ISSN 2304-1579. Visnyk Odesk. Nats. Univers. Mat. i Mekh.–2014 .–V.19,Is.2(22).–P.66–74

Mathematical Subject Classification: 11L05, 11L07, 11L40
UDC 511.321

S. S. Sergeev
Odesa I. I. Mechnikov National University

CHARACTER SUMS ANALOGUE OF KLOOSTERMAN SUMS ON NORM GROUP

Сергєєв С. С. Суми характерів, аналог сум Клостермана на нормових групах. Розглядаются суми характерів, котрі є аналогами сум Клостермана на нормових групах у кільці цілих гаусових чисел. Отримані нетривіальні оцінки експоненціальних сум та сум характерів по модулю p^m, где p — просте рациональне число, $\mathrm{p} \equiv 3 \pmod 4$.
Ключові слова: суми характерів, суми Клостермана, нормові групи.

Сергеев С. С. Суммы характеров, аналог сумм Клостермана на норменных группах. Рассматриваются суммы характеров, являющиеся аналогами сумм Клостермана на норменных группах в кольце целых гауссовых чисел. Получены нетривиальные оценки экспоненциальных сумм и сумм характеров по модулю p^m, где p — простое рациональное число, $\mathrm{p} \equiv 3 \pmod 4$.
Ключевые слова: суммы характеров, сумма Клостермана, норменные группы.

Sergeev S. S. Character sums analogue of Kloosterman sums on norm group. We consider character sums, analogue of Kloosterman sums over norm group in the ring of Guassian integers. We obtain non-trivial estimation of exponential sums and character sums modulo p^m, where p — prime number, $\mathrm{p} \equiv 3 \pmod 4$.
Key words: character sums, Kloosterman sums, norm group.

Introduction. Let χ and φ be multiplicative and additive characters of finite field k_q with $q = p^n$ elements. Usually consider three type sums

$$\sum_{x \in V \subset k_q} \chi(f(x)), \quad \sum_{x \in V \subset k_q^*} \chi(f(x)), \quad \sum_{x \in V \subset k_q^*} \chi(f(x))\varphi(g(x)),$$

where $f(x), g(x)$ are polynomials or rational functions, which respectively call exponential sum, character sum and mixed sum. When $V = k_q$ (resp. k_q^*), that sums call complete exponential sum, complete character sum and complete mixed sum (resp.). Otherwise, such sums call incomplete sums. Sometimes as V consider a subgroup k_q (or k_q^*, resp.). Prove by A. Weil [7] the Riemann Hypothesis for algebraic curves over finite field give leave to arrive at non-trivial bounds for mentioned above complete sums. In particular, for $f(x) = ax + bx^{-1}, x \in k_q^*$, A. Weil [7] proved uniprovable bound for Kloosterman sum

$$K(a, b; q) := \sum_{x \in k_q^*} \chi\left(ax + bx^{-1}\right) << q^{1/2}. \tag{1}$$

Similar results may be obtain for mentioned above sums over the ring of residue classes $\pmod q$ in $\mathbb{Z}$ ([2, 5, 6]). Our goal is construction of non-trivial estimates for character sums analogue of Kloosterman sums on norm group in the ring of residue classed (mod q) of the Gaussian integers.

Notation. We standardize some notation to be used throughout this paper. Lower case Roman (or Greek, respectively) letters usually denote rational (or Gaussian, respectively) integers; in particular, m, n, k are positive integers and p is always a rational prime $\mathrm{p} \equiv 3 \pmod 4$. We also define a norm on $\mathbb{Q}(i)$ into $\mathbb{Q}$ by $N(\alpha) = |\alpha^2|$. For the sake of convenience, we denote by G the set of the Gaussian integers. Let $\mathbb{Z}_q$ (or G_q respectively) denote the ring of residue classes modulo q and $\mathbb{Z}_q^*$ (or G_q^* respectively) denote the multiplicative group in $\mathbb{Z}_q$ (or G_q). If $x \in G_q^*$ we write x^{-1} for the multiplicative inverse of x (mod q), i.e. x^{-1} is Gaussian integer satisfying $xx^{-1} \equiv 1 \pmod q$. We denote by k_q a finite field with q elements, $q = \mathrm{p}^r$, p a prime. For a finite set X, $|X|$ denotes its cardinality. By $f << g$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f, g are defined, we mean synonymously that there exists a constant $C > 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. The "implied constant"may depend on the some parameters which are always specified or clear in context. As usual, $gcd(a, b)$ or (a, b) stand for the greatest common divisor of a and b, where $a, b \in \mathbb{Z}$ (or G). Though $\mathbb{Z}[x]$ (or $G[x]$) we denote the polynomial ring over $\mathbb{Z}$ (or G). For $a \in \mathbb{Z}$ (or $\alpha \in G$) it stands $\nu_{\mathrm{p}}(a)$ (or $\nu_{\mathrm{p}}(\alpha)$) if $\mathrm{p}^{\nu_{\mathrm{p}}}(a) \mid a, \mathrm{p}^{\nu_{\mathrm{p}}}(a+1) \nmid a$. Moreover, $\sum\limits_{S(C)}$ means the summation under the condition C is defined additionally, and $e_q(x) := e^{2\pi i \frac{x}{q}}$.

Auxiliary arguments. Before starting out study of character sums several lemmas will be used in the sequal.

Let us denote by E_m the following subgroup in G_{p}^m.

$$E_m := \left\{ x \in G_{\mathrm{p}^m}^* : N(x) \equiv 1 \ (\mathrm{mod}\ \mathrm{p}^m) \right\}. \tag{2}$$

The subgroup E_m we will call the norm group in $G_{\mathrm{p}^m}^*$.

Lemma 1. *The norm group E_m is a cyclic group of order* $(\mathrm{p}+1)\mathrm{p}^{m-1}$.

Let $u + iv$ be a generating element of E_m. Then

$$\begin{aligned} &(u+iv)^{\mathrm{p}+1} = 1 + \mathrm{p}^2 x_0 + i\mathrm{p} y_0, \quad x_0, y_0 \in \mathbb{Z}, \\ &x_0 + 2y_0^2 \equiv 0 \ (\mathrm{mod}\ \mathrm{p}), \quad (x_0, \mathrm{p}) = (y_0, \mathrm{p})) = 1, \end{aligned}$$

and also for any $t = 4, 5, \ldots, \mathrm{p}^{m-1} - 1$, we have modulo p^m

$$\begin{aligned} Re(u+iv)^{(\mathrm{p}+1)t} &\equiv A_0 + A_1 t + \cdots + A_{m-1} t^{m-1}, \\ Im(u+iv)^{(\mathrm{p}+1)t} &\equiv B_0 + B_1 t + \cdots + B_{m-1} t^{m-1}, \end{aligned}$$

where

$$\begin{array}{ll} A_0 \equiv 1 \ (\mathrm{mod}\ \mathrm{p}^4), & B_0 \equiv 0 \ (\mathrm{mod}\ \mathrm{p}^4), \\ A_1 \equiv \mathrm{p}^2(x + \frac{1}{2}y_0^2 \ (\mathrm{mod}\ \mathrm{p}^3), & B_1 \equiv \mathrm{p} y_0 \ (\mathrm{mod}\ \mathrm{p}^3), \\ A_2 \equiv -\frac{1}{2}\mathrm{p}^2 y_0^2 \ (\mathrm{mod}\ \mathrm{p}^3), & B_2 \equiv 0 \ (\mathrm{mod}\ \mathrm{p}^3), \\ A_j \equiv B_j \equiv 0 \ (\mathrm{mod}\ \mathrm{p}^3), & j = 3, 4, \ldots, m-1. \end{array}$$

Denote

$$(u+iv)^k = u(k) + iv(k), 0 \leqslant k \leqslant \mathrm{p}.$$

An arbitrary element from E_m has unique representation $w = (u+iv)^{(\mathrm{p}+1)t+k}$. Thus

$$w = (u+iv)^{(\mathrm{p}+1)t+k} \equiv \sum_{j=0}^{m-1} \left(A_j(k) + iB_j(k)\right) t^j \pmod{\mathrm{p}^m}. \tag{3}$$

It is clear

$$\begin{array}{l} A_j(k) = A_j u(k) - B_j v(k), \\ B_j(k) = A_j v(k) + B_j u(k). \end{array}$$

Corollary 1. *For $k = 1, 2, \dots, \mathrm{p}$, we have*

$$\begin{array}{ll} (u(k),\mathrm{p}) = (v(k),\mathrm{p}) = 1, & \text{if } k \neq \frac{\mathrm{p}+1}{2}, \\ u(0) = 1, v(0) = 0, & u\left(\frac{\mathrm{p}+1}{2}\right) \equiv 0 \pmod{\mathrm{p}}, \left(\frac{\mathrm{p}+1}{2}, \mathrm{p}\right) = 1, \end{array}$$

moreover, for $k \neq \frac{\mathrm{p}+1}{2}$

$$\begin{array}{l} A_0(k) \equiv u(k), \quad B_0(k) \equiv v(k) \pmod{\mathrm{p}}, \\ \mathrm{p} \mid\mid A_1(k), \quad \mathrm{p} \mid\mid B_1(k), \quad \mathrm{p}^2 \mid\mid A_2(k), \quad \mathrm{p}^2 \mid\mid B_2(k); \end{array}$$

and

$$\begin{array}{l} A_1(0) \equiv 0, \quad B_1(v) \equiv \mathrm{p}y_0 \pmod{\mathrm{p}^4}, \quad \mathrm{p}^2 \mid\mid A_2(0), \quad B_2(0) \equiv 0 \pmod{\mathrm{p}^3}, \\ A_0\left(\frac{\mathrm{p}+1}{2}\right) \equiv 0 \pmod{\mathrm{p}}, \quad \left(B_0\left(\frac{\mathrm{p}+1}{2}\right), \mathrm{p}\right) = 1, \\ \mathrm{p} \mid\mid A_1\left(\frac{\mathrm{p}+1}{2}\right), \quad \mathrm{p}^2 \mid\mid B_1\left(\frac{\mathrm{p}+1}{2}\right), \quad \mathrm{p}^2 \mid\mid A_2\left(\frac{\mathrm{p}+1}{2}\right), \quad B_2\left(\frac{\mathrm{p}+1}{2}\right) \equiv 0 \pmod{\mathrm{p}^3}; \end{array}$$

$$A_j(k) = B_j(k) \equiv 0 \pmod{\mathrm{p}^3}, \quad k = 0, 1, \dots, \mathrm{p}, j \geqslant 3.$$

For the proof of Lemma 1 and its Corollary see [6] (Lemma 2).

Lemma 2. *Let $f(x), g(x)$ be polynomials over G,*

$$f(x) = \sum_{j=1}^{r} A_j x^j, G(x) = \sum_{j=1}^{s} B_j x^j, r, s \geqslant 3,$$

and, moreover, let

$$\begin{array}{l} 0 \leqslant \nu_{\mathrm{p}}(A_2) < \nu_{\mathrm{p}}(A_j), j \geqslant 3; \\ (B_1, \mathrm{p}) = 1, \nu_{\mathrm{p}}(B_j) \geqslant 1, j = 2, 3, \dots \end{array}$$

Then

$$\begin{array}{l} \left| \sum\limits_{x \in G_{\mathrm{p}^m}} e_{\mathrm{p}^m}\left(Re\left(f(x)\right)\right) \right| \leqslant \\ \leqslant \begin{cases} 0 & \text{if } \nu_{\mathrm{p}}(A_1) < \nu_{\mathrm{p}}(A_2); \\ 2^{\frac{m}{2}} \mathrm{p}^{m+\frac{1}{2}\nu_{\mathrm{p}}(A_2)} & \text{if } \nu_{\mathrm{p}}(A_2) < m, \nu_{\mathrm{p}}(A_1) \geqslant \nu_{\mathrm{p}}(A_2); \\ \mathrm{p}^{2m} & \text{if } \nu_{\mathrm{p}}(A_2) \geqslant m; \end{cases} \end{array} \tag{4}$$

$$\left| \sum_{x \in G^*_{\mathrm{p}^m}} e_{\mathrm{p}^m}\left(Re(f(x) + \alpha x^{-1})\right) \right| \leqslant 2 I_0^{\frac{m}{2}} \mathrm{p}^m, \tag{5}$$

where I_0 is the number of solutions of the congruence over G^*_{p}

$$A_1 u^2 - B_1 \equiv 0 \pmod{\mathrm{p}}.$$

The assertion of this Lemma it is well-known (see, for example, [6], Lemma 3).

Lemma 3. *Let k_q be a finite field and let χ be a non-trivial multiplicative character of k_q^* of order $d > 1$. Suppose $f \in k_q[x]$ has m distinct roots and f is not a perfect d-th power (mod p). Then we have*

$$\left|\sum_{x\in k_q} \chi(f(x))\right| \leqslant (m-1)q^{1/2} \tag{6}$$

(See [4], Ch. 2C', p. 43).

Lemma 4. *([6], Lemma 1) Let $\mathrm{p} \equiv 3 \pmod 4$ be a prime, $n \geqslant 3$ be a positive integer, $U_n = \{1 + \mathrm{p}u : u \in G_{\mathrm{p}^{n-1}}\}$ be the subgroup of $G^*_{\mathrm{p}^n}$. Then for any character chi of the group $G^*_{\mathrm{p}^n}$ there exists a polynomial f(n) with coefficients from G*

$$f(u) = u + a_2u^2 + \cdots + a_{N-1}\mathrm{p}^{N-1}, N = n + \left[\frac{n}{\mathrm{p}+1}\right] + 1,$$

such that we have

$$\chi(1 + \mathrm{p}u) = e_{\mathrm{p}^{n-1}}, (Re(\Lambda f(u))),$$

where $\Lambda \in G^*_{\mathrm{p}^{n-1}}$ depends only on chi, and the coefficients satisfy the inequalities

$$\nu_\mathrm{p}(a_k) \geqslant k - \nu_\mathrm{p}(k) - 1, \quad k = 2, 3, \ldots, N - 1.$$

Proof. It is well-known that the multiplicative group G^*_p is a cyclic group. We may select a generator g of G^*_p in such a way that $g^{\mathrm{p}^2-1} = 1 + \mathrm{p}u_1, u_1 \in G^*_\mathrm{p}$. Then, using the continuation of p-adic valuation for Q to $Q(i)$, and stating one-to-one correspondence between $(1 + \mathrm{p}u_1)^k$ and

$$1 + k\mathrm{p}u_1 + \mathrm{p}^2u_1^2\frac{k(k-1)}{2} + \mathrm{p}^{n+n_0}u_1^{n+n_0}\frac{k(k-1)\ldots(k-n_0-1)}{n_0!} := 1 + \mathrm{p}u_k$$

for any $k \in G_{\mathrm{p}^{n-1}}$, where $n_0 = \left[\frac{n}{\mathrm{p}-1}\right] + 1$, we conclude that the multiplicative group U_n and additive group $G_{\mathrm{p}^{n-1}}$ are isomorphic (see [1] Ch. IV, 3.2, p. 375-376). Let k_0 be such that $(1 + \mathrm{p}u)^{k_0} \equiv 1 + \mathrm{p} \pmod{\mathrm{p}^n}$. Then $g_0 = g^{k_0}$ is also a generatic element of G^*_p.

Denote

$$f(u) = u - \mathrm{p}\frac{u^2}{2} + \mathrm{p}^2\frac{u^3}{3} - \cdots \pmod{\mathrm{p}^{n-1}}.$$

Consequently

$$f(u) \equiv u + a_2u^2 + \cdots + a_{N-1}u^{N-1} \pmod{\mathrm{p}^{n-1}},$$

where $N = n + \left[\frac{n}{\mathrm{p}-1}\right] + 1, a_k \equiv (-1)^{k+1}\frac{\mathrm{p}^{k-1}}{k} \pmod{\mathrm{p}^{n-1}}, \quad k = 2, 3, \ldots, N - 1.$

Define Λ from the congruence

$$\Lambda f(1) \equiv k_0 \pmod{\mathrm{p}^{n-1}}.$$

It is clear that $\Lambda \in G^*_{\mathrm{p}^{n-1}}$.

Therefore we deduce that the transformation $G_{\mathrm{p}^{n-1}} \to \mathbb{C}$ given by

$$1 + \mathrm{p}u \to e_{\mathrm{p}^{n-1}}(Re(\Lambda u)), \Lambda \in G^*_{\mathrm{p}^{n-1}}$$

defines a character of the group U_n.

Remark. *Lemma 4 was proved in [6] but here we give more detailed proof.*

Corollary 2. *Let* $q = \mathrm{p}^m, \mathrm{p} \equiv 3 \pmod 4$ *and* χ *by a non-trivial character of* $G^*_{\mathrm{p}^m}$ *of order* $d > 1$*. Suppose* $F(x) \in G_{\mathrm{p}^m}[x]$ *of a degree* n*. Then we have*

$$\left| \sum_{x \in G_{\mathrm{p}^m}} \chi(F(x)) \right| \leqslant 2^{\frac{m}{2}}(n-1)\mathrm{p}^m. \tag{7}$$

Proof. For $m = 1$ the assertion of Corollary follows from Lemma 3.

Let $m > 1$. Using the representation $x = x_0(1 + \mathrm{p}x_1), x_0 \in G^*_{\mathrm{p}}, x_1 \in G_{\mathrm{p}^{m-1}}$ for $x \in G_{\mathrm{p}^m}$ and also Lemmas 2 and 4 we successively go into a case $m = 1, q = \mathrm{p}$ so that Lemma 3 gives the assertion of Corollary 2.

Main Results. Description of elements E_m (see L. 1 for $m \geqslant 2$) and Lemmas 2 and 3 allow us to obtain Lemma 3 results and Corollary 2 for the character sums on nor subgroup E_m for the linear-inverse functions $\alpha x + \beta x^{-1}, \alpha, \beta$ are fixed from G_{p^m}.

Let χ be a non-trivial character of $G^*_{\mathrm{p}^m}$. Consider the sum

$$S_\chi(\alpha; \beta; E_m) = \sum_{x \in E_m} \chi(\alpha x + \beta x^{-1}), \quad \alpha, \beta \in G_{\mathrm{p}^m}. \tag{8}$$

This sum we will call character sum analogue of Kloosterman sum over a norm group.

Theorem 1. *Under conditions above we have next estimation*

$$|S_\chi(\alpha; \beta; E_m)| = \left| \sum_k \chi(\omega_0(k)) \sum_{t=0}^{\mathrm{p}^{m-1}-1} e_{\mathrm{p}^{m-1}}(C_0(k) + C_1(k)t + C_2(k)t^2 + \dots) \right| \leqslant c \cdot \mathrm{p}^{\frac{m}{2}}$$

with the absolute constant c*.*

Proof. The case $m = 1$ was studied by Li [2].

Let $m > 1$. By the representation (3) we can write

$$\chi(\omega) = \chi(\omega_0)\chi(1 + \mathrm{p}\omega_1)$$

where

$$\begin{aligned} &\omega_0 = A_0(k) + iB_0(k), (\omega_0, \mathrm{p}) = 1, \\ &\omega_1 = \omega_0^{-1} \left((A'_1(k) + iB'_1(k))\, t + \mathrm{p} \sum_{j=2}^{m-1} \left(A'_j(k) + iB'_j(k)\right) t^j \right), \end{aligned} \tag{9}$$

moreover,

$$\begin{aligned} &(A'_1(k)B'_1(k), \mathrm{p}) = 1, \quad (B'_2(k), \mathrm{p}) = 1, \\ &A'_j(k) = \tfrac{1}{\mathrm{p}} A_j(k), \quad B'_j(k) = \tfrac{1}{\mathrm{p}} B_j(k) \end{aligned}$$

if $k \neq 0, \mathrm{p}+1$, and

$$\begin{aligned} &\left(\tfrac{1}{\mathrm{p}} A'_1(k), \mathrm{p}\right) = (B'_1(k), \mathrm{p}) = 1, \\ &A'_j(k) \equiv B'_j(k) \equiv 0 \pmod{\mathrm{p}^2} \end{aligned}$$

if $k = 0$ or $\mathrm{p} + 1$.

Without restricting the generality we will suppose that $\alpha, \beta \in \mathbb{Z}_{p^m}$, i.e. $\alpha = a, \beta = b$. Then a straightforward computation gives

$$\chi(1 + p\omega_1) = e_{p^{m-1}} \left(C_0(k) + C_1(k)t + C_2(k)t^2 + C_3(k)t^3 + \dots\right),$$

where $C_2(k) \equiv 0 \pmod{p}, C_j(k) \equiv 0 \pmod{p^3}, j \geqslant 3,$ and $\nu_p(C_2(k)) > \nu_p(C_1(k))$ for all $k = 0, 1, \dots, p$ unless $O(1)$ values of k when $\nu_p(C_1(k)) \geqslant \nu_p(C_2(k)) = 1$.

Thus by application of Lemma 2 we obtain

$$|S_\chi(\alpha; \beta; E_m)| = \\ = \left| \sum_k \chi(\omega_0(k)) \sum_{t=0}^{p^{m-1}-1} e_{p^{m-1}}(C_0(k) + C_1(k)t + C_2(k)t^2 + \dots) \right| \leqslant c p^{\frac{m}{2}} \qquad (10)$$

with the absolute constant c. This completes our proof of Theorem 1.

In 2001 Ping Xi [3] studied the sum

$$K(\chi, q) = \sum_{m,n \in \mathbb{Z}_q} |S_\chi(m, n; q)|^2$$

and proved the following statement:

Let q be a positive integer, $q = \prod_{j=1}^{l} p_j^{a_j}$ and χ be character $mod q$, $\chi = \prod_{j=1}^{l} \chi_j$, χ is character $mod p_j^{a_j}$, and also $\chi_j(-1) = 1, j = 1, \dots, l$. Then for $8 \nmid q$ the inequality

$$q\varphi^2(q) \leqslant K(\chi, q) \leqslant 2^l q \varphi^2(q)$$

holds.

We will consider an analogue of $K(\chi, q)$ for character sum over $E(q)$ with a non-trivial character χ, where

$$E(q) := \{\omega \in G_q : N(\omega) \equiv 1 \pmod{q}\}.$$

More exactly, we will consider only case $q = p^m, p \equiv 3 \pmod 4$, since a general case may be study by analogy.

Theorem 2. *Let χ be an even non-trivial multiplicative character of $G^*_{p^m}$ (i. e. $\chi(-1) = 1$). Then the following equality*

$$K(\chi, p^m) = 2(p + 1)(p^2 - 1)p^{4m-2}$$

holds

Proof. We have

$$S_\chi(\alpha, \beta; E_m) = \sum_{x \in E_m} \chi(\alpha x + \beta x^{-1}) = \sum_{\gamma \in G^*_{p^m}} \chi(\gamma) \sum_{\substack{x \in E_m \\ \alpha x + \beta x^{-1} \equiv \gamma \pmod{p^m}}} 1$$

Hence,

$$K(\chi, E_m) = \sum_{\alpha, \beta \in G_{p^m}} |S_\chi(\alpha, \beta; E_m)|^2 = \sum_{\gamma_1, \gamma_2 \in G^*_{p^m}} \chi(\gamma_1)\bar{\chi}(\gamma_2) \sum_{S(C)} 1, \qquad (11)$$

where

$$C : \left\{x, y \in E_m, \alpha, \beta \in G^*_{\mathrm{p}^m} : \alpha x + \beta x^{-1} \equiv \gamma_1, \alpha y + \beta y^{-1} \equiv \gamma_2 \pmod{\mathrm{p}^m}\right\}.$$

First, let $m = 1$. The system of the congruences (in α, β) modulo p^m

$$\begin{cases} \alpha x + \beta x^{-1} \equiv \gamma_1 \\ \alpha y + \beta y^{-1} \equiv \gamma_2 \end{cases}$$

is a solvable system if $(x^2 - y^2) \mid (x\gamma_1 - y\gamma_2)$. With this provision system under consideration has exactly

$$N(gcd(x^2 - y^2, \mathrm{p})) = \begin{cases} 1 & \text{if } x^2 \not\equiv y^2 \pmod{\mathrm{p}}, \\ N(\mathrm{p}) & \text{if } x^2 \equiv y^2 \pmod{\mathrm{p}}, \end{cases}$$

solutions.

Thus we infer

$$K(\chi, E_1) = \sum_{\delta \mid \mathrm{p}} N(\delta) \sum_{\gamma_1, \gamma_2 \in G^*_{\mathrm{p}}} \chi(\gamma_1)\bar{\chi}(\gamma_2) \sum_{S(C)} 1, \tag{12}$$

where

$$C : \left\{ \begin{array}{l} x, y \in E_1 : x^2 \equiv y^2 \pmod{\delta}, x\gamma_1 \equiv y\gamma_2 \pmod{\delta}, \\ gcd\left(\frac{x^2 - y^2}{\delta}, \frac{\hat{\mathrm{p}}}{\delta}\right) = 1 \end{array} \right\}.$$

Now, if $\delta = 1$ then $\sum\limits_{S(C)} 1 = |E_1|^2$. Consequently, the contribution of a summand with $\delta = 1$ is equal

$$|E_1|^2 \sum_{\gamma_1, \gamma_2 \in G^*_{\mathrm{p}}} \chi(\gamma_1)\bar{\chi}(\gamma_2) = 0.$$

Further, for $\delta = \mathrm{p}$ we obtain the contribution

$$N(\mathrm{p}) \sum_{\gamma_1, \gamma_2 \in G^*_{\mathrm{p}}} \chi(\gamma_1)\bar{\chi}(\gamma_2) \sum_{S(C)} 1 = 2\,|E_1|\, N(\mathrm{p})\tilde{\varphi}(\mathrm{p}) = 2(\mathrm{p}+1)\mathrm{p}^2(\mathrm{p}^2 - 1)$$

where

$$C : \left\{ \begin{array}{l} x, y, \in E_1 : x\gamma_1 \equiv y\gamma_2, x^2 \equiv y^2 \pmod{\mathrm{p}}, \\ gcd\left(\frac{x^2 - y^2}{\mathrm{p}}, \frac{\bar{\mathrm{p}}}{\mathrm{p}}\right) = 1 \end{array} \right.,$$

$\tilde{\varphi}(\gamma)$ denote the Euler's totient function in G.

So,

$$K(\chi, E_1) = 2(\mathrm{p}+1)\mathrm{p}^2(\mathrm{p}^2 - 1). \tag{13}$$

Let $m > 1$. By an analogue with relation (12) we have

$$K(\chi, E_m) = \sum_{\nu=0}^{m} N(\mathrm{p}^\nu) \sum_{\gamma_1, \gamma_2 \in G^*_{\mathrm{p}^m}} \chi(\gamma_1)\bar{\chi}(\gamma_2) \sum_{S(C)} 1$$

where

$$C : \left\{ x, y \in E_m, \alpha, \beta \in G_m : \begin{array}{l} \alpha x + \beta x^{-1} \equiv \gamma_1 \\ \alpha y + \beta y^{-1} \equiv \gamma_2 \end{array} \pmod{\mathrm{p}^m} \right\}.$$

So we have

$$K(\chi, E_m) = \sum_{\nu=0} + \sum_{\nu=1}^{m-1} + \sum_{\nu=m} := \sum_0 + \sum_1 + \sum_2 .$$

Now,

$$\begin{aligned} \sum\nolimits_0 &= \sum_{\gamma_1,\gamma_2\in G^*_{\mathrm{p}^m}} \chi(\gamma_1)\bar{\chi}(\gamma_2)(\mathrm{p}^2-1)^2\,|E_m|^2 = 0; \\ \sum\nolimits_1 &= \sum_{\nu=1}^{m-1} N(\mathrm{p}^\nu) \sum_{\gamma_1,\gamma_2\in G^*_{\mathrm{p}^m}} \chi(\gamma_1)\bar{\chi}(\gamma_2)\left(\sum_{S(C_1')} 1 + \sum_{S(C_2')} 1\right), \end{aligned} \tag{14}$$

where

$$\begin{aligned} &C_1' : \{x, y \in E_m, x \equiv \gamma_2, y \equiv \gamma_1, x \equiv y \ (\mathrm{mod}\ \mathrm{p}^\nu)\}, \\ &C_2' : \{x, y \in E_m, x \equiv \gamma_2, y \equiv -\gamma_1, x \equiv -y \ (\mathrm{mod}\ \mathrm{p}^\nu)\}. \end{aligned}$$

Hence,

$$\sum\nolimits_1 = \sum_{\nu=1}^{m-1} N(\mathrm{p}^\nu)\left\{ \sum_{\substack{\gamma_1,\gamma_2\in G^*_{\mathrm{p}^m} \\ \gamma_1\equiv\gamma_2(\mathrm{p}^m)}} \chi(\gamma_1)\bar{\chi}(\gamma_2)N(\mathrm{p}^{m-\nu}) + \sum_{\substack{\gamma_1,\gamma_2\in G^*_{\mathrm{p}^m} \\ \gamma_1\equiv-\gamma_2(\mathrm{p}^m)}} \chi(\gamma_1)\bar{\chi}(\gamma_2)N(\mathrm{p}^{m-\nu}) \right\} =$$

$$\begin{aligned} &= 2N(\mathrm{p}^m) \sum_{\nu=1}^{m-1} \sum_{\gamma_1\in G^*_{\mathrm{p}^\nu}} \chi(\gamma_1) \sum_{\delta\in G_{\mathrm{p}^{m-\nu}}} \chi(1+\mathrm{p}^\nu\delta) = \\ &= 2N(\mathrm{p}^m) \sum_{\nu=1}^{m-1} \sum_{\delta\in G_{\mathrm{p}^{m-\nu}}} \chi(1+\mathrm{p}^\nu\delta) \sum_{\gamma_1\in G_{\mathrm{p}^\nu}} \chi(\gamma_1) = 0, \end{aligned} \tag{15}$$

$$\begin{aligned} \sum\nolimits_2 &= N(\mathrm{p}^m) \sum_{\substack{\gamma_1,\gamma_2\in G^*_{\mathrm{p}^m} \\ \gamma_1\equiv\gamma_i 2(\mathrm{p}^m)}} \chi(\gamma_1)\bar{\chi}(\gamma_2) \sum_{\substack{\alpha\equiv\pm\beta(\mathrm{p}^m) \\ \alpha,\beta\in E_m}} 1 = N(\mathrm{p}^m)\tilde{\varphi}(\mathrm{p}^m)\,|E_m| = \\ &= 2\mathrm{p}^{4m-2}(\mathrm{p}^2-1)(\mathrm{p}+1). \end{aligned} \tag{16}$$

As a consequently (14)-(16) we have

$$K(\chi, \mathrm{p}^m) = 2(\mathrm{p}+1)(\mathrm{p}^2-1)\mathrm{p}^{4m-2}. \tag{17}$$

The result of Theorem 2 shows that the upper bound for individual sum $S(\alpha, \beta; \chi)$ is optimal bound in certain sense.

By the similar method may be investigated close sum

$$K_E(\alpha, \beta; \chi) := \sum_{\alpha,\beta\in E_m} |S(\alpha, \beta; \chi)|^2 .$$

Conclusion. We obtain a non-trivial estimation of exponential sums and character sums which are analogue of Kloosterman sums over norm group in the ring of Guassian integers. Described proof method can be used for estimation of sums in close forms.

1. **Borevich Z.** Number Theory / Z. Borevich, I. Shafarevic. – London: Academic Press., Inc., 1966. – 436 p.
2. **Li W.-C. W.** Character sums over norm group / W.-C. W. Li // Finite fields and their Application. – 2006. – Vol. 12. – P. 1–15.
3. **Ping Xi** Mean values of character sums analogue of Kloosterman sums / Ping Xi, Yuan Yi // Proc. Amer. Math. Soc. – 2013. – Vol. 141. – P. 1233–1240.
4. **Schmidt W. M.** Equations over finite fields. An elementary approach / W. M. Schmidt // Lecture Notes in Math, Springer Verlag. – 1976. – Vol. 536. – 272 p.
5. **Sergeev S.** Twisted Kloosterman sum over norm group / Sergeev S. // International Journal of Applied Mathematics. – 2014. – Vol. 27, to appear.
6. **Varbanets P.** Generalized twisted exponential sum / P. Varbanets, S. Varbanets // Siauliai Math. Semin. – 2013. – Vol. 8(16). – P. 267–279.
7. **Weil A.** On some exponential sums / A. Weil // Proc. Nat. Acad. Sci. USA. – 1948. – Vol. 34. – P. 204–207.