ISSN 2304-1579. Visnyk Odesk. Nats. Univers. Mat. i Mekh.–2014 .–V.19,Is.3(23).–P.40–47

Mathematical Subject Classification: 11L05
UDC 511

L. V. Balyas
Odesa I. I. Mechnikov National University

EXPONENTIAL SUMS WITH THE BINOMIAL IN THE EXPONENT OVER THE RING OF GAUSSIAN INTEGERS

Баляс Л. В. Тригонометричні суми із двочленом у показнику над кільцем цілих гаусових чисел. У даній роботі нами були отримані нетривіальні оцінки для тригонометричних сум із многочленом виду $f(x) = ax^n + bx$ у показнику, де $(a, p) = (b, p) = (n, p) = 1, n \geqslant 2$, над кільцем цілих гаусових чисел.
Ключові слова: тригонометричні суми, кільце цілих гаусових чисел, неприміτивний характер.

Баляс Л. В. Тригонометрические суммы с двучленом в показателе над кольцом целых гауссовых чисел. В данной работе нами получены нетривиальные оценки для тригонометрических сумм с многочленом $f(x) = ax^n + bx$ в показателе, где $(a, p) = (b, p) = (n, p) = 1, n \geqslant 2$, над кольцом целых гауссовых чисел.
Ключевые слова: тригонометрические суммы, кольцо целых гауссовых чисел, непримитивный характер.

Balyas L. V. Exponential sums with the binomial in the exponent over the ring of Gaussian integers. In this work nontrivial estimates for the exponential sums with the polynomial $f(x) = ax^n + bx$ in the exponent, where $(a, p) = (b, p) = (n, p) = 1, n \geqslant 2$, over the ring of the gaussian integers were obtained.
Key words: exponential sums, the ring of the Gaussian integers, nonprimitive character.

Introduction. Exponential sums is an important tool for the solving of problems, connected with integers, and problems, which can not be solved with the use of other methods. Many questions of number theory are reduced to the application of the apparatus of exponential sums.

In the work of T. Cochrane [3] nontrivial estimates of exponential sums with the function $f(x) = ax^n + bx$ in the exponent were obtained. Using Weil's estimate [7] for the exponential sums with a polynomial in the exponent over the finite field, the author got the estimate of the following type

$$|S(ax^n + bx, \chi, p^m)| \leqslant np^{\frac{2}{3}}(b, p^m)^{\frac{1}{3}}. \tag{1}$$

In the paper we build the analogue of Cochrane's result for the exponential sums with the polynomial of the special form in the exponent over the ring of the Gaussian integers. Let G be the ring of the Gaussian integers and let $f(x) = ax^n + bx$ be a polynomial with integer coefficients. The aim of the paper is the investigation of exponential sums of the form

$$S(ax^n + bx, \chi, p^n) = \sum_{x \in G_{p^n}} \chi(x) e_{p^n}(ax^n + bx), \tag{2}$$

where χ is a nonprimitive character modulo p^n, p is a prime number and $p \equiv 3(mod\ 4), (a,p) = (b,p) = (n,p) = 1, n \geqslant 2$; and

$$S(ax^n + bx, \chi(N(x), p^n) = \sum_{x \in G_{p^n}} \chi(N(x)) e_{p^n}(ax^n + bx), \tag{3}$$

where χ is a nonprimitive character modulo p^n, p is a prime number and $p \equiv 1(mod\ 4), (a,p) = (b,p) = (n,p) = 1, n \geqslant 2$.

Notation. We will use the following notations:

- $G := \left\{a + bi | a, b \in \mathbb{Z}, i^2 = -1\right\}$;
- for $\alpha \in G$ we denote $N(\alpha) = |\alpha|^2, Sp(\alpha) = 2Re(\alpha)$;
- $gcd(a, b$ or (a, b) - the greatest common divisor of a and b;
- for $a \in \mathbb{Z}$ (or $\alpha \in G$) $\nu_p(a)$ (or $\nu_p(\alpha)$) stands that $p^{\nu_p(a)} | a, p^{\nu_p(a)+1}$ does not divide a;
- G_{p^n} (respectively, $G^*_{p^n}$ denotes the complete (respectively, reduced) system of residues modulo p^n in G;
- $e_{p^n}(t) = e^{2\pi Re(\frac{t}{p^n})}$;
- $\sum\limits_{(l)}$ (respectively, $\sum\limits_{(l)^*}$) means the summation over the complete (respectively, reduced) system of residues modulo l in G.

Auxiliary arguments. Before the studying of such kind of sums we present several lemmas, which will be used in the sequel.

Lemma 1. *Let $p \equiv 3(mod\ 4)$ be a prime, $n \in \mathbb{Z}^+$. Then there exists the polynomial $f(u)$ with coefficients from G*

$$f(u) = u + a_2 u^2 + \ldots + a_{N-1} p^{N-1}, \tag{4}$$

such that for any character χ of the group $U_n \subset G^*_{p^n}, U_n := \left\{1 + pu | u \in G_{p^{n-1}}\right\}$ we have

$$\chi(1 + pu) = e_{p^{n-1}}(\lambda f(u)), \tag{5}$$

where $\lambda \in G_{p^{n-1}}$ depends only on χ, and the coefficients a_l satisfy the inequalities

$$\nu_p(a_k) \geqslant k - \nu_p(k) - 1, k = 2, 3, \ldots$$

Proof. It is well known that the multiplicative group G^*_p is a cyclic group. We can select a generator g of group G^*_p in such way that

$$g^{p^2-1} = 1 + pu_1, (u_1, p) = 1.$$

Then using the continuation of p-adic valuation from $\mathbb{Q}$ to $\mathbb{Q}(i)$ and stating one-one correspondence between

$$(1+pu_1)^k := 1 + kpu_1 + p^2u_1^2\frac{k(k-1)}{2} + ... + p^{n+n_0}u_1^{n+n_0}\frac{k(k-1)\dots(k-n_0-1)}{n_0!}$$

and $1+pu_k$ for any $k \in G_{p^{n-1}}$, where $n_0 = \left[\frac{n}{p-1}\right]+1$, we conclude that multiplicative group U_n and the additive group $G_{p^{n-1}}$ are isomorphic (for the detales see [2]).

Since $u_k \equiv u_1k + pu_1^2\frac{k(k-1)}{2} + \dots (mod\ p^{n-1})$ we deduce that the transformation $G_{p^{n-1}} \to \mathbb{C}$ defined by

$$1 + pu \mapsto e_{p^{n-1}}(Re(\lambda u)), \lambda \in G_{p^{n-1}} \tag{6}$$

defines a character of the group U_n.

So we have proved the assertion of the lemma. ■

Lemma 2. *Let ρ be the Gaussian prime „ odd “ number ($\rho \neq 1+i$),$n \in \mathbb{Z}^+, \alpha_1, \dots, \alpha_k \in G, (\alpha_j, \rho) = 1, j = 2, 3, \dots; \nu_3, \dots, \nu_k \geqslant 2$. Then for*

$$S = \sum_{x \in G_{\rho^n}} e_{\rho^n}(\alpha_1 x + \alpha_2\rho x^2 + \alpha_3\rho^{\nu_3}x^3 + \dots + \alpha_k\rho^{\nu_k}x^k)$$

the estimate

$$|S| \leqslant \begin{cases} 0, & if \quad \alpha_1 \not\equiv 0(mod\ \rho); \\ N(\rho)^{\frac{n+1}{2}}, & if \quad \alpha_1 \equiv 0(mod\ \rho) \end{cases} \tag{7}$$

holds.

The following lemma can be used as a corollary to the previous lemma.

Lemma 3. *Let ρ be the Gaussian prime „ odd “, $n \in \mathbb{Z}^+$, and let $f(x)$ be a polynomial over G: $f(x) = A_1x + A_2x^2 + \dots$. And, moreover, let $\nu_\rho(A_2) = \alpha \geqslant 0, \nu_\rho(A_j) > \alpha, j = 3, 4, \dots$. Then for the sum*

$$S = \sum_{x \in G_{\rho^n}} e_{\rho^n}(f(x))$$

the estimate

$$|S| \leqslant \begin{cases} 0, & if \quad \nu_\rho(A_1) < \alpha; \\ 2^{\frac{n}{2}}N(\rho)^{\frac{n+\alpha}{2}}, & if \quad \alpha < n, \nu_\rho(A_1) \geqslant \alpha; \\ N(\rho^{n-1})(N(\rho)-1), & if \quad \alpha \geqslant n \end{cases} \tag{8}$$

holds.

The assertions of these lemmas are the consequences of the estimates of complete linear sum and Gauss sum, to which we can reduce the primary sums (for the proof see [6]).

Main Results. So, we get the next results.

Theorem 1. *Let $p \equiv 3(mod\ 4)$ be a prime, $a, b \in \mathbb{Z}, (a,p) = (b,p) = (n,p) = 1, n \in \mathbb{Z}^+, n \geqslant 2$, and let χ be a nonprimitive character modulo p^n. The for the sum*

$$S = S(ax^n + bx, \chi, p^n) = \sum_{x \in G_{p^n}} \chi(x) e_{p^n}(ax^n + bx)$$

the following estimate

$$|S| \leqslant \begin{cases} 0, & if \quad \nu_p(a_1) < \alpha \\ 2^{\frac{n-2}{2}}(n-1, p-1)N(p)^{\frac{n+\alpha}{2}}, & if \quad nu_p(a_1) \geqslant \alpha, \alpha < n-2 \end{cases} \tag{9}$$

holds.

Proof. Putting $x = u(1 + p^{n-1}v), v \in G_p, u \in G_{p^{n-1}}$, we obtain

$$ax^n + bx \equiv (au^n + bu) + p^{n-1}v(nau^n + bu)(mod\ p^n).$$

The application of Lemma 1 gives

$$S = \sum_{u \in G^*_{p^{n-1}}} \chi(u) e_{p^n}(au^n + bu) \sum_{v \in G_p} e_p(v(nau^n + bu + \lambda)),$$

where

$$\sum_{v \in G_p} e_p(v(nau^n + bu)) = \begin{cases} N(p), & if \quad nau^n + bu \equiv 0(mod\ p) \\ 0, & otherwise \end{cases}$$

and $\lambda \equiv 0(mod\ p)$ in view of a nonprimitivity of χ.

Hence we have

$$S = N(p) \sum_{S(C)} \chi(u) e_{p^n}(au^n + bu),$$

where $S(C) := \left\{ u \in G^*_{p^{n-1}} : nau^n + bu \equiv (mod\ p) \right\}$.

Let $C = u_1, u_2, \ldots, u_l$ be a set of the solutions of the congruence $nau^n + bu \equiv 0(mod\ p)$. Let u_j be an arbitrary solution of this congruence. We consider such $u \in G^*_{p^{n-1}}$, for which the condition $u \equiv u_j(mod\ p)$ holds.

Putting $u \equiv u_j(1 + pv), v \in G_{p^{n-2}}$ and using Lemma 1, we get

$$S = N(p) \sum_{j=1}^{l} \sum_{u_j \in G_p} \chi(u_j) e_{p^n}(au_j + bu_j) S_1,$$

where

$$S_1 = \sum_{v \in G_{p^{n-2}}} e_{p^{n-1}} \Bigg(v(nau_j^n + \lambda' n + bu_j) + \\ + pv^2 \left(\frac{n(n-1)}{2} \lambda' + \frac{n(n-1)}{2} au_j^n \right) + \ldots \Bigg).$$

Let us consider S_1. Because of the nonprimitivity of χ we have $\lambda^{'} \equiv 0(mod\ p)$. And that is why the congruence $nau_j^n + bu_j \equiv 0(mod\ p)$ holds. Therefore, the coefficient at v is divisible at least by p. Moreover, it is important to know the value of the function $\nu_p(y)$ at the point $y = \frac{n(n-1)}{2}$. We assume, that $\nu_p(n-1) = \alpha, \alpha \geqslant 0$ and

$$\nu_p\left(\frac{n(n-1)}{2}\lambda^{'} + \frac{n(n-1)}{2}au_j^n\right) = \alpha.$$

The application of Lemma 3 gives

$$|S_1| \leqslant \begin{cases} 0, & if \quad \nu_p(a_1) < \alpha; \\ \\ 2^{\frac{n-2}{2}} N(p)^{\frac{n-2+\alpha}{2}}, & if \quad \nu_p(a_1) \geqslant \alpha, \alpha < n-2. \end{cases} \tag{10}$$

It is obvious that the congruence $nau^n + bu \equiv 0(mod\ p)$ has at most $(n-1, p-1)$ solutions.

Taking into account that $N(p) = p^2$, we get the following estimate for the sum S

$$|S| \leqslant \begin{cases} 0, & if \quad \nu_p(a_1) < \alpha \\ \\ 2^{\frac{n-2}{2}}(n-1, p-1)p^{n+\alpha}, & if \quad \nu_p(a_1) \geqslant \alpha, \alpha < n-2, \end{cases} \tag{11}$$

which is the required result. ■

Theorem 2. *Let $p \equiv 1(mod\ 4), a, b \in \mathbb{Z}, n \in \mathbb{Z}^+, n \geqslant 2$ and let χ be a nonprimitive character modulo p^n. Then the following estimate*

$$\left|\sum_{x \in G_{p^n}} \chi(N(x)) e_{p^n} f(x)\right| \leqslant (n-1, p-1)^2 p^n,$$

where $f(x) = ax^n + bx$ is the polynomial with integer coefficients.

Proof. It is known that in the ring of Gaussian integers $p \equiv 1(mod\ 4)$ can be represented in the form $p = \rho \cdot \overline{\rho}$, where ρ and $\overline{\rho}$ are the complex conjugate Gaussian prime numbers. We denote $\overline{\rho} = c - di, \rho = c + di$ with $(c, p) = (d, p) = 1$.

Then the residue system [5] modulo p^n can be written as

$$x = g^{l_1}\overline{\rho}^n + g^{l_2}\rho^n, 0 \leqslant l_1, l_2 \leq (p-1)p^{n-1} - 1,$$

where g is a primitive root modulo p^n such that $g^{p-1} = 1 + pH, (H, p) = 1$.
Hence

$$N(x) = x \cdot \overline{x} = g^{2l_1}p^n + g^{2l_2}p^n + g^{l_1+l_2}\overline{\rho}^{2n} + g^{l_1+l_2}\rho^{2n} \equiv g^{l_1+l_2} Sp(\rho^{2n})(mod\ p^n).$$

Thus, the summands in our sum will be modified as follows

$$ax^n + bx \equiv (ag^{nl_1}\overline{\rho}^{n^2} + bg^{l_1}\overline{\rho}^n) + (ag^{nl_2}\rho^{n^2} + bg^{l_2}\rho^n)(mod\ p^n).$$

Then

$$S = \chi(Sp(\rho^{2n})) \sum_{(l_1)} \chi(g^{l_1}) e_{p^n}(ag^{nl_1}\overline{\rho}^{n^2} + bg^{l_1}\overline{\rho}^n) \sum_{(l_2)} \chi(g^{l_2}) e_{p^n}(ag^{nl_2}\rho^{n^2} + bg^{l_2}\rho^n).$$

We put $l_1 = (p-1)t_1 + z_1, l_2 = (p-1)t_2 + z_2$, where $t_i (mod\ p^{n-1})$ and $z_i = 0, 1, \ldots, p-2, i = \overline{1,2}$. Using this, one can get

$$g^{l_1} = g^{z_1}(1 + a_1 p t_1 + a_2 p^2 t_1^2 + a_3 p^{\lambda_3} t_1^3 + \ldots)(mod\ p^{n-1}) \tag{12.1}$$

with $a_1 = -H, a_2 \equiv -2H^2 (mod\ dp), \lambda_j \geqslant 3$.

$$g^{l_2} = g^{z_2}(1 + b_1 p t_2 + b_2 p^2 t_2^2 + a_3 p^{\mu_3} t_2^3 + \ldots)(mod\ p^{n-1}) \tag{12.2}$$

with $b_1 = -H, b_2 \equiv -2H^2 (mod\ p), \mu_j \geqslant 3$. Therefore

$$g^{nl_1} = g^{nz_1}(1 + a_1(n) p t_1 + a_2(n) p^2 t_1^2 + \ldots)(mod\ p^{n-1}), \tag{13.1}$$

where $a_1(n) = n a_1, a_2(n) = \left(n a_2 + \frac{n(n-1)}{2} a_1^2\right)$ and so on.

$$g^{nl_2} = g^{nz_2}(1 + b_1(n) p t_2 + b_2(n) p^2 t_2^2 + \ldots)(mod\ p^{n-1}), \tag{13.2}$$

where $b_1(n) = n b_1, b_2(n) = \left(n b_2 + \frac{n(n-1)}{2} b_1^2\right)$ and so on.

By (12.1), (12.2), (13.1), (13.2) we get

$$a g^{nl_1} \overline{\rho}^{n^2} + b g^{l_1} \overline{\rho}^n = (a g^{nz_1} \overline{\rho}^{n^2} + b g^{z_1} \overline{\rho}^n) + p t_1 (a_1(n) a \overline{\rho}^{n^2} g^{nz_1} + b \overline{\rho}^n g^{z_1} a_1) +$$

$$+ p^2 t_1^2 (a_2(n) a g^{nz_1} \overline{\rho}^{n^2} + a_2 b g^{z_1} \overline{\rho}^n) + \ldots = A_0 + A_1 p t_1 + A_2 p^2 t_1^2 + \ldots$$

In a similar way we have

$$a g^{nl_2} \rho^{n^2} + b g^{l_2} \rho^n = (a g^{nz_2} \rho^{n^2} + b g^{z_2} \rho^n) + p t_2 (b_1(n) a \rho^{n^2} g^{nz_2} + b \rho^n g^{z_2} b_1) +$$

$$+ p^2 t_2^2 (b_2(n) a g^{nz_2} \rho^{n^2} + b_2 b g^{z_2} \rho^n) + \ldots = B_0 + B_1 p t_2 + B_2 p^2 t_2^2 + \ldots$$

Then our sum takes on the form on the form

$$S = \chi(Sp(\rho^{2n})) S(z_1) S(t_1) S(z_2) S(t_2),$$

where

$$S(z_1) = \sum_{z_1=0}^{p-2} \chi(g^{z_1}) e_{p^n}(a g^{nz_1} \overline{\rho}^{n^2} + b g^{z_1} \overline{\rho}^n),$$

$$S(z_2) = \sum_{z_2=0}^{p-2} \chi(g^{z_2}) e_{p^n}(a g^{nz_2} \rho^{n^2} + b g^{z_2} \rho^n)$$

and

$$S(t_1) = \sum_{t_1 (mod\ p^{n-1})} \chi(1 + p(a_1 t_1 + a_2 p t_1^2 + \ldots)),$$

$$S(t_2) = \sum_{t_2 (mod\ p^{n-1})} \chi(1 + p(b_1 t_1 + b_2 p t_1^2 + \ldots)).$$

For the sums over $t_i (mod\ p^{n-1}), i = \overline{1,2}$ we will use the Postnikov's lemma about characters [4]

$$\chi(1 + p(a_1 t_1 + a_2 p t_1^2 + \ldots)) = e_{p^{n-1}}\left(p a_1^{'} t_1 + p^2 a_2^{'} t_1^2 + \ldots\right),$$

where $a_1^{'} = n\lambda a_1, a_2^{'} = \lambda\left(na_2 + \frac{n(n-1)}{2}a_1^2\right), a_j \equiv 0(mod\ p^3), j = 3, 4\ldots$ and $\lambda \equiv 0(mod\ p)$ in a view of a nonprimitivity of χ.

In a similar way we get

$$\chi(1 + p(b_1t_2 + b_2pt_2^2 + \ldots)) = e_{p^{n-1}}\left(pb_1^{'}t_1 + p^2b_2^{'}t_2^2 + \ldots\right),$$

where $b_1^{'} = n\lambda^{'}b_1, b_2^{'} = \lambda^{'}\left(nb_2 + \frac{n(n-1)}{2}b_1^2\right), b_j \equiv 0(mod\ p^3), j = 3, 4\ldots$ and $\lambda^{'} \equiv 0(mod\ p)$ in a view of a nonprimitivity of χ.

We will impose some restrictions on the coefficients at the first degree of t_1 and t_2.

Because of the dependence of the coefficients A_1 and B_1 on g^{nz_i} and g^{z_i} with $i = \overline{1,2}$, we have to know, for which $z_i, i = \overline{1,2}$, the congruences $A_1(z_1) \equiv 0(mod\ p)$ and $B_1(z_2) \equiv 0(mod\ p)$ hold. Let us consider $A_1(z_1)$

$$A_1(z_1) = na_1ag^{nz_1}\overline{\rho}^{n^2} + ba_1g^{z_1}\overline{\rho}^n = a_1\overline{\rho}^ng^{z_1}(na\overline{\rho}^{(n^2-n)}g^{z_1(n-1)} + b).$$

Taking into account, that $a_1 = -H$, where $(H, p) = 1$, we get $(a_1, p) = 1$. So we have to study the congruence

$$Re\left(na\overline{\rho}^{(n^2-n)}g^{z_1(n-1)} + b\right) \equiv 0(mod\ p), \tag{14}$$

which is equivalent to the congruence

$$nag_0^{(n-1)z_1}Re(\overline{\rho}^{(n^2-n)}) + b \equiv 0(mod\ p) \tag{15}$$

with $n, a, b \in \mathbb{Z}^+$ and g_0 is a primitive root in the ring of the rational integers modulo p.

The fact of the relative primality of $Re\overline{\rho} = c$ and p, $Im\overline{\rho} = d$ and p leads us in the investigation of (15) to the binomial congruence

$$A^m \equiv B(mod\ p), \tag{16}$$

which has at most $(n-1, p-1)$ solutions. The congruences (14), (15) and (16) are equivalent. So the congruence (14) has at most $(n-1, p-1)$ solutions.

In the same manner one can get the similar results for the congruence $B_1(z_2) \equiv 0(mod\ p)$.

Arranging in order the coefficients at the powers of t_1 and t_2 in the summands, we obtain

$$p^2(A_1^{'} + a_1^*)t_1 + p^2(A_2^{'} + a_2^*)t_1^2 + \ldots = C_1t_1 + C_2t_1^2 + \ldots$$

$$p^2(B_1^{'} + b_1^*)t_2 + p^2(B_2^{'} + b_2^*)t_2^2 + \ldots = D_1t_2 + D_2t_2^2 + \ldots$$

So, the original sum takes on the next form

$$S = \chi\left(Sp(\rho^{2n})\right) \times$$

$$\times S(z_1) \sum_{t_1 (mod\ p^{n-1})} (C_1 t_1 + C_2 t_1^2 + \ldots) \times$$

$$\times S(z_2) \sum_{t_2 (mod\ p^{n-1})} (D_1 t_2 + D_2 t_2^2 + \ldots)$$

$S(z_i)$ can be estimated in the following away

$$|S(z_i)| \leqslant (n-1, p-1), i = \overline{1,2},$$

where $(n-1, p-1)$ is the number of the solutions of the congruences $A_1(z_1) \equiv 0 (mod\ p)$ and $B_1(z_2) \equiv 0 (mod\ p)$.

The application of Lemma 2 gives the estimate

$$\left| \sum_{x \in G_{p^n}} \chi(N(x)) e_{p^n} f(x) \right| \leqslant (n-1, p-1)^2 p^n, \tag{17}$$

which proves the theorem. ■

Conclusion. The estimates from the theorems can be applied to the problem of the distribution of the solutions of the congruence $y^k \equiv \alpha x^n + \beta x (mod\ \gamma)$, where α, β, γ are the gaussian integers [1].

1. **Balyas L.** Twisted exponential sums over the ring of Gaussian integers / Balyas L., Varbanets P. // Annales Univ. Sci. Budapest, Sect. Comp. – 2013. – V.40. – P. 95–103.
2. **Borevich Z. I.** Number theory / Borevich Z. I., Shafarevich I. R. – London: Academic Press., 1966. – 439 p.
3. **Cochrane T.** Bound for certain exponential sums / Cochrane T., Zheng Z. // Asian Journal of Mathematics. – 2000. – V. 4(4). – P. 757–774.
4. **Postnikov A. G.** On sum of characters modulo of power prime / Postnikov A. G. // Izv. Akad. Nauk USSR, Ser. Math. – 1955. – V. 19(1). – P. 11–16.
5. **Varbanets S.** General Kloosterman sums over ring of gaussian integers / Varbanets S. // Ukr. Math. J. – 2007. – V. 59(9). – P. 1179–2000.
6. **Varbanets P.** On inversive congruential generator with a variable shift with prime power modulus / Varbanets P., Varbanets S. // Annales Univ. Sci. Budapest, Sect. Comp. – 2010. – V. 32. – P. 151–176.
7. **Weil A.** On the exponential sums / Weil A. // I. London Math Soc. (2). – 1948. – V. 3. – P. 204–207.