ACTA ARITHMETICA
LXXXVI.3 (1998)

Hyper-Kloosterman sums and estimation of exponential sums of polynomials of higher degrees

by

Yangbo Ye (Iowa City, Iowa)

1. Introduction. From a Davenport–Hasse identity of Gauss sums we will deduce identities of hyper-Kloosterman sums. Using these identities the theory of Kloosterman sheaves and equidistribution of hyper-Kloosterman sums can be applied to the exponential sum

$$\sum_{x \bmod q} \mathrm{e}\left(\frac{bx + cx^k}{q}\right)$$

for some large k, where $q = p^a$ with $a \geq 1$, and b and c are relatively prime to the prime p. Using bounds of hyper-Kloosterman sums by Deligne, Katz, Dąbrowski, and Fisher we then deduce new estimates of the above exponential sum. Our bounds cannot be obtained by traditional methods as our k may reach the order of q.

1.1. *Davenport–Hasse identities of Gauss sums.* Davenport and Hasse established an identity of Gauss sums in [3]. Let p be an odd prime and $m > 1$ a divisor of $p - 1$. Let η be a ramified character of order m on the multiplicative group $\mathbb{Q}_p^\times$ of the p-adic field $\mathbb{Q}_p$. Here by η being *ramified* we mean that it is nontrivial on $R_p^\times$; the *order* of η is by definition the smallest positive integer m such that $\eta^m = 1$. Then we know that the conductor exponent of η, denoted by $a(\eta)$, is equal to 1. Let ψ be an additive character of $\mathbb{Q}_p$ whose order is 0. Here the *order* of an additive character φ, denoted by $n(\varphi)$, is the largest integer n such that the character φ is trivial on $p^{-n}R_p$. Let χ be any ramified multiplicative character on $\mathbb{Q}_p$ satisfying

$$a(\chi) = a(\chi\eta) = \ldots = a(\chi\eta^{m-1}) = 1.$$

Then the Davenport–Hasse identity of Gauss sums over the finite field $\mathbb{F}_p$ can be written as

1991 *Mathematics Subject Classification*: Primary 11L05.
Supported in part by NSF Grant #DMS 97-01225.

$$\chi(m^m)\varepsilon(\chi^m,\psi;dx)\varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx) = \varepsilon(\chi,\psi;dx)\varepsilon(\chi\eta,\psi;dx)\dots\varepsilon(\chi\eta^{m-1},\psi;dx). \tag{1}$$

Here for a nontrivial additive character φ the *ε-factor* is defined as

$$\varepsilon(\chi,\varphi;dx) = \begin{cases} \displaystyle\int_{p^{-a(\chi)-n(\varphi)}R_p^\times} \chi^{-1}(x)\varphi(x)\,dx & \text{if } \chi \text{ is ramified,} \\ \chi(p^{n(\varphi)})p^{n(\varphi)} & \text{if } \chi \text{ is unramified,} \end{cases} \tag{2}$$

where dx is a Haar measure on $\mathbb{Q}_p$ normalized by volume$(R_p) = 1$.

We point out that in (1) the conductor exponent $a(\chi)$ of the character χ has to be 1. In order to have a Davenport–Hasse identity over the p-adic field $\mathbb{Q}_p$ we have to consider the case of $a(\chi) = a > 1$. In [12] a generalized Davenport–Hasse identity of Gauss sums is proved:

$$\chi^m(m)\varepsilon(\chi^m,\psi;dx)q^{m-1}\prod_{1<j\le m}\int_{p^{[a/2]}R_p}\chi\left(1+\frac{j-1}{2j}y_j^2\right)dy_j = (\varepsilon(\chi,\psi;dx))^m \tag{3}$$

when $1 < m < p$ and $q = p^a$ with $a > 1$. If a is even, then it simplifies to

$$\chi^m(m)q^{(m-1)/2}\varepsilon(\chi^m,\psi;dx) = (\varepsilon(\chi,\psi;dx))^m.$$

We will use the approach in [12] to prove in Section 2 the following generalization of the Davenport–Hasse identity.

THEOREM 1. *Let $m > 1$ be a divisor of $p-1$, η a ramified multiplicative character of order m, and ψ an additive character of order zero. Then for any ramified multiplicative character χ with conductor exponent $a(\chi) = a > 1$ we have*

$$\chi^m(m)\eta^{m(m-1)/2}(m)\varepsilon(\chi^m\eta^{m(m-1)/2},\psi;dx) \times q^{m-1}\prod_{1<j\le m}\int_{p^{[a/2]}R_p}\chi\left(1+\frac{j-1}{2j}y_j^2\right)dy_j = \varepsilon(\chi,\psi;dx)\varepsilon(\chi\eta,\psi;dx)\dots\varepsilon(\chi\eta^{m-1},\psi;dx) \tag{4}$$

where $q = p^a$.

1.2. *Identities of exponential sums.* We write $\mathrm{e}(x) = e^{2\pi ix}$. For a multiplicative character χ modulo an odd integer $c > 1$ we denote the Gauss sum by

$$\tau_c(\chi) = \sum_{\substack{x \bmod c \\ (x,c)=1}} \chi(x)\mathrm{e}\left(\frac{x}{c}\right).$$

From the original Davenport–Hasse identity in (1) we will deduce in Section 3 the following identity between a hyper-Kloosterman sum with character η and an exponential sum.

THEOREM 2. *Let p be a prime and $m > 1$ a divisor of $p-1$. Denote by η a multiplicative character modulo p of order m. Then for any integer z which is relatively prime to p we have*

$$\sum_{\substack{x_1,\dots,x_m \bmod p\\(x_1,p)=\dots=(x_m,p)=1}} \eta(x_2x_3^2\dots x_m^{m-1})\mathrm{e}\left(\frac{x_1+\dots+x_m+z\overline{x}_1\dots\overline{x}_m}{p}\right) = \tau_p(\eta)\dots\tau_p(\eta^{m-1})\sum_{\substack{x \bmod p\\(x,p)=1}}\mathrm{e}\left(\frac{mx+z\overline{x}^m}{p}\right) \tag{5}$$

where $x\overline{x} \equiv 1 \bmod p$.

We point out that this identity is indeed the Diophantine manifestation of a geometric isomorphism of sheaves in [8], Theorem 9.2.3. The generalized Davenport–Hasse identity in Theorem 1 will imply a similar identity of the hyper-Kloosterman sum. Its proof will be given in Section 4.

THEOREM 3. *Let p be a prime, $m > 1$ a divisor of $p-1$, and $q = p^a$ with $a > 1$. Denote by η a multiplicative character modulo q of order m which is also a multiplicative character modulo p. Then for any integer z which is relatively prime to p we have*

$$\sum_{\substack{x_1,\dots,x_m \bmod q\\(x_1,p)=\dots=(x_m,p)=1}} \eta(x_2x_3^2\dots x_m^{m-1})\mathrm{e}\left(\frac{x_1+\dots+x_m+z\overline{x}_1\dots\overline{x}_m}{q}\right) \tag{6}$$

$$= \begin{cases} q^{(m-1)/2}\displaystyle\sum_{\substack{x \bmod q\\(x,p)=1}} \eta^{m(m-1)/2}(x)\mathrm{e}\left(\frac{mx+z\overline{x}^m}{q}\right) & \text{if } a \text{ is even},\\ q^{(m-1)/2}\left(\dfrac{2^{m-1}z^{m-1}m}{p}\right)\varepsilon_p^{m-1}\displaystyle\sum_{\substack{x \bmod q\\(x,p)=1}} \eta^{m(m-1)/2}(x)\mathrm{e}\left(\frac{mx+z\overline{x}^m}{q}\right) & \text{if } a \text{ is odd}, \end{cases}$$

where $x\overline{x} \equiv 1 \pmod q$ and ε_p by definition equals 1 if $p \equiv 1 \pmod 4$ and equals i if $p \equiv 3 \pmod 4$.

Note that when m is odd, the character $\eta^{m(m-1)/2}$ is indeed trivial. When m is even, $\eta^{m(m-1)/2}$ is a quadratic character. From the identity of Gauss sums in (3) we can get a similar identity using the same proof.

THEOREM 4. *Let p be a prime, $1 < m < p$, and $q = p^a$ with $a > 1$. Then for any integer z which is relatively prime to p,*

$$\sum_{\substack{x_1,\dots,x_m \bmod q\\(x_1,p)=\dots=(x_m,p)=1}} \mathrm{e}\left(\frac{x_1+\dots+x_m+z\overline{x}_1\dots\overline{x}_m}{q}\right) \tag{7}$$

$$= \begin{cases} q^{(m-1)/2} \sum\limits_{\substack{x \bmod q \\ (x,p)=1}} \mathrm{e}\Big(\dfrac{mx + z\overline{x}^m}{q}\Big) & \text{if } a > 1 \text{ is even,} \\ q^{(m-1)/2} \Big(\dfrac{2^{m-1} z^{m-1} m}{p}\Big) \varepsilon_p^{m-1} \sum\limits_{\substack{x \bmod q \\ (x,p)=1}} \mathrm{e}\Big(\dfrac{mx + z\overline{x}^m}{q}\Big) & \text{if } a > 1 \text{ is odd.} \end{cases}$$

1.3. *Applications and estimation of exponential sums.* We note that the exponential sums on the left side of the identities in Theorems 2, 3, and 4 are all hyper-Kloosterman sums. Hyper-Kloosterman sums over a finite field, like the one in Theorem 2, are studied extensively by Deligne [4] and Katz [6] and [7]. In particular, these sums can be represented by Kloosterman sheaves and their values are equidistributed with respect to a Haar measure. Our identity in Theorem 2 implies that the same Kloosterman sheaves can be used to study exponential sums of the type

$$\sum_{\substack{x \bmod p \\ (x,p)=1}} \mathrm{e}\Big(\frac{mx + z\overline{x}^m}{p}\Big) \quad \text{or} \quad \sum_{x \bmod p} \mathrm{e}\Big(\frac{bx + cx^{p-m-1}}{p}\Big)$$

when $m \mid p-1$, where b, c, and z are relatively prime to p. Indeed, these exponential sums have the same equidistribution pattern as the hyper-Kloosterman sums.

In [4], [6] and [7] the estimate of hyper-Kloosterman sums with characters was given implicitly (Theorem 4.1.1(1) of [7]): For the sum on the left side of (5) we have

$$\Big| \sum_{\substack{x_1,\ldots,x_m \bmod p \\ (x_1,p)=\ldots=(x_m,p)=1}} \eta(x_2 x_3^2 \ldots x_m^{m-1}) \mathrm{e}\Big(\frac{x_1 + \ldots + x_m + z\overline{x}_1 \ldots \overline{x}_m}{p}\Big) \Big| \le (m+1)p^{m/2}.$$

We know that the Gauss sums in (5) have absolute value $p^{1/2}$. Therefore the identity in (5) implies an estimate of the exponential sum on the right side

$$\Big| \sum_{\substack{x \bmod p \\ (x,p)=1}} \mathrm{e}\Big(\frac{mx + zx^{p-m-1}}{p}\Big) \Big| \le (m+1)p^{1/2} \tag{8}$$

when $m \mid p-1$.

Now let us turn to Theorem 4. By [2] (Example 1.17), the hyper-Kloosterman sum on the left side of (7) has the bounds

$$\Big| \sum_{\substack{x_1,\ldots,x_m \bmod q \\ (x_1,p)=\ldots=(x_m,p)=1}} \mathrm{e}\Big(\frac{x_1 + \ldots + x_m + z\overline{x}_1 \ldots \overline{x}_m}{q}\Big) \Big| \tag{9}$$

$$\begin{aligned}
&\le (m+1)q^{m/2} && \text{when } 1 < m < p-1 \text{ and } a > 1;\\
&\le p^{1/2}q^{m/2} && \text{when } m = p-1 \text{ and } a \ge 5;\\
&\le pq^{m/2} && \text{when } m = p-1 \text{ and } a = 4;\\
&\le p^{1/2}q^{m/2} && \text{when } m = p-1 \text{ and } a = 3;\\
&\le q^{m/2} && \text{when } m = p-1 \text{ and } a = 2,
\end{aligned}$$

where $p > 2$ and $q = p^a$. The identity in (7) then implies bounds for the exponential sum on the right side

$$\sum_{\substack{x \bmod q\\(x,p)=1}} \mathrm{e}\Big(\frac{mx + z\overline{x}^m}{q}\Big) = \sum_{\substack{x \bmod q\\(x,p)=1}} \mathrm{e}\Big(\frac{mx + zx^{\phi(q)-m}}{q}\Big)$$

where $\phi(q) = p^{a-1}(p-1)$ is the Euler function. Together with the result in (8) on the case of $q = p$ we proved the following theorem. Note that

$$\sum_{\substack{x \bmod q\\p \mid x}} \mathrm{e}\Big(\frac{mx + zx^{\phi(q)-m}}{q}\Big) = 0$$

when $a > 1$ and $1 < m < p$.

THEOREM 5. *Let p be an odd prime, $q = p^a$, $a \ge 1$, and $1 < m < p$. Then for any b and c relatively prime to p we have*

$$\begin{aligned}
(10)\quad &\Big|\sum_{x \bmod q} \mathrm{e}\Big(\frac{bx + cx^{\phi(q)-m}}{q}\Big)\Big|\\
&\le (m+1)p^{1/2} + 1 && \textit{when } m > 1,\ m \mid p-1,\ \textit{and } a = 1;\\
&\le (m+1)q^{1/2} && \textit{when } 1 < m < p-1 \textit{ and } a > 1;\\
&\le p^{1/2}q^{1/2} && \textit{when } m = p-1 \textit{ and } a \ge 5;\\
&\le pq^{1/2} && \textit{when } m = p-1 \textit{ and } a = 4;\\
&\le p^{1/2}q^{1/2} && \textit{when } m = p-1 \textit{ and } a = 3;\\
&\le q^{1/2} && \textit{when } m = p-1 \textit{ and } a = 2.
\end{aligned}$$

We point out that our bounds cannot be obtained by traditional estimation methods of exponential sums of the type (cf. Vaughan [11])

$$\sum_{x \bmod q} \mathrm{e}\Big(\frac{ax + bx^k}{q}\Big).$$

Indeed, in the case of p Carlitz and Uchiyama [1] proved that

$$\Big|\sum_{x \bmod p} \mathrm{e}\Big(\frac{P(x)}{p}\Big)\Big| \le (k-1)p^{1/2} \tag{11}$$

based on the work of Weil on Riemann hypothesis for curves over finite fields. Here $P(x) = a_k x^k + \ldots + a_1 x \in \mathbb{Z}[x]$ is a polynomial of degree k with $(a_k, \ldots, a_1, p) = 1$. Loxton and Vaughan [10] proposed a question of estimating exponential sums with polynomials of higher degrees and conjectured that the bound in (11) should be reduced to $(kp)^{1/2}$. For the polynomial $bx + cx^{p-m-1}$ with b and c relatively prime to p and $m \mid p-1$ our estimate $(m+1)p^{1/2}$ is better and indeed nontrivial when m is fixed and $p \equiv 1 \pmod m$ is large.

In the case of $q = p^a$ with $a > 1$ Loxton and Smith [9] and Loxton and Vaughan [10] improved an estimate of Hua [5] on

$$\sum_{x \bmod q} \mathrm{e}\Big(\frac{P(x)}{q}\Big).$$

For $P(x) = bx + cx^k$ with b and c relatively prime to p they proved that

$$\Big|\sum_{x \bmod q} \mathrm{e}\Big(\frac{bx + cx^k}{q}\Big)\Big| \le q^{1/2} d_{k-1}(q) \tag{12}$$

where $d_{k-1}(q)$ is the number of representations of q as a product of $k-1$ positive integers (e.g. $d_{k-1}(p) = k-1$). Since $d_{k-1}(p^a)$ is a polynomial of k of degree a, Loxton and Smith's estimate in (12) becomes worst than trivial when k is not $O(p^{1/2})$. Our results in Theorem 5 can treat some of the cases of high degree polynomials, namely $bx + cx^k$ with degree k between $p^a - p^{a-1} - p$ and $p^a - p^{a-1} - 1$.

Exponential sums associated with high degree polynomials have high volatility. Their estimation might have applications in Waring's problem and other number theory problems.

Finally, let us go back to Theorem 3. As we remarked earlier the character $\eta^{m(m-1)/2}$ is trivial when m is odd. Consequently, the identities in (6) and (7) imply that

$$\sum_{\substack{x_1,\ldots,x_m \bmod q \\ (x_1,p)=\ldots=(x_m,p)=1}} \eta(x_2 x_3^2 \ldots x_m^{m-1}) \mathrm{e}\Big(\frac{x_1 + \ldots + x_m + z\overline{x}_1 \ldots \overline{x}_m}{q}\Big)$$
$$= \sum_{\substack{x_1,\ldots,x_m \bmod q \\ (x_1,p)=\ldots=(x_m,p)=1}} \mathrm{e}\Big(\frac{x_1 + \ldots + x_m + z\overline{x}_1 \ldots \overline{x}_m}{q}\Big)$$

when $m > 1$ is an odd divisor of $p-1$ for $q = p^a$ with $a > 1$. Therefore the

estimates of Dąbrowski and Fisher [2] in (9) in this case are also true for the sum twisted by the character η. This suggests that the same estimates might also be true for hyper-Kloosterman sums twisted by other multiplicative characters in the case of $q = p^a$ with $a > 1$.

2. The Davenport–Hasse identity over a p-adic field. In this section we prove Theorem 1. The proof of the identity in (3), which holds for any m greater than 1 and less than p, not necessarily dividing $p-1$, is similar and can be found in [12]. Let χ be a ramified multiplicative character of $\mathbb{Q}_p$ with conductor exponent $a(\chi) = a > 1$ and let η be a ramified multiplicative character of $\mathbb{Q}_p$ of order $m > 1$, where $m \mid p-1$. Then $a(\eta) = 1$ and

$$a(\chi) = a(\chi\eta) = \ldots = a(\chi\eta^{m-1}) = a.$$

For any additive character ψ of order zero we use the definition of local ε-factor in (2) and get

$$\begin{aligned}&\varepsilon(\chi,\psi;dx)\varepsilon(\chi\eta,\psi;dx)\ldots\varepsilon(\chi\eta^{m-1},\psi;dx)\\ &= \int\limits_{(q^{-1}R_p^\times)^m} \chi^{-1}(x_1\ldots x_m)\eta^{-1}(x_2x_3^2\ldots x_m^{m-1})\psi(x_1+\ldots+x_m)\,dx_1\ldots dx_m.\end{aligned}$$

Using new variables $y_1 = x_1 q$ and $y_i = x_i q/y_1$ for $i = 2,\ldots,m$, we get

$$\begin{aligned}&q^m\chi^m(q)\eta^{m(m-1)/2}(q)\int\limits_{(R_p^\times)^m}\chi^{-1}(y_1^m y_2\ldots y_m)\\ &\quad\times\eta^{-1}(y_1^{m(m-1)/2}y_2y_3^2\ldots y_m^{m-1})\psi\left(\frac{y_1}{q}(1+y_2+\ldots+y_m)\right)dy_1\ldots dy_m.\end{aligned}$$

Note that the character $\eta^{m(m-1)/2}$ is either unramified or ramified with conductor exponent equal to 1. Since $m < p$ and $a > 1$, the conductor exponents of χ^m and $\chi^m\eta^{m(m-1)/2}$ are still a. Consequently, the integral with respect to y_1 vanishes unless $1 + y_2 + \ldots + y_m \in R_p^\times$. Setting $z = y_1(1+y_2+\ldots+y_m)/q$ we get

$$\begin{aligned}(13)\qquad &\varepsilon(\chi,\psi;dx)\varepsilon(\chi\eta,\psi;dx)\ldots\varepsilon(\chi\eta^{m-1},\psi;dx)\\ &= q^{m-1}\int\limits_{q^{-1}R_p^\times}\chi^{-m}(z)\eta^{-m(m-1)/2}(z)\psi(z)\,dz\\ &\quad\times\int\limits_{\substack{y_2,\ldots,y_m\in R_p^\times\\ 1+y_2+\ldots+y_m\in R_p^\times}}\chi\left(\frac{(1+y_2+\ldots+y_m)^m}{y_2\ldots y_m}\right)\\ &\quad\times\eta\left(\frac{(1+y_2+\ldots+y_m)^{m(m-1)/2}}{y_2y_3^2\ldots y_m^{m-1}}\right)dy_2\ldots dy_m.\end{aligned}$$

The first integral on the right side equals $\varepsilon(\chi^m\eta^{m(m-1)/2},\psi;dx)$. Denote the second integral by I_m. Since $a(\chi)=a>1$, we set $y_m=y_0(1+u)$ where

$$y_0\in(R_p^\times-(-(1+y_2+\ldots+y_{m-1})+pR_p))/(1+p^{[(a+1)/2]}R_p)$$

and $u\in p^{[(a+1)/2]}R_p$. Rewrite the integrand of I_m accordingly and integrate it with respect to u; then we discover that the integral with respect to u vanishes unless $y_0\in(1+y_2+\ldots+y_{m-1})/(m-1)+p^{[a/2]}R_p$. Therefore the integral with respect to y_m in I_m is actually taken over $y_m\in(1+y_2+\ldots+y_{m-1})/(m-1)+p^{[a/2]}R_p$ with $1+y_2+\ldots+y_{m-1}\in R_p^\times$. Consequently, by setting $y_m=(1+y_2+\ldots+y_{m-1})/(m-1)+y$ with $y\in p^{[a/2]}R_p$ we can rewrite the integrand of I_m as

$$\chi\biggl(\frac{m^m}{(m-1)^{m-1}}\biggr)\eta\biggl(\frac{m^{m(m-1)/2}}{(m-1)^{(m-1)(m-2)/2}}\biggr)\chi\biggl(\frac{(1+y_2+\ldots+y_{m-1})^{m-1}}{y_2\ldots y_{m-1}}\biggr)$$
$$\times\eta\biggl(\frac{(1+y_2+\ldots+y_{m-1})^{(m-1)(m-2)/2}}{y_2y_3^2\ldots y_{m-1}^{m-2}}\biggr)\chi\biggl(1+\frac{(m-1)^3y^2/(2m)}{(1+y_2+\ldots+y_{m-1})^2}\biggr).$$

Changing variables we get

$$I_m=I_{m-1}\chi\biggl(\frac{m^m}{(m-1)^{m-1}}\biggr)\eta\biggl(\frac{m^{m(m-1)/2}}{(m-1)^{(m-1)(m-2)/2}}\biggr)\times\int\limits_{p^{[a/2]}R_p}\chi\biggl(1+\frac{(m-1)y^2}{2m}\biggr)\,dy. \tag{14}$$

Recall here that $m<p$. By using (14) repeatedly we finally get

$$I_m=\chi^m(m)\eta^{m(m-1)/2}(m)\prod_{1<j\le m}\int\limits_{p^{[a/2]}R_p}\chi\biggl(1+\frac{j-1}{2j}y_j^2\biggr)\,dy_j. \tag{15}$$

Theorem 1 follows from (13) and (15). ∎

3. Identities of exponential sums over a finite field. We will now deduce Theorem 2 from the Davenport–Hasse identity in (1). Let p be an odd prime, and $m>1$ a divisor of $p-1$. Using a ramified multiplicative character η on $\mathbb{Q}_p^\times$ of order m and an additive character ψ of order zero of $\mathbb{Q}_p$ we actually want to prove the following identity for any $z\in R_p^\times$:

$$\eta^{m(m-1)/2}(p)\sum_{x_1,\ldots,x_m\in R_p^\times/(1+pR_p)}\eta^{-1}(x_2x_3^2\ldots x_m^{m-1})\times\psi\biggl(\frac{1}{p}\biggl(x_1+\ldots+x_m+\frac{z}{x_1\ldots x_m}\biggr)\biggr)$$
$$=\varepsilon(\eta,\psi;dx)\ldots\varepsilon(\eta^{m-1},\psi;dx)\sum_{x\in R_p^\times/(1+pR_p)}\psi\biggl(\frac{1}{p}\biggl(mx+\frac{z}{x^m}\biggr)\biggr). \tag{16}$$

We will show that the Mellin transformations of the two sides of (16) are equal for any multiplicative character χ of $\mathbb{Q}_p$. Indeed, the Mellin transformation of the left side is equal to

$$p^m\eta^{m(m-1)/2}(p)\int\limits_{R_p^\times}\chi^{-1}(z)\,dz\int\limits_{(R_p^\times)^m}\eta^{-1}(x_2x_3^2\dots x_m^{m-1})\\ \times\psi\biggl(\frac{1}{p}\biggl(x_1+\ldots+x_m+\frac{z}{x_1\dots x_m}\biggr)\biggr)\,dx_1\dots\,dx_m$$

where we wrote the sum with respect to $x_1,\dots,x_m$ in terms of an integral. Changing variables from z to $y=z/(px_1\dots x_m)$ and from x_i to $y_i=x_i/p$, $i=1,\dots,m$, we get

$$p^{-1}\chi^{-(m+1)}(p)\int\limits_{p^{-1}R_p^\times}\chi^{-1}(y)\psi(y)\,dy\int\limits_{p^{-1}R_p^\times}\chi^{-1}(y_1)\psi(y_1)\,dy_1\\ \times\int\limits_{p^{-1}R_p^\times}\chi^{-1}\eta^{-1}(y_2)\psi(y_2)\,dy_2\dots\int\limits_{p^{-1}R_p^\times}\chi^{-1}\eta^{1-m}(y_m)\psi(y_m)\,dy_m.$$

Now we consider characters χ with $a(\chi)=1$ and $\chi^m\ne1$. Then we can express the above integral as a product of local ε-factors and get the following expression for the Mellin transformation of the left side of (16):

$$p^{-1}\chi^{-(m+1)}(p)\varepsilon(\chi,\psi;dx)^2\varepsilon(\chi\eta,\psi;dx)\dots\varepsilon(\chi\eta^{m-1},\psi;dx). \tag{17}$$

On the other hand, the Mellin transformation of the right side of (16) equals

$$p\varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx)\int\limits_{R_p^\times}\chi^{-1}(z)\,dz\int\limits_{R_p^\times}\psi\biggl(\frac{1}{p}\biggl(mx+\frac{z}{x^m}\biggr)\biggr)\,dx.$$

If we change variables to $y_1=z/(px^m)$ and $y_2=mx/p$, we get

$$p^{-1}\chi^{-(m+1)}(p)\chi^m(m)\varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx)\\ \times\int\limits_{p^{-1}R_p^\times}\chi^{-1}(y_1)\psi(y_1)\,dy_1\int\limits_{p^{-1}R_p^\times}\chi^{-m}(y_2)\psi(y_2)\,dy_2.$$

When the character χ satisfies $a(\chi)=1$ and $\chi^m\ne1$, we get the following expression for the Mellin transformation of the right side of (16):

$$p^{-1}\chi^{-(m+1)}(p)\chi^m(m)\varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx)\\ \times\varepsilon(\chi^m,\psi;dx)\varepsilon(\chi,\psi;dx). \tag{18}$$

By the Davenport–Hasse identity in (1) the expressions in (17) and (18) are equal. Consequently, we have

$$\eta^{m(m-1)/2}(p)\int\limits_{R_p^\times}\chi^{-1}(z)\,dz\sum_{x_1,\dots,x_m\in R_p^\times/(1+pR_p)}\eta^{-1}(x_2x_3^2\dots x_m^{m-1})\\ \times\psi\biggl(\frac{1}{p}\biggl(x_1+\ldots+x_m+\frac{z}{x_1\dots x_m}\biggr)\biggr) \tag{19}$$

$$= \varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx) \times \int\limits_{R_p^\times} \chi^{-1}(z)\,dz \sum_{x\in R_p^\times/(1+pR_p)} \psi\left(\frac{1}{p}\left(mx+\frac{z}{x^m}\right)\right)$$

when $a(\chi)=1$ and $\chi^m\neq 1$. By direct computation we can show that (19) holds for other χ. Indeed, the integrals with respect to z vanish for ramified χ with $a(\chi)\neq 1$. If $a(\chi)=1$ and $\chi^m=1$, then the two sides in (19) are both equal to

$$-p^{-1}\chi^{-1}(p)\varepsilon(\chi,\psi;dx)\varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx).$$

If χ is unramified, then the two sides of (19) become

$$p^{-1}\varepsilon(\eta,\psi;dx)\dots\varepsilon(\eta^{m-1},\psi;dx).$$

Since the equation in (19) now holds for any character χ, the identity in (16) and Theorem 2 follow from Fourier's inversion formula. ∎

4. Identities of exponential sums over a p-adic field. In this section we prove Theorem 3. If we set η to be the trivial character and take $m>1$ to be any integer less than p, not necessarily a divisor of $p-1$, our proof can be used verbatim to deduce Theorem 4 from the identity of local ε-factors in (3).

As in Section 3 let p be an odd prime, and $m>1$ a divisor of $p-1$. Denote by η a ramified multiplicative character on $\mathbb{Q}_p^\times$ of order m and by ψ an additive character of order zero of $\mathbb{Q}_p$. Let $a>1$ and set $q=p^a$. For any $z\in R_p^\times$ we want to prove that

$$\sum_{x_1,\dots,x_m\in R_p^\times/(1+qR_p)} \eta^{-1}(x_2x_3^2\dots x_m^{m-1}) \times \psi\left(\frac{1}{q}\left(x_1+\dots+x_m+\frac{z}{x_1\dots x_m}\right)\right) \tag{20}$$

$$= \begin{cases} q^{(m-1)/2} \displaystyle\sum_{x\in R_p^\times/(1+qR_p)} \eta^{-m(m-1)/2}(x)\psi\left(\frac{1}{q}\left(mx+\frac{z}{x^m}\right)\right) & \text{if } a \text{ is even,} \\ q^{(m-1)/2}\left(\dfrac{2^{m-1}z^{m-1}m}{p}\right)\varepsilon_p^{m-1} \times \displaystyle\sum_{x\in R_p^\times/(1+qR_p)} \eta^{-m(m-1)/2}(x)\psi\left(\frac{1}{q}\left(mx+\frac{z}{x^m}\right)\right) & \text{if } a \text{ is odd.} \end{cases}$$

Similarly to the computation in Section 3, for any multiplicative character χ with conductor exponent $a(\chi)=a$ the Mellin transform of the left side of (20) equals

$$q^{-1}\chi^{-(m+1)}(q)\eta^{-m(m-1)/2}(q)\varepsilon(\chi,\psi;dx)^2\varepsilon(\chi\eta,\psi;dx)\dots\varepsilon(\chi\eta^{m-1},\psi;dx).$$

By Theorem 1 the above becomes

$$\chi^m(m)\eta^{m(m-1)/2}(m)\chi^{-(m+1)}(q)\eta^{-m(m-1)/2}(q)\varepsilon(\chi,\psi;dx)$$
$$\times\varepsilon(\chi^m\eta^{m(m-1)/2},\psi;dx)q^{m-2}\prod_{1<j\le m}\int\limits_{p^{[a/2]}R_p}\chi\biggl(1+\frac{j-1}{2j}y_j^2\biggr)\,dy_j.$$

Since $m<p$, the conductor exponent of $\chi^m\eta^{m(m-1)/2}$ is still equal to a. By the definition of ε-factor in (2) we get

$$\chi^m(m)\eta^{m(m-1)/2}(m)\chi^{-(m+1)}(q)\eta^{-m(m-1)/2}(q)$$
$$\times\int\limits_{(q^{-1}R_p^\times)^2}\chi^{-1}(x_1)\chi^{-m}\eta^{-m(m-1)/2}(x_2)\psi(x_1+x_2)\,dx_1\,dx_2$$
$$\times q^{m-2}\prod_{1<j\le m}\int\limits_{p^{[a/2]}R_p}\chi\biggl(1+\frac{j-1}{2j}y_j^2\biggr)\,dy_j.$$

Changing variables from x_1 and x_2 to $y=x_2q/m$ and

$$z=\frac{x_1y^mq}{\prod_{1<j\le m}\bigl(1+\frac{j-1}{2j}y_j^2\bigr)}$$

we get

$$(21)\qquad q^m\int\limits_{R_p^\times}\chi^{-1}(z)\,dz\int\limits_{R_p^\times}\eta^{-m(m-1)/2}(y)\,dy$$
$$\times\int\limits_{(p^{[a/2]}R_p)^{m-1}}\psi\biggl(\frac{1}{q}\biggl(my+\frac{z}{y^m}\prod_{1<j\le m}\biggl(1+\frac{j-1}{2j}y_j^2\biggr)\biggr)\biggr)\,dy_2\,\dots\,dy_m$$
$$=q^m\int\limits_{R_p^\times}\chi^{-1}(z)\,dz\int\limits_{R_p^\times}\eta^{-m(m-1)/2}(y)\psi\biggl(\frac{1}{q}\biggl(my+\frac{z}{y^m}\biggr)\biggr)\,dy$$
$$\times\prod_{1<j\le m}\int\limits_{p^{[a/2]}R_p}\psi\biggl(\frac{(j-1)z}{2jqy^m}y_j^2\biggr)\,dy_j.$$

When a is even, the last integral with respect to y_j equals $q^{-1/2}$ and the product on the right side equals $q^{(1-m)/2}$. When a is odd, the integral equals

$$q^{-1/2}\gamma\biggl(\frac{(j-1)z}{jpy^m},\psi\biggr)=q^{-1/2}\gamma\biggl(\frac{j(j-1)y^mz}{p},\psi\biggr)$$

where γ is the Weil constant defined by

$$\int_{R_p} \psi\left(\frac{bx^2}{2}\right) dx = |b|_p^{-1/2}\gamma(b,\psi)$$

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

$$\gamma\left(\frac{j(j-1)y^m z}{p},\psi\right) = \left(\frac{2j(j-1)y^m z}{p}\right)\varepsilon_p$$

where ε_p equals 1 if $p \equiv 1 \pmod 4$ and equals i if $p \equiv 3 \pmod 4$. Consequently, the product on the right side of (21) becomes

$$q^{(1-m)/2} \prod_{1<j\le m} \left(\frac{2j(j-1)y^m z}{p}\right)\varepsilon_p = q^{(1-m)/2}\varepsilon_p^{m-1}\left(\frac{2^{m-1}z^{m-1}m}{p}\right).$$

Back to (21), we have proved that

$$\begin{aligned}(22)\qquad &\int_{R_p^\times} \chi^{-1}(z)\,dz \sum_{x_1,\dots,x_m \in R_p^\times/(1+qR_p)} \eta^{-1}(x_2x_3^2\dots x_m^{m-1}) \\ &\qquad\qquad \times \psi\left(\frac{1}{q}\left(x_1+\dots+x_m+\frac{z}{x_1\dots x_m}\right)\right) \\ &= \begin{cases} q^{(m-1)/2}\displaystyle\int_{R_p^\times} \chi^{-1}(z)\,dz \sum_{y\in R_p^\times/(1+qR_p)} \eta^{-m(m-1)/2}(y)\psi\left(\frac{1}{q}\left(my+\frac{z}{y^m}\right)\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } a \text{ is even}, \\ q^{(m-1)/2}\varepsilon_p^{m-1}\displaystyle\int_{R_p^\times} \chi^{-1}(z)\left(\frac{2^{m-1}z^{m-1}m}{p}\right) dz \\ \quad \times \displaystyle\sum_{y\in R_p^\times/(1+qR_p)} \eta^{-m(m-1)/2}(y)\psi\left(\frac{1}{q}\left(my+\frac{z}{y^m}\right)\right) \quad \text{if } a \text{ is odd}, \end{cases}\end{aligned}$$

for any multiplicative character χ with $a(\chi) = a$ and for any $z \in R_p^\times$, when $a > 1$.

Note that when m is even the above Jacobi symbol is a multiplicative character of z with conductor exponent equal to 1, because p is odd. Consequently, when χ is unramified or when χ is ramified with $a(\chi) \neq a$, the product of this Jacobi symbol and χ^{-1} is either unramified or is ramified with conductor exponent not equal to a, because $a > 1$. From this observation and the fact that $a > 1$ we can see that both sides of (22) vanish when χ is unramified or when χ is ramified with $a(\chi) \neq a$. Therefore (22) holds for any multiplicative character χ. By the Fourier inversion formula we prove (20) and Theorem 3. ∎

Acknowledgements. The author would like to thank Jia Chaohua and Luo Wenzhi for helpful discussions.

References

[1] L. C a r l i t z and S. U c h i y a m a, *Bounds for exponential sums*, Duke Math. J. 24 (1957), 37–41.

[2] R. D ą b r o w s k i and B. F i s h e r, *A stationary phase formula for exponential sums over* $\mathbb{Z}/p^m\mathbb{Z}$ *and applications to* GL(3)*-Kloosterman sums*, Acta Arith. 80 (1997), 1–48.

[3] H. D a v e n p o r t und H. H a s s e, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1935), 151–182.

[4] P. D e l i g n e, *Applications de la formule des traces aux sommes trigonométriques*, in: Cohomologie Etale (SGA 4 1/2), Lecture Notes in Math. 569, Springer, Berlin, 1977, 168–232.

[5] L. K. H u a, *On exponential sums*, J. Chinese Math. Soc. 2 (1940), 301–312.

[6] N. M. K a t z, *Sommes exponentielles*, Astérisque 79 (1980).

[7] —, *Gauss Sums*, *Kloosterman Sums*, *and Monodromy Groups*, Ann. of Math. Stud. 116, Princeton Univ. Press, Princeton, 1988.

[8] —, *Exponential Sums and Differential Equations*, Ann. of Math. Stud. 124, Princeton Univ. Press, Princeton, 1990.

[9] J. H. L o x t o n and R. A. S m i t h, *On Hua's estimate for exponential sums*, J. London Math. Soc. 26 (1982), 15–20.

[10] J. H. L o x t o n and R. C. V a u g h a n, *The estimation of complete exponential sums*, Canad. Math. Bull. 28 (1985), 440–454.

[11] R. C. V a u g h a n, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Tracts in Math. 125, Cambridge Univ. Press, Cambridge, 1997.

[12] Y. Y e, *The lifting of an exponential sum to a cyclic algebraic number field of a prime degree*, Trans. Amer. Math. Soc., to appear.

Department of Mathematics
The University of Iowa
Iowa City, Iowa 52242-1419
U.S.A.
E-mail: yey@math.uiowa.edu

Received on 14.2.1998 (3336)