Šiauliai Math. Semin.,
10 (18), 2015, 213–223

ŠIAULIAI
MATHEMATICAL
SEMINAR
http://siauliaims.su.lt

TWISTED EXPONENTIAL SUMS OVER THE RING OF GAUSSIAN INTEGERS

Pavel Varbanets, Sergey Varbanets

Abstract. We obtain formulae and estimates for twisted exponential sums of the form $S(\chi, f, p^m) = \sum \chi(x)\mathrm{e}^{2\pi i \mathrm{Re}\,(f(x)/p^m)}$, where x runs the elements of certain subgroups of the group of residue classes modulo p^m in the ring of Gaussian integers.

Key words and phrases: Kloosterman sum, norm group, twisted exponential sum.

2010 Mathematics Subject Classification: 11L03, 11L05, 11L07.

Submitted: 26 September 2013

1. Introduction

Classical Kloosterman sums are special exponential sums of the form

$$Kl(a,b;q) = \sum_{x\in\mathbb{Z}}^{*} \mathrm{e}^{2\pi i(ax+bx^{-1})/q},$$

where a, b, q are integers and $q \geqslant 1$, $xx^{-1} \equiv 1 \,(\mathrm{mod}\, q)$.

These sums were introduced by Kloosterman in 1926 on occasion to give an asymptotic expression for the number of representations of a large integer by a diagonal quaternary definite quadratic form. He also provided a non-trivial bound for these sums. In 1948, as a consequence of his solution of the Riemann hypothesis for zeta-functions of curves over a finite field, Weil [7] established the stronger (probably optimal) bound

$$|Kl(a,b;q)| \leqslant q^{1/2}(a,b,q)^{1/2}\tau(q),$$

where $\tau(q)$ is the divisor function.

Ever since, Kloosterman sums play an important role in analytic number theory. For asymptotic problems of analytic number theory, one consider incomplete

Kloosterman sums

$$Kl(a,b;q,I)=\sum_{x\in I\subset\mathbb{Z}_q^*}{}^{*}\mathrm{e}^{2\pi i(ax+bx^{-1})/q},$$

in particular, when I is some subgroup of $\mathbb{Z}_q^*$ (for instance, see [2, 4, 8]).

The Kloosterman sum admits generalizations to the rings of integer elements of finite extensions of the rational number field $\mathbb{Q}$.

In our paper, we consider exponential sums over the ring of Gaussian integers $\mathbb{Z}[i]$. Let $\mathfrak{p}$ be a Gaussian prime number, $\mathfrak{p}\neq 1+i$, i.e., $\mathfrak{p}$ is an "odd" prime number in $\mathbb{Z}$. It is well known that the additive group of residue classes modulo $\mathfrak{p}^m$ is isomorphic to the additive group of residues $(\mathrm{mod}\ p^m)$ in $\mathbb{Z}$ if $\mathfrak{p}\notin\mathbb{Z}$, $N(\mathfrak{p})=p\equiv 1\ (\mathrm{mod}\ 4)$ (and similarly, for the multiplicative group of residue classes modulo $\mathfrak{p}^m$ and modulo p^m, respectively). Thus, henceforth, we suppose that $\mathfrak{p}=p\equiv 3\ (\mathrm{mod}\ 4)$ and $m\in\mathbb{N}$.

Our aim is the investigation of exponential sums associated with two subgroups U_m and E_m of the ring of residue classes modulo p^m, $p\equiv 3\,(\mathrm{mod}\ 4)$.

2. Some notations and preliminary results

Recall the standard notations which will be used in what follows. Let $G:=\left\{a+bi|a,b\in\mathbb{Z},\ i^2=-1\right\}$. For $\alpha\in G$, denote by $N(\alpha)=|\alpha|^2$ the norm of α, and by $Sp(\alpha)=2\mathrm{Re}\,\alpha$ the trace of α. G_γ (respectively, G_γ^*) denotes the complete (respectively, reduced) system of residues modulo γ in G. Moreover, for $\alpha\in\mathbb{Q}(i)$, $\alpha=\mathfrak{p}^k\frac{\alpha_0}{\beta_0}$, $\alpha_0,\beta_0\in G$, $(\alpha_0,\mathfrak{p})=(\beta_0,\mathfrak{p})=1$, denote $\nu_p(\alpha)=k$, $k\in\mathbb{Z}$. As usual $\gcd(a,b)$ is the greatest common divisor of a and b.

Let $p\equiv 3\,(\mathrm{mod}\ 4)$ be a rational prime number, and denote by E_m the following subgroup of G_{p^m}:

$$E_m:=\left\{x\in G_{p^m}\,|\,N(x)\equiv 1\,(\mathrm{mod}\ p^m)\right\}.$$

Moreover, let

$$U_m:=\left\{x\in G_{p^m}\,|\,x\equiv 1\,(\mathrm{mod}\ p)\right\}.$$

The subgroups E_m and U_m will be called the norm group in G_{p^m} and the group of principal identity, respectively.

Lemma 1. *The norm group E_m is a cyclic group of order $2(p+1)p^{m-1}$. Moreover, if $u+iv$ is a generating element of E_1, then $u+iv$ is a generating element of E_m for any fixed $m\in\mathbb{N}$, and*

$$(u+iv)^{2(p+1)}=1+p^2x_0+ipy_0,\quad x_0+2y_0^2\equiv 0\,(\mathrm{mod}\ p),\quad (x_0,p)=(y_0,p)=1,$$

so that, for any $t=0,1,\ldots$, one has modulo p^m

$$\mathrm{Re}\,(u+iv)^{2(p+1)t}\ \equiv\ A_0+A_1t+A_2t^2+\ldots+A_{m-1}t^{m-1},$$

$$\mathrm{Im}\,(u+iv)^{2(p+1)t} \equiv B_0 + B_1 t + B_2 t^2 + \ldots + B_{m-1}t^{m-1}, \tag{1}$$

where

$$\begin{aligned}
&A_0 \equiv 1 \,(\mathrm{mod}\, p), \quad B_0 \equiv 0 \,(\mathrm{mod}\, p),\\
&A_1 \equiv p^2 x_0 + \frac{1}{2} y_0^2 p^2 \,(\mathrm{mod}\, p^3), \quad \textit{i.e.,} \quad A_1 \equiv 0 \,(\mathrm{mod}\, p^3),\\
&A_2 \equiv -\frac{1}{2} y_0^2 p^2 \,(\mathrm{mod}\, p^3), \quad \textit{i.e.,} \quad A_2 = p^2 A_2', \quad (A_2', p) = 1,\\
&B_1 \equiv p y_0 \,(\mathrm{mod}\, p^3), \quad \textit{i.e.,} \quad B_1 = p B_1', \quad (B_1', p) = 1,\\
&B_2 \equiv A_3 \equiv B_3 \equiv \ldots \equiv A_{n-1} \equiv B_{n-1} \equiv 0 \,(\mathrm{mod}\, p^3).
\end{aligned}$$

This statement is contained in Lemma 2.4 in [5].

Next, let us assume that, for $k \in \{0, 1, \ldots, 2p+1\}$,

$$(u+iv)^k = u(k) + iv(k).$$

Then we have

$$\begin{aligned}
&(u(k), p) = (v(k), p) = 1 \quad \text{if} \quad k \neq 0, \frac{p+1}{2}, p+1, \frac{3(p+1)}{2},\\
&u(0) = 1, \quad v(0) = 0, \quad (u(p+1), p) = 1, \quad p \| v(p+1),\\
&u(k) \equiv 0 \,(\mathrm{mod}\, p), \quad (v(k), p) = 1 \quad \text{for} \quad rk = \frac{p+1}{2}, \frac{3(p+1)}{2}.
\end{aligned} \tag{2}$$

The parameters $u(k)$ and $v(k)$ also have been studied in [5], except for $k = \frac{1}{2}(p+1)$ and $k = \frac{3}{2}(p+1)$. However, these cases can be considered likewise.

Finally, it is easy to verify that the equations (1) hold true for all integers $t \in \mathbb{Z}$.

Moreover, from

$$(u(k) + iv(k)) \cdot (u(-k) + iv(-k)) = (u+iv)^{k-k} = 1,$$

we infer

$$u(k) \equiv u(-k), \quad v(k) \equiv v(-k) \,(\mathrm{mod}\, p).$$

Now, for any positive integers $\ell = 2(p+1)t + k$, $0 \leqslant k < 2(p+1)$, we can write

$$\begin{aligned}
\mathrm{Re}\,(u+iv)^{2(p+1)t+k} &\equiv A_0(k) + A_1(k)t + A_2 t^2 + \sum_{j=2}^{m-1} A_j(k) t^j,\\
\mathrm{Im}\,(u+iv)^{2(p+1)t+k} &\equiv B_0(k) + B_1(k)t + B_2 t^2 + \sum_{j=2}^{m-1} B_j(k) t^j,
\end{aligned} \tag{3}$$

where

$$\begin{aligned}
&A_j(k) = A_j u(k) - B_j v(k), \quad B_j(k) = B_j u(k) + A_j v(k), \quad j = \overline{0, m-1},\\
&A_0(k) \equiv u(k) \,(\mathrm{mod}\, p), \quad B_0(k) \equiv v(k) \,(\mathrm{mod}\, p),
\end{aligned}$$

$$
\begin{aligned}
&A_j(k) \equiv B_j(k) \equiv 0 \,(\mathrm{mod}\, p^4), \quad k = 0, 1, \dots, 2p+1, \quad j \geqslant 3,\\
&p||B_1(k), \quad p||A_1(k), \quad p^2||A_2(k), \quad p^2||B_2(k)\\
&\qquad \text{if} \quad k \neq 0, \frac{1}{2}(p+1), (p+1), \frac{3}{2}(p+1),\\
&A_1(0) \equiv 0 \,(\mathrm{mod}\, p^4), \quad B_1(0) \equiv py_0 \,(\mathrm{mod}\, p^3),\\
&p^2||A_2(0), \quad B_2(0) \equiv 0 \,(\mathrm{mod}\, p^3),\\
&(A_0(p+1), p) = 1, \quad p||B_0(p+1), \quad p^2||A_1(p+1), \quad p||B_1(p+1),\\
&p^2||A_2(p+1), \quad B_2(p+1) \equiv 0 \,(\mathrm{mod}\, p^3),\\
&p||A_1(k), \quad p^2||B_1(k), \quad p^2||A_2(k), \quad B_2(k) \equiv 0 \,(\mathrm{mod}\, p^3)\\
&\qquad \text{if} \quad k = \frac{1}{2}(p+1) \text{ or } \frac{3}{2}(p+1). \qquad (4)
\end{aligned}
$$

The following lemma is a generalization of the well-known Postnikov lemma which allows to replace a nontrivial multiplicative character mod p^n by an additive character.

LEMMA 2. *Let $p \equiv 3 \,(\mathrm{mod}\, 4)$ be a prime number, and $m \geqslant 3$ be a positive integer. Then there exists a polynomial $f(u)$ with coefficients from G*

$$f(u) = u + a_2 u^2 + \dots + a_{N-1} p^{N-1}$$

such that, for any character χ of the group $U_m \subset G^*_{p^m}$,

$$U_m := \{1 + pu |\, u \in G_{p^{m-1}}\},$$

we have

$$\chi(1 + pu) = e_{p^{m-1}}(\Lambda f(u)),$$

where $\Lambda \in G_{p^{m-1}}$ depends only on χ, and the coefficients a_k satisfy the inequalities

$$\nu_p(a_k) \geqslant k - \nu_p(k) - 1, \quad k = 2, 3, \dots.$$

Proof. Since the residue classes modulo $p, p \equiv 3 \,(\mathrm{mod}\, 4)$ over G form a field, the order of the multiplicative group G_p^* is equal to $p^2 - 1$. We may select a generating element g of G_p^* in such a way that $g^{p^2-1} = 1 + pu$, $u \in G_{p^{m-1}}$, $(u, p) = 1$.

Now, for any $k \in G_{p^{m-1}}$, the series

$$1 + kpu_1 + p^2 u_1^2 \frac{k(k-1)}{2} + \dots$$

converges to the function $(1 + pu)^k$ with respect to the continuation of the p-adic valuation from $\mathbb{Q}$ to $\mathbb{Q}[i]$.

Putting modulo p^{m-1}

$$
\begin{aligned}
u_k \quad :\equiv \quad & ku + pu^2 \frac{k(k-1)}{2} + \dots\\
& + p^{m+m_0} u^{m+m_0} \frac{k(k-1)\dots(k-m-m_0+1)}{(m+m_0)!},
\end{aligned}
$$

where $m_0 = \left[\frac{m}{p-1}\right] + 1$, we conclude that the multiplicative group U_m and the additive group $G_{p^{m-1}}$ are isomorphic (for details, see [1], pp. 379–381). Moreover, the mapping $G_{p^{m-1}} \to \mathbb{C}$ defined by

$$1 + pu \to e_{p^{m-1}}(\mathrm{Re}\,(\Lambda f(u))), \quad \Lambda \in G_{p^{m-1}}, \quad \Lambda \neq 0, \tag{5}$$

where

$$f(u) = u + a_2u^2 + \ldots + a_{N-1}u^{N-1} \,(\mathrm{mod}\, p^m),$$
$$a_s \equiv (-1)^{s-1}p^{s-1} \cdot \frac{1}{s} \,(\mathrm{mod}\, p^m), \quad s = \overline{2, N-1}, \quad N = m + \left[\frac{m}{p-1}\right] + 1,$$

assigns a character of the group U_m.

Since different values $\Lambda \in G_{p^{m-1}}$ define different characters of the group U_m and the order U_m is equal to the order of $G_{p^{m-1}}$, we conclude that any nontrivial character of U_m is constructed by formula (5).

We denote by χ_Λ the character modulo p^m with respect to the parameter Λ in Lemma 2.

LEMMA 3. *Let $f(x) = Ax + Bx^2 + p(Cx^3 + Dx^4 + \ldots)$ be a polynomial over $\mathbb{Z}$, and let $(B, p) = 1, p > 2$ be a prime number. Then we have*

$$|S(f; p^n)| := \left| \sum_{x \in \mathbb{Z}_{p^n}} \mathrm{e}^{2\pi i f(x)/p^n} \right| \leqslant p^{n/2}.$$

COROLLARY 1. *Let $f(x) = Bx + Cx^2 + Dx^3 + \ldots$ be a polynomial over $\mathbb{Z}$, and $(C, p) = 1$. Then, for any $A \in \mathbb{Z}$, we have*

$$|S(f; p^n)| := \left| \sum_{x \in \mathbb{Z}^*_{p^n}} \mathrm{e}^{2\pi i (Ax + f(x^{-1}))/p^n} \right| \leqslant 2p^{n/2},$$

where x^{-1} denotes the multiplicative inverse of x in $\mathbb{Z}^*_{p^n}$.

For the proofs of Lemma 3 and Corollary 1, see [6].

3. Exponential sums over E_m, $m > 1$

Let $x \in E_m$. By (3) and (4), we have

$$x = x_0(k) + p \sum_{j=1}^{m-1} \left(A'_j(k) + iB'_j(k)\right) t^j,$$

where $x_0(k) = A_0(k) + iB_0(k)$, $A_j(k) = pA'_j(k)$, $B_j(k) = pB'_j(k)$.

Now, for an arbitrary polynomial $f(z) \in G[z]$ and $x \in E_m$, $x = (u+iv)^{2(p+1)t} \cdot (u(k)+iv(k))$, we can write

$$\begin{aligned} f(x) &= f(x_0(k)) + pf'(x_0(k)) \sum_{j=1}^{m-1} (A'_j(k) + iB'_j(k))t^j \\ &\quad + \frac{1}{2} f''(x_0(k))p^2 \Bigg(\sum_{j=1}^{m-1} (A'_j(k) + iB'_j(k))t^j \Bigg)^2 + \dots \\ &= f(x_0(k)) + pC_1(k)t + p^2C_2(k)t^2 + p^3C_3(k)t^3 + \dots, \end{aligned} \tag{6}$$

where, for $k \in \{0, 1, \dots, 2p+1\}$,

$$\begin{aligned} C_1(k) &= p(A'_1(k) + iB'_1(k))f'(x_0(k)), \\ C_2(k) &= p^2(A'_2(k) + iB'_2(k))f'(x_0(k)) + (A'_1(k) + B'_1(k))^2 \frac{f''(x_0(k))}{2}, \\ C_j(k) &\equiv 0 \pmod{p^3}. \end{aligned} \tag{7}$$

By direct calculation, for $k \neq 0, \frac{1}{2}(p+1), (p+1), \frac{3}{2}(p+1)$, we can assure that

a) $\nu_p(C_1(k)), \nu_p(C_j(k)) \geqslant 2$, $j \geqslant 2$, if $\nu_p(f'(x_0(k))) = 0$,

b) $\nu_p(C_1(k)) \geqslant 2$, $\nu_p(C_2(k)) \geqslant 2$, $\nu_p(C_j(k)) \geqslant 3$, $j \geqslant 3$, if $\nu_p(f'(x_0(k))) \geqslant 1$, $\nu_p(f''(x_0(k))) = 0$,

c) $\nu_p(C_1(k)) = 2$, $\nu_p(C_2(k)) \geqslant 2$, $\nu_p(C_j(k)) \geqslant 3$, $j \geqslant 3$, if $k = p+1$ and $(f'(x_0(k)), p) = 1$,

d) $\nu_p(C_1(k)) \geqslant 2$, $\nu_p(C_2(k)) = 2$, $\nu_p(C_j(k)) \geqslant 3$, $j \geqslant 3$, if $k = p+1$ and $f'(x_0(k)) \equiv 0 \pmod{p}$,

e) $\nu_p(C_1(k)) = 1 + \nu_p(f'(x_0(k)))$, $\nu_p(C_2(k)) = 2 + \nu_p(f'(x_0(k)))$, $\nu_p(C_j(k)) \geqslant 3$, $j \geqslant 3$, if $k = \frac{p+1}{2}$ or $3\frac{p+1}{2}$,

f) $\nu_p(C_1(0)) \geqslant 4$, $\nu_p(C_2(0)) = 2$, $\nu_p(C_j(0)) \geqslant 3$, $j \geqslant 3$, if $f'(1) + 2f''(1) \not\equiv 0 \pmod{p}$.

THEOREM 1. *Let $f(x) \in G_{p^m}[x]$, and let d be the degree of $f(x)$, $(d,p) = 1$. Assume that $f'(x)$ has no multiple roots in G_p^* and $f'(1) + f''(1) \not\equiv 0 \pmod{p}$. Then the estimate*

$$\left| \sum_{x \in E_m} \mathrm{e}^{2\pi i (\mathrm{Re}\, f(x))/p^m} \right| \leqslant (d+1)p^{m/2}$$

holds.

Proof. From (6)–(7), we have

$$\left| \sum_{x \in E_m} \mathrm{e}^{2\pi i (\mathrm{Re}\, (f(x)))/p^m} \right|$$

$$\leqslant \sum_{k=0}^{2p+1} \left| \sum_{t=0}^{p^{m-1}-1} \mathrm{e}^{2\pi i \mathrm{Re}\left((C_1(k)t+pC_2(k)t^2+p^2C_3(k)t^3+\ldots)/p^{m-1}\right)} \right|. \tag{8}$$

By Lemma 3 in the case (a), the inner sum over t on the right-hand side of (8) tends to zero. Otherwise, this sum has absolute value $\leqslant p^{\frac{m}{2}}$, and we deduce

$$\left| \sum_{x \in E_m} \mathrm{e}^{2\pi i (\mathrm{Re}\,(f(x)))/p^m} \right| \leqslant (d+1)p^{m/2}.$$

Here, we take into account that, for $0 \leqslant k \leqslant 2p+1$, the cases (b)–(f) may appear at most $d-1+2 = d+1$ times.

The following statement is an immediate consequence of Theorem 1.

COROLLARY 2. *For any* $\alpha \in G_{p^m}^*$ *and* $n \in \mathbb{N}$, $(n,p)=1$,

$$\left| \sum_{x \in E_m} \mathrm{e}^{2\pi i (\mathrm{Re}\,(\alpha x^n))/p^m} \right| \leqslant 2p^{m/2}. \tag{9}$$

Let us consider the exponential sum

$$K_{E_m}(1,\alpha) := \sum_{\substack{x,y \in E_m \\ xy \equiv 1 \,(\mathrm{mod}\, p^m)}} \mathrm{e}^{2\pi i \mathrm{Re}\left((x+\alpha y)/p^m\right)}. \tag{10}$$

The sum K_{E_m} is called the Kloosterman sum associated with the norm group E_m.

Let $\alpha = a+bi$, $x = u+iv^{2(p+2)t+k}$, $xy \equiv 1 \,(\mathrm{mod}\, p^m)$. Then, by (2)–(4), we can write modulo p^m

$$\mathrm{Re}\,(x+\alpha y) = \sum_{j=0}^{m-1} C_j(k)t^j, \quad 0 \leqslant k \leqslant 2p+1, \quad t \in \mathbb{Z}_{p^{m-1}},$$

where

$$\begin{aligned} C_j(k) &= A_j(u(k)+(-1)^j au(k)+(-1)^j bv(k)) \\ &\quad +B_j(-v(k)+(-1)^j av(k)-(-1)^j bu(k)). \end{aligned}$$

In particular,

$$\begin{aligned} C_1(k) &\equiv py_0((1+a)v(k)+bu(k)) \,(\mathrm{mod}\, p^3), \\ C_2(k) &\equiv -\frac{1}{2}p^2y_0^2((1+a)u(k)+bv(k)) \,(\mathrm{mod}\, p^3). \end{aligned}$$

Denote

$$\Delta := \begin{vmatrix} b & -(1+a) \\ 1+a & b \end{vmatrix} = (b^2+(1+a)^2).$$

Since the congruence $\Delta \equiv 0 \pmod p$ is impossible if $(a+1,b,p)=1$, we conclude, by Lemma 3, that

$$\left|\sum_{t=0}^{p^{m-1}-1} \mathrm{e}^{2\pi i(C_0(k)+C_1(k)t+C_2(k)t^2+\ldots)/p^m}\right| \leqslant \begin{cases} 0 & \text{if} \quad (1+a)v(k)-bu(k) \not\equiv 0 \pmod p, \\ p^{m/2} & \text{if} \quad (1+a)v(k)-bu(k) \equiv 0 \pmod p. \end{cases}$$

In view of the condition $u^2+v^2 \equiv 1 \pmod p$, the congruence $(1+a)v(k)-bu(k) \equiv 0 \pmod p$ may hold for at most two values k, $k \in \{0,1,\ldots,2p+1\}$. Indeed, let $(1+a)v(k)-bu(k) \equiv 0 \pmod p$. We have modulo p

$$1 \equiv u^2(k)+v^2(k) \equiv \left(\left(\frac{1+a}{b}\right)^2+1\right)v^2(k) \quad \text{if} \quad b \not\equiv 0.$$

Hence, we have at most two values of $v(k)$ for which $(1+a)v(k)-bu(k) \equiv 0 \pmod p$. Moreover, if $0 \leqslant k_1 < k_2 \leqslant 2p+1$, we have $(u+iv)^{k_1} \equiv (u+iv)^{k_2} \pmod p$. The situation is similar for $1+a \not\equiv 0 \pmod p$. So, for $\alpha \in G$, $\alpha = a+bi$, $(a+1,b,p)=1$, we have

$$|K_{E_m}(1,\alpha)| \leqslant 2p^{m/2}. \tag{11}$$

In the case $a \equiv -1 \pmod p$ and $b \equiv 0 \pmod p$, it is easy to deduce

$$\left|K_{E_m}(1,\alpha)\right| \leqslant \begin{cases} 0 & \text{if} \quad \nu_p(\gcd(1+a,b))=1, \\ 2p^{m+1/2} & \text{if} \quad \nu_p(\gcd(1+a,b))>1. \end{cases} \tag{12}$$

Thus, we proved the following assertion.

THEOREM 2. *Let $\alpha = a+bi \in G$, and let p be a prime rational number, $p \equiv 3 \pmod 4$. Then*

$$\left|K_{E_m}(1,\alpha)\right| \leqslant \begin{cases} 2p^{m/2} & \textit{if} \quad \nu_p(\gcd(1+a,b))=0, \\ 0 & \textit{if} \quad \nu_p(\gcd(1+a,b))=1, \\ 2p^{(m+1)/2} & \textit{if} \quad \nu_p(\gcd(1+a,b))>1. \end{cases}$$

Now we will make an estimate of the twisted exponential sum over the group of principal identity U_m

$$S(\chi,f)=\sum_{x \in U_m} \chi(x)\mathrm{e}^{2\pi i \mathrm{Re}\left(f(x)/p^m\right)}. \tag{13}$$

THEOREM 3. *Let χ_Λ be a nontrivial character modulo p^m over G, and $F(x) \in G[x]$, where $F'(1) \not\equiv -2F''(1) \pmod p$. Then we have*

$$\left|\sum_{x \in U_m} \chi_\Lambda(x)\mathrm{e}^{2\pi i \mathrm{Re}\left(F(x)/p^m\right)}\right| \leqslant \begin{cases} N(p)^{m/2} & \textit{if} \quad F'(1)+\Lambda \equiv 0 \pmod p, \\ 0 & \textit{otherwise.} \end{cases} \tag{14}$$

Proof. For $x \in U_m$, we write $x = 1+pu$, $u \in G_{p^{m-1}}$. Hence, a formal expansion by Taylor's formula gives modulo p

$$\begin{aligned} F(x) &= F(1+pu) \\ &\equiv F(1) + puF'(1) + b_2F''(1)u^2 + \ldots + b_mF^{(m)}(1)u^m, \end{aligned} \tag{15}$$

where $b_2 = \frac{1}{2}p^2F''(1)$, $\nu_p(b_j) \geqslant j - \nu_p(j!) \geqslant \left[\frac{j}{p-1}\right]$, $j = 3, 4, \ldots, M$, $M = \left[m\frac{p-1}{p-2}\right]$. Moreover, by Lemma 2, we have

$$\chi_\Lambda(x) = \chi_\Lambda(1+pu) = \mathrm{e}^{2\pi i \mathrm{Re}\left(\Lambda(u+a_2pu^2+a_3p^2u^3+\ldots)/p^{m-1}\right)}. \tag{16}$$

Thus, from (15) and (16), we infer

$$\chi_\Lambda(x)\mathrm{e}^{2\pi i \mathrm{Re}\left(F(x)/p^m\right)} = \mathrm{e}^{2\pi i \mathrm{Re}\left(F(1)/p^{m-1}\right)}\mathrm{e}^{2\pi i \mathrm{Re}\left((A_1u+A_2u^2+\ldots)/p^{m-1}\right)},$$

where

$$A_1 = p(F'(1)+\Lambda), \quad A_2 = \frac{1}{2}p^2(F''(1)-\Lambda), \quad A_j \equiv 0 \,(\mathrm{mod}\, p^3), \quad j \geqslant 3.$$

From the condition $F'(1) + F''(1) \not\equiv 0 \,(\mathrm{mod}\ p)$, it follows that the congruences mod p

$$F'(1) + \Lambda \equiv 0 \quad \text{and} \quad F''(1) - \Lambda \equiv 0$$

cannot be realized simultaneously. Therefore, by Lemma 2, we obtain the statement of the theorem.

COROLLARY 3. *Let χ_Λ be a nontrivial character modulo p^m over G, and $F(x)$ be an arbitrary polynomial from $G[x]$ such that the system of congruences $zF'(z) + \Lambda \equiv 0 \,(\mathrm{mod}\, p)$, $z^2F''(z) - \Lambda \equiv 0 \,(\mathrm{mod}\, p)$ has no solutions. Then the estimate holds*

$$\left| \sum_{x \in G^*_{p^m}} \chi_\Lambda(x)\mathrm{e}^{2\pi i \mathrm{Re}\left(F(x)/p^m\right)} \right| \leqslant \mathfrak{I}_F(p)(N(p))^{m/2}, \tag{17}$$

where

$$\mathfrak{I}_F(p) = \#\left\{z \in G^*_p |\ zF'(z) + \Lambda \equiv 0 \,(\mathrm{mod}\, p)\right\}.$$

Proof. Putting $x = z(1+pu)$, $z \in G^*_p$, $u \in G_{p^{m-1}}$ and taking into account the expansion

$$F(z(1+pu)) \equiv F(z) + puzF'(z) + \frac{1}{2}p^2u^2z^2F''(z) + \ldots \,(\mathrm{mod}\, p^m),$$

we obtain

$$\sum_{x \in G^*_{p^m}} \chi_\Lambda(x)\mathrm{e}^{2\pi i \mathrm{Re}\left(F(x)/p^m\right)}$$

$$= \sum_{z\in G_{p^*}} \mathrm{e}^{2\pi i \mathrm{Re}\left(F(z)/p^m\right)} \chi_\Lambda(z) \sum_{u\in G_{p^{m-1}}} \mathrm{e}^{2\pi i \mathrm{Re}\left((A_1u+A_2u^2+\ldots)/p^{m-1}\right)},$$

where

$$A_1 = zF'(z)+\Lambda, \quad A_2 = \frac{1}{2}p(z^2F''(z)-\Lambda), \quad A_j \equiv 0 \,(\mathrm{mod}\, p^2), \quad j \geqslant 3.$$

Now the assertion of the corollary follows immediately from Lemma 3.

REMARK 1. The exponential sums over E_1 can be investigated with help of the fundamental works of Weil [7] and Katz [3]. In a similar way, it can be deduced an estimate for the sum

$$\sum_{x\in G_{p^m}} \chi_\Lambda(R(x)), \tag{18}$$

where $R(x)$ is a rational function over G.

The assertion of sums (14) and (18) have applications in the problems of generating the sequences of pseudorandom numbers by congruential polynomial and inversive generators.

References

[1] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Nauka, Moscow, 1964 (in Russian).

[2] A.A. Karatsuba, Analogous of incomplete Kloosterman sums and their applications, Number Theory (Liptovsky Ián, 1995), *Tatra Mt. Math. Publ.*, **11**, 89–120 (1997).

[3] N.M. Katz, *Gauss Sums, Kloosterman Sums and Monodromy Groups*, Ann. of Math. Stud. 116, Princeton Univ. Press, Princeton, NY, 1988.

[4] M.A. Korolev, Incomplete Kloosterman sums and their applications, *Izv. Ross. Akad. Nauk, Ser. Math.*, **64**, 41–64 (2000) (in Russian) = *Izv. Math.*, **64**, 1129–1152 (2000).

[5] S. Varbanets, General Kloosterman sums over ring of Gaussian integers, *Ukr. Math. J.*, **59**(9), 1179–1200 (2007).

[6] P. Varbanets, S. Varbanets, Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus, in: *Proc. of 4th Intern. Conf. on Analytic Number Theory and Spatial Tessellations*, Book 4, Vol. 1, Kyiv, Ukraine, September 22–28, 112–130, 2008.

[7] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.*, **34**, 204–207 (1948).

[8] P. Xi, Incomplete Kloosterman sums and Hooley's R^*-conjecture, arXiv:1111.5459v2[math.NT].

Pavel Varbanets, Sergey Varbanets
Department of Computer Algebra and Discrete Mathematics,
I.I. Mechnikov Odessa National University,
Dvoryanskaya Str. 2, 65026 Odessa, Ukraine;
e-mail: varb@sana.od.ua