplicative character of $\mathbb{Q}_p$ of order ℓ which is trivial on $\mathrm{N}_{E_p/\mathbb{Q}_p}(E_p^\times)$, and $d\beta$ is a suitable Haar measure on E_p. Here the local factor $\lambda_{E_p/\mathbb{Q}_p}(\psi_p)$ is defined as in Jacquet and Langlands [7] and it is equal to 1 when $\mathbb{Q}_p$ is unramified in E_p. When this is the

case, the measure $d\beta$ is the one given by $\mathrm{vol}(R_{E_p}) = 1$. This is indeed the base change formula for $GL(1)$ (cf. Gérardin and Labesse [5]). We will use (6) later.

Proof of Theorem 2. As before, let χ be a ramified character with conductor exponent $a(\chi) = a$, and set $q = p^a$. Then

$$
\left(\varepsilon(\chi, \psi_p; dx)\right)^n = \int_{p^{-a}R_p^\times} \chi^{-1}(x_1)\psi_p(x_1)\, dx_1 \cdots \int_{p^{-a}R_p^\times} \chi^{-1}(x_n)\psi_p(x_n)\, dx_n
$$

$$
= \int_{(p^{-a}R_p^\times)^n} \chi^{-1}(x_1\cdots x_n)\psi_p(x_1 + \cdots + x_n)\, dx_1 \cdots dx_n.
$$

Changing variables $x_i = x_1 y_i$ for $i = 2,\ldots,n$, we get

$$
q^{n-1}\int_{(R_p^\times)^{n-1}} \chi^{-1}(y_2\cdots y_n)\, dy_2 \cdots dy_n \int_{p^{-a}R_p^\times} \bar{\chi}^n(x_1)\psi_p(x_1(1 + y_2 + \cdots + y_n))\, dx_1.
$$

Since $p > n$, we know that $a(\chi^n) = a$ and the inner integral above vanishes unless $1 + y_2 + \cdots + y_n \in R_p^\times$. Thus

$$
\left(\varepsilon(\chi, \psi_p; dx)\right)^n
$$

$$
= q^{n-1}\varepsilon(\chi^n, \psi_p; dx) \int_{\substack{y_2,\ldots,y_n \in R_p^\times,\\ 1+y_2+\cdots+y_n \in R_p^\times}} \chi\left(\frac{(1 + y_2 + \cdots + y_n)^n}{y_2\cdots y_n}\right) dy_2 \cdots dy_n.
$$

The theorem then follows from the following lemma.

Lemma. *Let χ be a ramified character with $a(\chi) = a > 1$ and $q = p^a$. Assume that $p > n$. Then*

(7)
$$
\int_{\substack{y_2,\ldots,y_n \in R_p^\times,\\ 1+y_2+\cdots+y_n \in R_p^\times}} \chi\left(\frac{(1 + y_2 + \cdots + y_n)^n}{y_2\cdots y_n}\right) dy_2 \cdots dy_n
$$

$$
= \chi^n(n) \prod_{1 < j \leq n} \int_{p^{[a/2]}R_p} \chi\left(1 + \frac{j-1}{2j}y_j^2\right) dy_j.
$$

If a is even, then the right side above equals $\chi^n(n)q^{(1-n)/2}$.

Proof. We set $y_2,\ldots,y_{n-1} \in R_p^\times$ and $y_n = y_0(1 + m)$, where

$$
y_0 \in \left(R_p^\times - \left(-(1 + y_2 + \cdots + y_{n-1}) + pR_p\right)\right)\Big/\left(1 + p^{[(a+1)/2]}R_p\right)
$$

and $m \in p^{[(a+1)/2]}R_p$. Then the integrand on the left side of (7) equals

$$
\chi\left(\frac{(1 + y_2 + \cdots + y_{n-1} + y_0)^n}{y_2\cdots y_{n-1}y_0}\right)\chi\left(1 - \frac{1 + y_2 + \cdots + y_{n-1} - (n-1)y_0}{1 + y_2 + \cdots + y_{n-1} + y_0}m\right).
$$

Hence the integral with respect to m is nonzero only if $(n-1)y_0 \in 1 + y_2 + \cdots + y_{n-1} + p^{[a/2]}R_p$; note that here $[a/2] \geq 1$ because we have assumed $a > 1$. Since $p > n$ we see that $y_0 \in (1 + y_2 + \cdots + y_{n-1})/(n-1) + p^{[a/2]}R_p$, and the integral with respect to y_n on the left side of (7) is actually taken over

$$
y_n \in (1 + y_2 + \cdots + y_{n-1})/(n-1) + p^{[a/2]}R_p \quad \text{with } 1 + y_2 + \cdots + y_{n-1} \in R_p^\times.
$$

Consequently

$$\int\limits_{\substack{y_2,\dots,y_n \in R_p^\times, \\ 1+y_2+\cdots+y_n \in R_p^\times}} \chi\Big(\frac{(1+y_2+\cdots+y_n)^n}{y_2\cdots y_n}\Big)\, dy_2\cdots dy_n$$

$$= \int\limits_{\substack{y_2,\dots,y_{n-1} \in R_p^\times, \\ 1+y_2+\cdots+y_{n-1} \in R_p^\times}} dy_2\cdots dy_{n-1}$$

$$\cdot \int\limits_{\frac{1+y_2+\cdots+y_{n-1}}{n-1}+p^{[a/2]}R_p} \chi\Big(\frac{(1+y_2+\cdots+y_n)^n}{y_2\cdots y_n}\Big)\, dy_n.$$

Setting $y_n = (1+y_2+\cdots+y_{n-1})/(n-1)+y$ with $y \in p^{[a/2]}R_p$, we can rewrite the integrand as

$$\chi\Big(\frac{n^n}{(n-1)^{n-1}}\Big)\chi\Big(\frac{(1+y_2+\cdots+y_{n-1})^{n-1}}{y_2\cdots y_{n-1}}\Big)\chi\Big(1+\frac{(n-1)^3 y^2/(2n)}{(1+y_2+\cdots+y_{n-1})^2}\Big).$$

Changing variables, we get

$$\int\limits_{\substack{y_2,\dots,y_n \in R_p^\times, \\ 1+y_2+\cdots+y_n \in R_p^\times}} \chi\Big(\frac{(1+y_2+\cdots+y_n)^n}{y_2\cdots y_n}\Big)\, dy_2\cdots dy_n$$

$$= \int\limits_{\substack{y_2,\dots,y_{n-1} \in R_p^\times, \\ 1+y_2+\cdots+y_{n-1} \in R_p^\times}} \chi\Big(\frac{(1+y_2+\cdots+y_{n-1})^{n-1}}{y_2\cdots y_{n-1}}\Big)\, dy_2\cdots dy_{n-1}$$

$$\cdot \int\limits_{p^{[a/2]}R_p} \chi\Big(\frac{n^n}{(n-1)^{n-1}}\Big)\chi\Big(1+\frac{(n-1)y^2}{2n}\Big)\, dy.$$

By an induction argument we get the first formula in the lemma. The second formula is a direct consequence of the first.   Q.E.D.

To prove Theorem 1 we want to write (4) in a different way:

$$\varepsilon(\chi^n,\psi_p;dx)\varepsilon(\bar\chi,\psi_p;dx) \prod_{1<j\le n}\int\limits_{p^{[a/2]}R_p} \chi\Big(1+\frac{j-1}{2j}y_j^2\Big)\, dy_j$$

$$= \bar\chi^n(n)q^{1-n}\varepsilon(\bar\chi,\psi_p;dx)\Big(\varepsilon(\chi,\psi_p;dx)\Big)^n.$$

By the classical identity $\varepsilon(\chi,\psi_p;dx)\varepsilon(\bar\chi,\psi_p;dx) = \chi(-1)q$ for ramified χ with $a(\chi) = a$, we can rewrite the right side above as

$$\chi(-1)\bar\chi^n(n)q^{2-n}\Big(\varepsilon(\chi,\psi_p;dx)\Big)^{n-1}.$$

Now we assume that $\ell = n-1$ is an odd prime and $p > n$. Let E be a cyclic algebraic number field of degree ℓ such that p is inert unramified in E. Let $\eta = \eta_\mathbb{R}\prod_{p<\infty}\eta_p$ be the idele class character of $\mathbb{Q}$ attached to E by the abelian class field theory. Then η_p is a nontrivial unramified character on $\mathbb{Q}_p^\times$ with $\eta_p^\ell = 1$. Since ℓ is an odd prime and $\ell|(1+\cdots+(\ell-1))$, we have $\eta_p\cdots\eta_p^{\ell-1} = 1$. Writing $\varepsilon(\chi,\psi_p;dx) =$

$\eta_p^{-j}(q)\varepsilon(\chi\eta_p^j, \psi_p; dx)$ for $0 \le j < \ell$, we can express the Davenport–Hasse relation in the following way:

$$\varepsilon(\chi^n, \psi_p; dx)\varepsilon(\bar{\chi}, \psi_p; dx) \prod_{1<j\le n} \int_{p^{[a/2]}R_p} \chi\Big(1 + \frac{j-1}{2j}y_j^2\Big) dy_j$$

$$= \bar{\chi}(-n^n)q^{2-n} \prod_{0\le j<\ell} \varepsilon(\chi\eta_p^j, \psi_p; dx).$$

By (6) we get

(8)
$$\varepsilon(\chi^n, \psi_p; dx)\varepsilon(\bar{\chi}, \psi_p; dx) \prod_{1<j\le n} \int_{p^{[a/2]}R_p} \chi\Big(1 + \frac{j-1}{2j}y_j^2\Big) dy_j$$

$$= \bar{\chi}(-n^n)q^{2-n}\varepsilon\Big(\chi \circ \mathrm{N}_{E_p/\mathbb{Q}_p}, \psi_p \circ \mathrm{tr}_{E_p/\mathbb{Q}_p}; d\beta\Big)$$

because $\lambda_{E_p/\mathbb{Q}_p}(\psi_p) = 1$ in our case.

3. THE EXPONENTIAL SUMS

Let us first compute the expression on the left side of (8):

$$\varepsilon(\chi^n, \psi_p; dx)\varepsilon(\bar{\chi}, \psi_p; dx) \prod_{1<j\le n} \int_{p^{[a/2]}R_p} \chi\Big(1 + \frac{j-1}{2j}y_j^2\Big) dy_j$$

$$= \int_{p^{-a}R_p^\times} \chi^{-n}(x)\psi_p(x)\, dx$$

$$\cdot \int_{p^{-a}R_p^\times} \chi(z)\psi_p(z)\, dz \int_{(p^{[a/2]}R_p)^{n-1}} \chi\Big(1 + \sum_{1<j\le n}\frac{j-1}{2j}y_j^2\Big) dy_2 \cdots dy_n.$$

If we change variables from x and z to x/q and z/q, we get

$$q^2\chi(q^{n-1}) \int_{\substack{x,z\in R_p^\times,\\ y_2,\dots,y_n\in p^{[a/2]}R_p}} \chi\Big(\frac{z}{x^n}\Big(1 + \sum_{1<j\le n}\frac{j-1}{2j}y_j^2\Big)\Big)\psi_p\Big(\frac{x+z}{q}\Big) dx\, dy_2 \cdots dy_n\, dz,$$

or, with another change of variables,

$$q^2\chi(q^{n-1}) \int_{\substack{x,z\in R_p^\times,\\ y_2,\dots,y_n\in p^{[a/2]}R_p}} \chi(z)\psi_p\Big(\frac{x}{q} + \frac{x^n z}{q(1 + \sum_{1<j\le n}\frac{j-1}{2j}y_j^2)}\Big) dx\, dy_2 \cdots dy_n\, dz.$$

Since the order of ψ_p is zero, we can modify this integral to get

$$q^2\chi(q^{n-1}) \int_{R_p^\times} \chi^{-1}(z)\, dz$$

$$\cdot \int_{\substack{x\in R_p^\times,\\ y_2,\dots,y_n\in p^{[a/2]}R_p}} \psi_p\Big(\frac{1}{q}\Big(x + \frac{x^n}{z}\Big(1 - \sum_{1<j\le n}\frac{j-1}{2j}y_j^2\Big)\Big)\Big) dx\, dy_2 \cdots dy_n.$$

Note that $\ell = n - 1$ is an odd prime and hence n is even. Changing variables from y_j to $jzx^{-n/2}y_j$, we get

$$q^2\chi(q^{n-1}) \int\limits_{R_p^\times} \chi^{-1}(z)\,dz \int\limits_{R_p^\times} \psi_p\Big(\frac{1}{q}\Big(x + \frac{x^n}{z}\Big)\Big)\,dx$$

$$\cdot \int\limits_{(p^{[a/2]}R_p)^{n-1}} \bar{\psi}_p\Big(\sum_{1<j\le n} \frac{j(j-1)z}{2q}y_j^2\Big)\,dy_2\cdots dy_n.$$

If a is even, then the integrand of the innermost integral is equal to 1, and hence

(9)
$$\varepsilon(\chi^n, \psi_p; dx)\varepsilon(\bar{\chi}, \psi_p; dx) \prod_{1<j\le n} \int\limits_{p^{[a/2]}R_p} \chi\Big(1 + \frac{j-1}{2j}y_j^2\Big)\,dy_j$$

$$= q^{2-(n-1)/2}\chi(q^{n-1}) \int\limits_{R_p^\times} \chi^{-1}(z)\,dz \int\limits_{R_p^\times} \psi_p\Big(\frac{1}{q}\Big(x + \frac{x^n}{z}\Big)\Big)\,dx.$$

If a is odd, however, the innermost integral above equals a product of the Weil constants

$$\int\limits_{(p^{[a/2]}R_p)^{n-1}} \bar{\psi}_p\Big(\sum_{1<j\le n} \frac{j(j-1)z}{2q}y_j^2\Big)\,dy_2\cdots dy_n$$

$$= q^{-(n-1)/2} \prod_{1<j\le n} \gamma\Big(\frac{j(j-1)z}{p}, \bar{\psi}_p\Big),$$

where we have set

$$\int\limits_{R_p} \psi_p\Big(\frac{bx^2}{2}\Big)\,dx = |b|_p^{-1/2}\gamma(b, \psi_p)$$

for $|b|_p > 1$. Since $p > \ell$ is odd, we know that

$$\gamma\Big(\frac{j(j-1)z}{p}, \bar{\psi}_p\Big) = \Big(\frac{2j(j-1)z}{p}\Big)\varepsilon_p.$$

Consequently

$$\prod_{1<j\le n} \gamma\Big(\frac{j(j-1)z}{p}, \bar{\psi}_p\Big) = \prod_{1<j\le n} \Big(\frac{2j(j-1)z}{p}\Big)\varepsilon_p = \Big(\frac{2nz}{p}\Big)\varepsilon_p^\ell.$$

Therefore when a is odd we have

(10)
$$\varepsilon(\chi^n, \psi_p; dx)\varepsilon(\bar{\chi}, \psi_p; dx) \prod_{1<j\le n} \int\limits_{p^{[a/2]}R_p} \chi\Big(1 + \frac{j-1}{2j}y_j^2\Big)\,dy_j$$

$$= q^{2-(n-1)/2}\chi(q^{n-1}) \int\limits_{R_p^\times} \chi^{-1}(z)\,dz \cdot \Big(\frac{2nz}{p}\Big)\varepsilon_p^\ell \int\limits_{R_p^\times} \psi_p\Big(\frac{1}{q}\Big(x + \frac{x^n}{z}\Big)\Big)\,dx.$$

Reversing the above computation, we can see that the integrals on the right side of (9) and (10) vanish when the conductor exponent of the ramified character χ is

not equal to a. This indeed results from the fact that for a ramified character χ the integral

$$\int_{p^{-a}R_p^{\times}} \chi^{-1}(x)\psi_p(x)\,dx$$

equals $\varepsilon(\chi,\psi_p;dx)$ when $a(\chi)=a$, and vanishes otherwise.

Now we turn to the right side of (8) and follow the computation in [13]:

$$\bar{\chi}(-n^n)q^{2-n}\varepsilon\Big(\chi\circ\mathrm{N}_{E_p/\mathbb{Q}_p},\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p};d\beta\Big)$$

$$=\bar{\chi}(-n^n)q^{2-n}\int_{\varpi_{E_p}^{-a}R_{E_p}^{\times}}\chi^{-1}\circ\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}(\beta)\,d\beta$$

because $a(\chi\circ\mathrm{N}_{E_p/\mathbb{Q}_p})=a(\chi)=a$ and the order of $\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}$ is still equal to zero in the unramified case. For any $\varepsilon\in R_{E_p}^{\times}$ with $\mathrm{N}_{E_p/\mathbb{Q}_p}(\varepsilon)=1$ we can replace the expression $\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}(\beta)$ by $\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}(\varepsilon\beta)$ in the above integral. Hence

$$\bar{\chi}(-n^n)q^{2-n}\varepsilon\Big(\chi\circ\mathrm{N}_{E_p/\mathbb{Q}_p},\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p};d\beta\Big)$$

$$=\bar{\chi}(-n^n)q^{2(2-n)}\frac{1-p^{-1}}{1-p^{1-n}}\int_{\varpi_{E_p}^{-a}R_{E_p}^{\times}}\chi^{-1}\circ\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)$$

$$\cdot\sum_{\substack{\varepsilon\in R_{E_p}^{\times}/(1+\varpi_{E_p}^{a}R_{E_p}),\\ \mathrm{N}_{E_p/\mathbb{Q}_p}(\varepsilon)=1}}\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}(\varepsilon\beta)\,d\beta$$

because the number of terms in the sum is $q^{n-2}(1-p^{1-n})/(1-p^{-1})$. Indeed,

$$\mathrm{N}_{E_p/\mathbb{Q}_p}:\quad R_{E_p}^{\times}/(1+\varpi_{E_p}^{a}R_{E_p})\longrightarrow R_p^{\times}/(1+qR_p)$$

is a surjective map because $\mathbb{Q}_p$ is unramified in E; since $R_{E_p}^{\times}/(1+\varpi_{E_p}^{a}R_{E_p})$ has $(1-p^{1-n})/q^{1-n}$ elements and $R_p^{\times}/(1+qR_p)$ has $(1-p^{-1})q$ elements, the kernel of the norm map $\mathrm{N}_{E_p/\mathbb{Q}_p}$ has $q^{n-2}(1-p^{1-n})/(1-p^{-1})$ elements.

Since the sum above depends only on $\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)$, we may define a function Ψ on $\mathbb{Q}_p$ such that

$$\Psi\Big(\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\Big)=\sum_{\substack{\varepsilon\in R_{E_p}^{\times}/(1+\varpi_{E_p}^{a}R_{E_p}),\\ \mathrm{N}_{E_p/\mathbb{Q}_p}(\varepsilon)=1}}\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}(\varepsilon\beta)$$

for any $\beta\in\varpi_{E_p}^{-a}R_{E_p}^{\times}$, and set $\Psi=0$ elsewhere. Note that $\Psi\Big(\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\Big)$ is constant on any coset $\alpha+R_{E_p}$ with $\alpha\in\varpi_{E_p}^{-a}R_{E_p}^{\times}$. Hence $\Psi(b)$ is constant on any

coset $b + q^{2-n}R_p$ with $b \in q^{1-n}R_p^\times$. Then we get

$$\bar{\chi}(-n^n)q^{2-n}\varepsilon\left(\chi \circ \mathrm{N}_{E_p/\mathbb{Q}_p}, \psi_p \circ \mathrm{tr}_{E_p/\mathbb{Q}_p}; d\beta\right)$$

$$= \bar{\chi}(-n^n)q^{2(2-n)}\frac{1-p^{-1}}{1-p^{1-n}}$$

$$\cdot \int_{\varpi_{E_p}^{-a}R_{E_p}^\times} \chi^{-1} \circ \mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\Psi\left(\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\right)d\beta$$

$$= \bar{\chi}(-n^n)q^{2(2-n)}\frac{1-p^{-1}}{1-p^{1-n}}$$

$$\cdot \sum_{\beta \in \varpi_{E_p}^{-a}(R_{E_p}^\times/(1+\varpi_{E_p}^a R_{E_p}))} \chi^{-1} \circ \mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\Psi\left(\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)\right).$$

Counting elements in the kernel of $\mathrm{N}_{E_p/\mathbb{Q}_p}$ again, we arrive at

$$\bar{\chi}(-n^n)q^{2-n}\varepsilon\left(\chi \circ \mathrm{N}_{E_p/\mathbb{Q}_p}, \psi_p \circ \mathrm{tr}_{E_p/\mathbb{Q}_p}; d\beta\right)$$

$$= \bar{\chi}(-n^n)q^{2-n} \sum_{b \in q^{1-n}(R_p^\times/(1+qR_p))} \chi^{-1}(b)\Psi(b)\,db$$

(11)

$$= \bar{\chi}(-n^n)q^{2(2-n)} \int_{q^{1-n}R_p^\times} \chi^{-1}(b)\Psi(b)\,db$$

$$= \bar{\chi}(-n^n)q^{3-n} \int_{R_p^\times} \chi^{-1}(bq^{1-n})\Psi(bq^{1-n})\,db.$$

If we reverse the above computation, we can see that for any ramified character χ the integral on the right side vanishes when the conductor exponent $a(\chi) \neq a$. Comparing (11) with the expressions of the left side of (8) in (9) and (10) we get for any ramified character χ that

$$q^{2-(n-1)/2}\chi(q^{n-1}) \int_{R_p^\times} \chi^{-1}(z)\,dz \int_{R_p^\times} \psi_p\left(\frac{1}{q}\left(x + \frac{x^n}{z}\right)\right)dx$$

(12)

$$= \bar{\chi}(-n^n q^{1-n})q^{3-n} \int_{R_p^\times} \chi^{-1}(b)\Psi(bq^{1-n})\,db$$

when a is even, and that

$$q^{2-(n-1)/2}\chi(q^{n-1}) \int_{R_p^\times} \chi^{-1}(z)\,dz \cdot \left(\frac{2nz}{p}\right)\varepsilon_p^\ell \int_{R_p^\times} \psi_p\left(\frac{1}{q}\left(x + \frac{x^n}{z}\right)\right)dx$$

(13)

$$= \bar{\chi}(-n^n q^{1-n})q^{3-n} \int_{R_p^\times} \chi^{-1}(b)\Psi(bq^{1-n})\,db$$

when a is odd. We point out that (12) and (13) are also true for unramified character χ because of our assumption of $a > 1$. (For $a = 1$, (12) and (13) do not

hold.) Therefore by changing variables from z to $b = -z/n^n$ and by the Fourier inversion formula we conclude that

$$\int\limits_{R_p^\times} \psi_p\left(\frac{1}{q}\left(x - \frac{x^n}{bn^n}\right)\right) dx = q^{(1-n)/2}\Psi(bq^{1-n})$$

when $a > 1$ is even, and that

$$\left(\frac{-2nb}{p}\right)\varepsilon_p^\ell \int\limits_{R_p^\times} \psi_p\left(\frac{1}{q}\left(x - \frac{x^n}{bn^n}\right)\right) dx = q^{(1-n)/2}\Psi(bq^{1-n})$$

when $a > 1$ is odd, for any $b \in R_p^\times$. Here we have used the fact that $\gamma(cb^2, \psi_p) = \gamma(c, \psi_p)$.

Since we have assumed that $\mathbb{Q}_p$ is unramified in E, we can always find $\beta \in R_{E_p}^\times$ such that $bq^{1-n} = \mathrm{N}_{E_p/\mathbb{Q}_p}(\beta/q)$, i.e., $b = \mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)$. Writing the integrals in terms of sums, we can finally prove the following local results.

Theorem 3. *Let p and ℓ be two odd primes with $p > \ell$ such that $\mathbb{Q}_p$ is unramified in a cyclic algebraic number field E of degree ℓ. Then for $n = \ell + 1$ and $q = p^a$ with $a > 1$ we have*

$$q^{(3-n)/2} \sum_{\substack{\beta \in R_{E_p}^\times/(1+\varpi_{E_p}^a R_{E_p}), \\ \mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)=b}} \psi_p \circ \mathrm{tr}_{E_p/\mathbb{Q}_p}\left(\frac{\beta}{q}\right)$$

(14)
$$= \sum_{x \in R_p^\times/(1+qR_p)} \psi_p\left(\frac{1}{q}\left(x - \frac{x^n}{bn^n}\right)\right) \qquad \text{if } a \text{ is even,}$$

$$= \left(\frac{2nb}{p}\right)\varepsilon_p^{-\ell} \sum_{x \in R_p^\times/(1+qR_p)} \psi_p\left(\frac{1}{q}\left(x - \frac{x^n}{bn^n}\right)\right) \qquad \text{if } a \text{ is odd,}$$

for any $b \in R_p^\times$.

Proof. If $\mathbb{Q}_p$ is inert in E, the above computation is the proof. Now we consider the case when p splits in E into $\ell = n - 1$ local fields $E_{p_1}, \dots, E_{p_\ell}$ each E_{p_i} isomorphic to $\mathbb{Q}_p$. In this case, any $\beta \in \mathbb{Q}_p \otimes_{\mathbb{Q}} E$ can be written as $\beta = (b_1, \dots, b_\ell)$ with $b_1, \dots, b_\ell \in \mathbb{Q}_p$. Furthermore, $\mathrm{tr}_{E_p/\mathbb{Q}_p}(\beta) = b_1 + \cdots + b_\ell$ and $\mathrm{N}_{E_p/\mathbb{Q}_p}(\beta) = b_1 \cdots b_\ell$. Therefore the left side of (14) now takes the form

$$q^{(3-n)/2} \sum_{\substack{b_1, \dots, b_\ell \in R_p^\times/(1+qR_p), \\ b_1 \cdots b_\ell = b}} \psi_p\left(\frac{b_1 + \cdots + b_\ell}{q}\right)$$

$$= q^{(3-n)/2} \sum_{b_1, \dots, b_{\ell-1} \in R_p^\times/(1+qR_p)} \psi_p\left(\frac{1}{q}\left(b_1 + \cdots + b_{\ell-1} + \frac{b}{b_1 \cdots b_{\ell-1}}\right)\right).$$

We note that this local exponential sum is the generalized Kloosterman sum studied by Katz [9]. Writing this sum in terms of integration, we get the following expression for the left side of (14):

$$q^{(n-1)/2} \int\limits_{(R_p^\times)^{\ell-1}} \psi_p\left(\frac{1}{q}\left(b_1 + \cdots + b_{\ell-1} + \frac{b}{b_1 \cdots b_{\ell-1}}\right)\right) db_1 \cdots db_{\ell-1}.$$

As before, we choose any ramified character χ and integrate the above expression against $\chi^{-1}(b)$ with respect to b. After changing variables we get

$$
\text{(15)} \quad q^{(1-n)/2}\chi^{-1}(q^{n-1}) \int\limits_{(\frac{1}{q}R_p^{\times})^{\ell}} \chi^{-1}(b)\psi_p(b)
$$

$$
\cdot \chi^{-1}(b_1)\psi_p(b_1) \cdots \chi^{-1}(b_{\ell-1})\psi_p(b_{\ell-1})\,db\,db_1\cdots db_{\ell-1},
$$

which equals

$$
q^{(1-n)/2}\chi^{-1}(q^{n-1})\Big(\varepsilon(\chi,\psi_p;dx)\Big)^{n-1}
$$

if the conductor exponent $a(\chi) = a$, and vanishes otherwise. When $a > 1$ we can also show that the integral in (15) vanishes for any unramified character χ. Comparing this with the results in (11) and recalling that

$$
\varepsilon\Big(\chi\circ\mathrm{N}_{E_p/\mathbb{Q}_p},\psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p};d\beta\Big) = \Big(\varepsilon(\chi,\psi_p;dx)\Big)^{n-1},
$$

we have shown that the integral

$$
\int\limits_{R_p^{\times}} \chi^{-1}(b)\left(q^{(3-n)/2}\sum_{\substack{\beta\in R_{E_p}^{\times}/(1+\varpi_{E_p}^{a}R_{E_p}),\\ \mathrm{N}_{E_p/\mathbb{Q}_p}(\beta)=b}} \psi_p\circ\mathrm{tr}_{E_p/\mathbb{Q}_p}\Big(\frac{\beta}{q}\Big)\right)db
$$

has the same values for both the inert and splitting cases. Therefore (14) is also true in the splitting case.   Q.E.D.

Now we can finally turn to the global situation. Consider the products of the sums in (14) over all prime factors of m and the product of the products of the Weil constants over those prime factors of m that divide m to odd powers. Recall that for any $x \in \mathbb{Q}$ we have $\prod_{p<\infty}\psi_p(x) = e^{-2\pi ix}$, because the global character $\psi = \psi_{\mathbb{R}}\prod_{p<\infty}\psi_p$ is trivial on $\mathbb{Q}$. Therefore we can express the products of the sums above as sums of exponential functions. By taking complex conjugates we arrive at the formula in Theorem 1.

References

1. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer: Berlin-Heidelberg-New York 1993. MR **94i:**11105
2. H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. Reine Angew. Math.* **172** (1935), 151-182.
3. W. Duke and H. Iwaniec, A relation between cubic exponential and Kloosterman sums, *Contemporary Math.* **143** (1993), 255-258. MR **93m:**11082
4. J. Greene and D. Stanton, The triplication formula for Gauss sums, *Aequationes Math.* **30** (1986), 134-141. MR **87g:**11162
5. P. Gérardin and J.P. Labesse, The solution of a base change problem for $GL(2)$ (following Langlands, Saito, Shintani), *Proc. Symp. Pure Math.* **33** (1979), part 2, 115-133. MR **82e:**10047
6. H. Jacquet, The continuous spectrum of the relative trace formula for $GL(3)$ over a quadratic extension, *Israel J. Math.* **89** (1995), 1-59. MR **96a:**22029
7. H. Jacquet and R.P. Langlands, *Automorphic Forms on $GL(2)$*, Lecture Notes in Math. Vol. 114, Springer: Berlin-Heidelberg-New York, 1970. MR **53:**5481
8. H. Jacquet and Y. Ye, Une remarque sur le changement de base quadratique, *C. R. Acad. Sci. Paris Ser. I Math.* **311** (1990), 671-676. MR **92j:**11046
9. N.M. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Ann. Math. Studies, No. 116, Princeton Univ. Press: Princeton 1988. MR **91a:**11028

10. D.S. Kubert and S. Lichtenbaum, Jacobi-sum Hecke characters and Gauss-sum identities, *Comp. Math.* **48** (1983), 55-87. MR **85c:**11108

11. Z. Mao and S. Rallis, A trace formula for dual pairs, *Duke Math. J.* **87** (1997), 321–341. CMP 97:11

12. J. Tate, Number theoretic background, *Proc. Symp. Pure Math.* **33** (1979), part 2, 3-26. MR **80m:**12009

13. Y. Ye, Kloosterman integrals and base change for $GL(2)$, *J. Reine Angew. Math.* **400** (1989), 57–121. MR **90i:**11134

14. Y. Ye, The lifting of Kloosterman sums, *J. Number Theory*, **51** (1995), 275-287. MR **97a:**11126

15. D. Zagier, Modular forms associated to real quadratic fields, *Invent. Math.* **30** (1975), 1-46. MR **52:**3062

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF IOWA, IOWA CITY, IOWA 52242-1419

E-mail address: yey@math.uiowa.edu