ON GENERAL KLOOSTERMAN SUMS

S. Kanemitsu (Iizuka, Japan)
Y. Tanigawa (Nagoya, Japan)
Yi Yuang and Zhang Wenpeng (Xi’an, China)

Dedicated to Professor Dr. Karl-Heinz Indlekofer
on his sixtieth birthday

Abstract. The general Kloosterman sum

\[ K(m, n; k; q) = \sum_{a \mod (q) \atop (a, q) = 1} e\left(\frac{ma^k + n\bar{a}^k}{q}\right) \]

was studied by the second and third authors in their research of a problem of D.H. Lehmer. In this paper, we shall improve the estimate of \( K(m, n; k; q) \) with respect to \( q \). We also consider the sum twisted by a Dirichlet character.

1. Introduction

In their research on a problem of D.H. Lehmer, Yi and Zhang [6] introduced the general Kloosterman sum defined for positive integers \( m, n \) and \( q \) by

\[ K(m, n; k; q) = \sum_{a=1}^{q^*} e\left(\frac{ma^k + n\bar{a}^k}{q}\right), \]

where \( k \) is a fixed positive integer, \( e(y) = \exp(2\pi iy) \), \( \sum^* \) means the summation over all \( 1 \leq a \leq q \) such that the greatest common divisor of \( a \) and \( q \) denoted by \( (a, q) \) is 1 and \( \bar{a} \) is the reciprocal to \( a \) modulo \( q \).
When \( k = 1 \), \( K(m, n; 1; q) \) is the classical Kloosterman sum usually denoted by \( S(m, n; q) \) (cf. [3]):

\[
S(m, n; q) = \sum_{a=1}^{q} e\left(\frac{ma + n\overline{a}}{q}\right).
\]

The estimate of these sums plays important role in the theory of numbers, e.g. it is applied to the study of upper bounds of coefficients of modular forms [3]. The well-known estimate of \( K(m, n; 1; q) \) is

\[
K(m, n; 1; q) \leq (m, n, q)^{1/2}q^{1/2}d(q), \quad q > 2.
\]

We note that the above estimate for \( q = p^\alpha \) with a prime \( p \) and \( \alpha \geq 2 \) is proved by elementary means [3]. But for the prime modulus case the estimate is very difficult and was proved by Weil [5] through a deep consideration of algebraic geometry.

For a general Kloostermann sum Yi and Zhang [6] proved that

\[
K(m, n; k; p^\alpha) \ll (m, n, p^\alpha)^{1/2}p^{\alpha/4}\sqrt{d(p^\alpha)},
\]

where \( f(x) \ll g(x) \) means the same as \( f(x) = O(g(x)) \).

In this paper we shall improve the above estimate (3). In the sequel, we assume that

\[
q \text{ is a positive odd integer, } (k, q) = 1 \text{ and } 1 \leq m, n \leq q - 1.
\]

**Theorem 1.** Let \( p \) be an odd prime and let \( k \) be a positive integer such that \( (k, p) = 1 \). Then we have

\[
|K(m, n, k; p^\alpha)| \leq 2k(m, n, p^\alpha)^{1/2}p^{\alpha/2},
\]

where \( \alpha \) is a positive integer.

For general modulus \( q \), we have

**Theorem 2.** Let \( q \) be a positive odd integer and \( k \) be a positive integer with \( (k, q) = 1 \). Then we have

\[
|K(m, n, k; q)| \leq d(q)\log 2k/\log 2(m, n, q)^{1/2}q^{1/2}.
\]
We shall also consider a Kloosterman sum twisted by a Dirichlet character \( \chi \mod q \):

\[
K_{\chi}(m, n, k; q) = \sum_{a=1}^{q} \chi(a)e\left(\frac{ma^k + n\bar{a}^k}{q}\right).
\]

The estimate \( |K_{\chi}(m, n, k; q)| \ll \sqrt{q} \) does not hold in general. In fact, Professor Z.Y. Zheng established that \( |K_{\chi}(m, n, 1; p^\alpha)| \gg p^{\frac{2}{3} \alpha} \) for some character \( \chi \mod p^\alpha \), where \( p \) is a prime and \( \alpha \geq 3 \) (see [9]). However in the case of prime modulus we can show the following theorem.

**Theorem 3.** Let \( p \) be an odd prime and let \( \chi \) be a Dirichlet character \( \mod p \). Then

\[
K_{\chi}(m, n, k; p) \ll \sqrt{p},
\]

where the implied constant depends only on \( k \).

2. Proofs of Theorems 1 and 2

We assume that \( k \geq 2 \) is a positive integer. First we shall treat the prime modulus case of Theorem 1.

A remarkable feature in this case is that by group-theoretic considerations, we may reduce the proof to the Weil estimate of the Kloosterman sums and to the Chowla-Salié estimate of the twisted Kloosterman sums.

The underlying group-theoretic structure is described as follows.

Let \( G \) be a finite abelian group, let \( N \) be its subgroup and let \( G/N \) be the quotient group. Also let \((G/N)^*\) denote the character group of \( G/N \).

We extend a character \( \varphi \in (G/N)^* \) to a homomorphism on \( G \) by defining

\[
\varphi(a) = \varphi(aN).
\]

For any complex-valued function \( f \) on \( G \) consider the sum

\[
S := \sum_{\varphi \in (G/N)^*} \sum_{a \in G} \varphi(a)f(a).
\]
Inverting the order of summation and recalling the orthogonality of characters, we find that
\[ S = (G : N) \sum_{\alpha \in N} f(\alpha), \]
where \((G : N) = \sharp G/N\) signifies the group index.

Now specialize \(N\) to be \(G^k\), the subgroup of all \(k\)-th powers of elements of \(G\). Also let \(G_k\) denote the subgroup of \(k\)-th roots of the identity element of \(G\). As is apparent from the homomorphism theorem, we have \(G/G_k \cong G^k\), whence
\[ \sharp G_k = \sharp G/\sharp G^k = (G : G^k). \]

Now consider the sum
\[ S' = \sum_{a \in G} f(a^k) = \sum_{\alpha \in G^k} f(\alpha) \sum_{b^k = \alpha} 1. \]
Since \(b^k = \alpha = a^k\) implies that \(b \in a G_k\), it follows that the number of \(b\)'s such that \(b^k = \alpha\) is \(\sharp G_k\), which is, as shown above, \((G : G^k)\). Hence
\[ S' = (G : G^k) \sum_{\alpha \in G^k} f(\alpha) = S. \]
Hence
\[ \sum_{a \in G} f(a^k) = \sum_{\varphi \in (G/G^k)^*} \sum_{a \in G} \varphi(a) f(a). \]

We apply (9) with \(G = (\mathbb{Z}/p\mathbb{Z})^\times\) and \(f(a) = e\left(\frac{ma + na}{p}\right)\) to obtain
\[
K(m, n, k; p) = \sum_{\varphi \in (G/G^k)^*} \sum_{a \in G} \varphi(a) e\left(\frac{ma + na}{p}\right) = \sum_{\varphi \in (G/G^k)^*} K_{\varphi}(m, n, 1; p).
\]

In order to estimate \(K(m, n, k; p)\) we apply the Weil estimate to \(K_{\varphi_0}\), with \(\varphi_0\) a trivial character and the Chowla-Salié estimate
\[ |K_{\varphi}(m, n, 1; p)| \leq 2\sqrt{p} \]
to \(K_{\varphi}\) with non-trivial \(\varphi\).
Thus we have

\[ |K(m, n, k; p)| \leq (G : G^k)2\sqrt{p} \leq 2k\sqrt{p}, \]

where we need the fact that \((G : G^k) = (k, p - 1) \leq k\). This proves Theorem 1 in the prime modulus case.

Following the method of Estermann [2], we consider the case of a prime power modulus \(p^\alpha\), \(\alpha \geq 2\). We note that if \((m, n, p^\alpha) = p^\xi\), where \(0 \leq \xi \leq \alpha - 1\) by the assumption (4), then

\[(10) \quad K(m, n, k; p^\alpha) = p^\xi K\left(\frac{m}{p^\xi}, \frac{n}{p^\xi}; k; p^{\alpha-\xi}\right), \]

and so it is enough to consider the case \((m, n, p) = 1\).

Let \(\beta = \left\lceil \frac{\alpha}{2} \right\rceil\) and \(\gamma = \alpha - \beta\), hence \(\alpha = \beta + \gamma \leq 2\gamma\). The element \(a\) of the reduced residue class mod \(p^\alpha\) can be written as

\[ a = u + vp^\gamma, \]

where \(1 \leq u \leq p^\gamma - 1\), \((u, p) = 1\) and \(0 \leq v \leq p^\beta - 1\). We choose \(\bar{u}\) so that

\[ 1 \leq \bar{u} \leq p^\alpha - 1 \quad \text{and} \quad u\bar{u} \equiv 1 \pmod{p^\alpha}. \]

Then we can easily see that

\[ \bar{a} \equiv \bar{u} - \bar{u}^2vp^\gamma \pmod{p^\alpha}, \]

from which we have

\[(11) \quad ma^k + n\bar{a}^k \equiv m(u + vp^{\gamma})^k + n(\bar{u} - \bar{u}^2vp^{\gamma})^k \pmod{p^\alpha} \equiv (mu^k + n\bar{u}^k) + kvp^{\gamma}(m - \bar{u}^2k)n^{k-1} \pmod{p^\alpha}. \]

From (11) we have

\[(12) \quad K(m, n, k; p^\alpha) = \sum_{\substack{\bar{u} \equiv 1 \\ (u, p) = 1}}^{p^{\gamma-1}} e\left(\frac{mu^k + n\bar{u}^k}{p^\alpha}\right) \sum_{v=0}^{p^{\beta-1}} e\left(\frac{kv(m - \bar{u}^2k)n^{k-1}}{p^\beta}\right). \]

The sum over \(v\) vanishes unless

\[ m \equiv \bar{u}^{2k}n \pmod{p^\beta}, \]
so that we have only to consider the case \((mn, p) = 1\). In this case the general Kloosterman sum is expressed as

\[
K(m, n, k; p^\alpha) = p^\beta \sum_{\substack{u = 1 \\ (u, p) = 1 \\ mu^{2k} \equiv n \pmod{p^\gamma}}}^{p^\gamma - 1} e\left(\frac{mu^k + nu^k}{p^\gamma}\right).
\]

(i) The case \(\beta = \gamma\)

We consider the congruence equation

\[
u^{2k} \equiv n \pmod{p^\beta}.
\]

From the assumption \((k, p) = 1\) each solution of \(nu^{2k} \equiv n \pmod{p}\) can be extended uniquely to the solution of (14) and vice versa. Therefore there are at most \(2k\) solutions of (14). This gives us

\[|K(m, n, k; p^\alpha)| \leq 2kp^\beta = 2kp^\frac{\alpha}{2}.
\]

(ii) The case \(\beta = \gamma - 1\)

In (13) \(u\) runs from 1 to \(p^\gamma - 1\) with the condition

\[
u^{2k} \equiv n \pmod{p^\beta}.
\]

Let \(u_1, u_2, \ldots, u_r\) \((r \leq 2k)\) be all the solutions of (15). If we write

\[u = u_j + vp^\beta \quad (0 \leq v \leq p - 1),\]

then we find that

\[
u \equiv \bar{u}_j - \bar{u}_j^2vp^\beta + \bar{u}_j^3v^2p^{2\beta} \pmod{p^\alpha},
\]

where \(u_j\bar{u}_j \equiv 1 \pmod{p^\alpha}\). Therefore

\[mu^{k} + nu^{k} \equiv (mu_j^{k} + nu_j^{k}) + kvp^\beta(mu_j^{2k} - n)u_j^{k+1} +
kv^2p^{2\beta}\left\{\frac{1}{2}m(k-1)u_j^{k-2} + nu_j^{k+2} + \frac{1}{2}n(k-1)u_j^{k+2}\right\} \pmod{p^\alpha}.
\]
The element in the braces on the right hand side is
\[
\begin{align*}
\frac{1}{2} m(k - 1)u_j^{k-2} + \frac{1}{2} n(k + 1)\bar{u}_j^{k+2} = \\
\frac{1}{2} \left\{ k(mu_j^{k-2} + nu_j^{k+2}) - (mu_j^{k-2} - nu_j^{k+2}) \right\} \equiv \\
\frac{1}{2} \left\{ k\bar{u}_j^{k+2}(mu_j^{2k} + n) - \bar{u}_j^{k+2}(mu_j^{2k} - n) \right\} \equiv \\
\equiv k\bar{u}_j^{k+2}n \not\equiv 0 \pmod{p}.
\end{align*}
\]

So the summation over \( v \) is a Gauss sum, hence its absolute value is bounded by \( \sqrt{p} \). Hence we have

\[
|K(m, n, k; p^\alpha)| \leq p^\beta 2k\sqrt{p} = 2kp^{\frac{\alpha}{2}}.
\]

Collecting these estimates and (10), we finally get

\[
|K(m, n, k; p^\alpha)| \leq 2k(m, n, p^\alpha)\frac{1}{2} p^{\frac{\alpha}{2}}
\]

for \( 1 \leq m, n \leq p^\alpha - 1 \) and \( (k, p) = 1 \), which proves Theorem 1.

For the proof of Theorem 2 we recall the multiplicative property of general Kloosterman sum shown in [6]:

\[
K(m, n, k; q) = K(m\bar{v}, n\bar{v}, k; u)K(m\bar{u}, n\bar{u}, k; v),
\]

where \( q = uv, (u, v) = 1, v\bar{v} \equiv 1 \pmod{u} \) and \( u\bar{u} \equiv 1 \pmod{v} \). Theorem 1 and the above property imply that

\[
|K(m, n, k; q)| \leq (2k)^{\nu(q)}(m, n, q)^{1/2}q^{1/2},
\]

where \( \nu(q) \) denotes the number of different prime factors of \( q \). The assertion of Theorem 2 follows immediately from the fact \( 2^{\nu(q)} \leq d(q) \).

3. Proof of Theorem 3

We shall prove Theorem 3 by induction on \( k \).
As noticed above, the assertion (8) in the case \( k = 1 \) is due to Chowla and Salié [1, 4].

Now suppose \( k > 1 \) and that the assertion of Theorem 3 is valid for all \( l < k \).

First we consider the case that \( k \) and \( p - 1 \) are coprimes. Then \( k \) is invertible mod \( p - 1 \), hence there exists an integer \( k_1 \) such that \( kk_1 \equiv 1 \pmod{p - 1} \). Since

\[
\chi(a) = \chi^{k_1}(a^k),
\]

we have

\[
K_{\chi}(m, n, k; p) = \sum_{a=1}^{p-1} \chi^{k_1}(a^k)e\left(\frac{ma^k + \bar{a}^k}{p}\right) = K_{\chi^{k_1}}(m, n, 1; p).
\]

Thus

\[
|K_{\chi}(m, n, k; p)| \leq 2\sqrt{p}
\]

for \((k, p - 1) = 1\).

Next we consider the case \( k_0 := (k, p - 1) > 1 \). Put \( k = k_0l \).

Let \( g \) be a primitive root mod \( p \), i.e. \( \mathbb{G} := (\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle \) and let \( h \) be an integer defined by \( \chi(g) = e^{2\pi i h} \).

If \( k_0 := (G : G^k) \) divides \( h \), i.e. \( h = k_0f \) with an integer \( f \), then we have

\[
\chi(a) = \chi'(a^{k_0})
\]

for any \( a \) and \( \chi' \) is a character such that \( \chi'(g) = e^{2\pi i f} \). Hence we may write

\[
K_{\chi}(m, n, k; p) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi'(a^{k_0})e\left(\frac{ma^{k_0}l + n(a^{k_0})l}{p}\right).
\]

Hence, by (9)

\[
K_{\chi}(m, n, k; p) = \sum_{\varphi \in (\mathbb{G}/G^{k_0})^*} \sum_{a \in G} \varphi(a)\chi'(a)e\left(\frac{ma^l + n\bar{a}^l}{p}\right) = \sum_{\varphi \in (\mathbb{G}/G^{k_0})^*} K_{\varphi\chi'}(m, n, l; p).
\]

Therefore we have, by the induction hypothesis,

\[
K_{\chi}(m, n, k; p) \ll \sqrt{p},
\]

where the implied constant depends only on \( k \).
When \( k_0 \mid h \), we shall show that the Kloosterman sum in question is equal to zero. For this purpose we consider the mean square of \( K_\chi(m, n, k; p) \) with respect to \( m \). Expanding \( |K_\chi(m, n, k; p)|^2 \), we have

\[
|K_\chi(m, n, k; p)|^2 = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) \bar{\chi}(b) e \left( \frac{m(a^k - b^k) + n(\bar{a}^k - \bar{b}^k)}{p} \right) = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(a) e \left( \frac{mb^k(a^k - 1) + nb^k(\bar{a}^k - 1)}{p} \right),
\]

where \( \bar{a} \) and \( \bar{b} \) are integers such that \( a \bar{a} \equiv 1 \pmod{p} \) and \( b \bar{b} \equiv 1 \pmod{p} \), respectively. Therefore

\[
\sum_{m=0}^{p-1} |K_\chi(m, n, k; p)|^2 = \sum_{a=1}^{p-1} \chi(a) \sum_{b=1}^{p-1} e \left( \frac{mb^k(a^k - 1)}{p} \right) \sum_{m=0}^{p-1} e \left( \frac{mb^k(a^k - 1)}{p} \right).
\]

Since the last summation is equal to \( p \) if \( a^k \equiv 1 \pmod{p} \) and 0 otherwise, we have

\[
\sum_{m=0}^{p-1} |K_\chi(m, n, k; p)|^2 = p(p-1) \sum_{a=1}^{p-1} \chi(a).
\]

When \( a \equiv g^j \pmod{p} \) with some \( j \), then

\[
a^k \equiv 1 \pmod{p} \iff j = rm \quad \text{for} \quad m = 0, 1, \ldots, k_0 - 1,
\]

therefore we have

\[
\sum_{a=1}^{p-1} \chi(a) = \sum_{m=0}^{k_0-1} e^{\frac{2\pi i a m}{p}} = \sum_{m=0}^{k_0-1} e^{\frac{2\pi i gm}{k_0}} = 0.
\]

The equations (19) and (17) show that \( K_\chi(m, n, k; p) = 0 \) when \( k_0 \mid h \).

This completes the proof of Theorem 3.

**Remark.** The above argument shows that

\[
\sum_{m=0}^{p-1} |K_\chi(m, n, k; p)|^2 = p(p-1)k_0.
\]
when \( k_0|h \).

References


S. Kanemitsu
Graduate School of Advanced Technology,
University of Kinki
Iizuka, Fukuoka, 820-8555, Japan
kanemitu@fuk.kindai.ac.jp

Y. Tanigawa
Graduate School of Mathematics
Nagoya University
Nagoya, 464-8602, Japan
tanigawa@math.nagoya-u.ac.jp

Yi Yuan and Zhang Wenpeng
Research Center for Basic Science
Xi’an Jiaotong University
Xi’an Shaanxi, China
yiyuan74@163.com and wpzhang@nwu.edu.cn