*Annales Univ. Sci. Budapest., Sect. Comp. 40 (2013) 95–103*

# TWISTED EXPONENTIAL SUMS OVER THE RING OF GAUSSIAN INTEGERS

**L. Balyas and P. Varbanets**

(Odessa, Ukraine)

*Dedicated to Professors Zoltán Daróczy and Imre Kátai on their 75th anniversary*

Communicated by Bui Minh Phong

(Received March 31, 2013; accepted May 10, 2013)

**Abstract.** A twisted exponential sum over a curve defined by $y^\ell \equiv f(x) \pmod{\mathfrak{p}^m}$ in the ring of Gaussian integers is investigated.

## 1. Introduction

Let $G$ be the ring of Gaussian integers and let $f(x)$ be a polynomial m-th degree from $G[x]$. Consider the congruence over $G$

$$y^\ell \equiv f(x) \pmod{\gamma}, \tag{1}$$

where $\ell \in \mathbb{Z}$, $\ell \geq 1$, $\gamma \in G$.

Denote through $C(\ell, f; \gamma)$ the set of all solutions of the congruence (1).

The purpose of our paper is the derivation of the estimate for the sums

$$S_l(f; \chi, \gamma) = \sum_{x,y \in C(\ell,f;\gamma)} \chi(f(x)) e^{\pi i Sp\left(\frac{\alpha x + \beta y}{\gamma}\right)}, \tag{2}$$

*Key words and phrases*: Twisted exponential sum, Gaussian integers, Dirichlet character.
*2010 Mathematics Subject Classification*: 11L07, 11L40.

where $\chi$ is an arbitrary character of the group $G_\gamma$, and $\alpha, \beta \in G$.

The exponential sums of a type of (2) over $\mathbb{Z}$ has been investigated by many authors ([2],[3], [4], [10]).

Bearing in mind that the right and left hand sides of the equation (2) are multiplicative at $q$, the problem of evaluation $S(f;\chi,\gamma)$ reduces to a consideration of the case of a prime power modulus $\gamma = \mathfrak{p}^n$, $\mathfrak{p}$ is a Gaussian prime number.

The estimate of the sum $S(f;\chi,\mathfrak{p}^m)$ will carried out in two steps.

First, we construct the parametric representation of the solutions of congruence (1) (for $\gamma = \mathfrak{p}^n$), and then, the estimate of $S(f;\chi,\mathfrak{p}^m)$ will be reduced to an estimate of a special exponential sum.

We will use the following **notations**:

- $G := \{a + bi | a, b \in \mathbb{Z}, i^2 = -1\}$;
- for $\alpha \in G$ we denote $N(\alpha) = |\alpha|^2$, $Sp(\alpha) = 2\Re(\alpha)$;
- $G_\gamma$ (respectively, $G_\gamma^*$) denotes the complete (respectively, reduced) system of residues modulo $\gamma$ in $G$;
- for $\alpha \in \mathbb{Q}(i)$, $\alpha = \mathfrak{p}^k \frac{\alpha_0}{\beta_0}$, $\alpha_0, \beta_0 \in G$, $(\alpha_0, \mathfrak{p}) = (\beta_0, \mathfrak{p}) = 1$ we denote $\nu_\mathfrak{p}(\alpha) = k$, $k \in \mathbb{Z}$.

## 2. Parametric representation of solutions

Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$, $a_j \in G_{\mathfrak{p}^n}$, $a_0 = 1$, $(a_n, \mathfrak{p}) = 1$, $\mathfrak{p}$ be a Gaussian prime integer.

For $\mathfrak{p} \in \mathbb{G}$ we have $N(\mathfrak{p}) = p$, where $p = 2$ or $p \equiv 1 \pmod 4$, and then $G_{\mathfrak{p}^n} \cong \mathbb{Z}_{p^n}$. Thus the investigation of the behavior of the sum $S(f,\chi;\mathfrak{p}^n)$ reduces to the consideration of the corresponding sum $S(f;\chi;\mathfrak{p}^n)$ reduces to the rational case. Hence, let further $\mathfrak{p} = p \equiv 3 \pmod 4$.

Now, for $n = 1$ the ring $G_p$ is a field $\mathbb{F}_{p^2}$, and the considered problem is a problem of an estimate of exponential sum over a finite field, which has been decided by A. Weil[9] (see, also E. Bombieri[1]).

We will assume that $n \geq 2$.

Let $(x_0, y_0)$ be an arbitrary solution of the congruence

$$y^\ell \equiv f(x) \pmod p. \tag{3}$$

First one we can conclude that $f(x_0) \not\equiv 0 \pmod p$. Then the congruence $f(x_0)z \equiv 1 \pmod{p^n}$ has the unique solution. Let us denote it as $z_0$. We will suppose that $0 \le x_0 \le p-1$, $1 \le z_0 \le p^n - 1$.

For every $t \in G_{p^{n-1}}$ we set $A(t) = f(x_0 + pt)$.

Assume that the congruence $y^\ell \equiv A(0) \pmod p$ has $k$, $k \ge 1$, solutions, and hence, the congruence

$$y^\ell \equiv A(t) \pmod{p^n} \tag{4}$$

also has $k$ solutions for every $t$.

Next, let us denote the solutions $y_1(t),\dots,y_k(t)$ for the congruence (4). In particularly, we have $k$ solutions $y_1(0),\dots,y_k(0)$. Let $y(0)$ be one of the solutions. From the definition of $z_0$ we conclude that the congruence (4) is an equivalent for

$$\begin{aligned} y^\ell \equiv f(x_0) \Bigg(1 + f'(x_0)ptz_0 + \frac{1}{2!}f''(x_0)p^2t^2z_0 + \cdots \\ \cdots + \frac{1}{m!}f^{(n)}(x_0)p^mt^mz_0\Bigg) \pmod{p^n}. \end{aligned} \tag{5}$$

Consider the function

$$F(\omega) = \left(1 + f'(x_0)z_0\omega + \frac{1}{2!}f''(x_0)z_0\omega^2 + \cdots + \frac{1}{m!}f^{(n)}(x_0)z_0\omega^m\right)^{\frac{1}{\ell}} \tag{6}$$

and let $\sum\limits_{j=0}^{\infty} X_j\omega^j$ be its formal expansion in Taylor's series. It is obvious that $X_j$ are functions in $x_0$, $z_0$ for $j = 0, 1, 2, \dots$.

Now we equate two expressions for logarithmic derivative of $F(\omega)$ and then equalize the coefficients at equal powers of $\omega$. We get the recurrence relation

$$\begin{aligned} \ell(j+1)X_{j+1} = f'(x_0)z_0(1-\ell j)X_j + f''(x_0)z_0\left(1 - \frac{\ell(j-1)}{2}\right)X_{j-1} + \\ + \frac{f'''(x_0)}{2!}z_0\left(1 - \frac{\ell(j-1)}{3}\right)X_{j-2} + \cdots \\ \cdots + \frac{f^{(m)}(x_0)}{(m-1)!}z_0\left(1 - \frac{\ell(j-m+1)}{m}\right)X_{j-m+1} \end{aligned} \tag{7}$$

By an induction we easily infer that $\ell(j+1)!X_{j+1}$ is Gaussian integer for every $j = 0, 1, 2, \dots$. Moreover, since $\nu_p(j!) \le \frac{j}{p-1}$, we conclude that

$$\nu_p(X_jp^j) \ge j - \frac{j}{p-1} - \nu_p(\ell). \tag{8}$$

Consider the polynomial $F_s(\omega) = \sum\limits_{j=0}^{s} X_j\omega^j$. For every $s = 1, 2, \ldots$, by the equation

(9)
$$F_s^\ell(\omega) - F^\ell(\omega) = (F_s(\omega) - F(\omega))\left(F_s^{\ell-1}(\omega) + F_s^{\ell-2}(\omega)F(\omega) + \cdots + F^{\ell-1}(\omega)\right),$$

we deduce that $F_s^\ell(\omega) - F^\ell(\omega)$ has an expansion in powers of $\omega$ and it does not contain $\omega^k$, $k = 0, 1, \ldots, s$.

Consequently, putting $X_j p^j = \overline{X}_j p^{\lambda_j}$, $\nu_p(\overline{X}_j) = 0$, we obtain that for the coefficients $b_j$ at $t^j$ of the polynomial $F_s^\ell(pt) - F^\ell(pt)$ the inequality $\nu_p(b_j) \geq \mu_j$, where $\mu_j \geq \min(\lambda_{j_1} + \lambda_{j_2}) \geq j\frac{p-2}{p-1}$, holds.

Thus, substituting the coefficients $b_j$ by Gaussian integers modulo $p^n$, we obtain that

$$F_s^\ell(pt) - F^\ell(pt) \equiv 0 \pmod{p^n} \text{ if } \left[(s+1)\frac{p-2}{p-1}\right] \geq n.$$

Denote $\Phi(x_0) \equiv \overline{X}_j \pmod{p^n}$, $\Phi(x_0) \in G^*_{p^n}$. So, we proved the following assertion

**Lemma 1.** *Let $(\ell, p) = 1$ and $s = \left[\frac{p-1}{p-2}n\right]$. There exists the polynomial $\varphi(t) \in \in G[t]$, $\deg\varphi(t) = s$,*

$$\varphi(t) = \Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0)t + p^{\lambda_2}\Phi_2(x_0)t^2 + \cdots p^{\lambda_s}\Phi_s(x_0)t^s, \tag{10}$$

*such that the solution of (5) that corresponds to $y(0)$ is determined by the congruence*

$$y(t) \equiv y(0)\varphi(t) \pmod{p^n},\ t \in G_{p^{n-1}}.$$

*Moveover, $\Phi_0(x_0) = 1$, $\lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_j \leq j\frac{p-2}{p-1}$, $j \geq 3$.*

**Corollary 1.** *Let $y_1(0), \ldots, y_k(0)$ be all the solutions of congruence $y^\ell \equiv f(x_0) \pmod{p^n}$, $(f(x_0), p) = 1$. Then all solutions of the congruence*

$$y^\ell \equiv f(x) \pmod{p^n} \tag{11}$$

*under condition $x \equiv x_0 \pmod{p}$, $y \equiv y_i(0) \pmod{p}$, $i = 1, \ldots, k$, have the representation*

$$x \equiv x_0 + pt,\ y = y_i(0)\varphi(t) \pmod{p^n},\ t \in G_{p^{n-1}}.$$

L.P. Postnikova[6] (see, also [8]) obtained an analogous assertion for the congruence $x^2 + y^2 \equiv \ell \pmod{p^n}$ over $\mathbb{Z}_{p^n}$.

Now let $f(x_0) \equiv 0 \pmod{p^n}$. Then we have $y_0 \equiv 0 \pmod{p}$. We will describe the solutions of the congruence (11) with the condition $y \equiv 0 \pmod{p}$.

Let us put $y = p^r y_1$, $r \geq 1$, $y_1 \in G^*_{p^{n-r}}$.

For $r\ell \geq n$ we have $f(x) \equiv 0 \pmod{p^n}$. Let $x_1,\ldots,x_n$ be all the solutions of the congruence $f(x) \equiv 0 \pmod{p^n}$ over $G_{p^n}$. Then the pairs $(x_j, p^{n_0}y)$, $n_0 = \left[\frac{n}{\ell}\right] + 1$, $y \in G_{p^{n-n_0}}$, $j = 1,\ldots,k$, generate all the solutions of the congruence (11) with the condition $y^\ell \equiv 0 \pmod{p^n}$, $f(x) \equiv 0 \pmod{p^n}$.

For $y = p^r y_1$, $y_1 \in G^*_{p^{n-r}}$, $r < n_0$, $x = x_0 + p^{r\ell}x_1$, $x_0 \in G_{p^{r\ell}}$, $x_1 \in G_{p^{n-r\ell}}$ the corresponding value $x$ finds from the solutions of the system of congruences

$$(12) \qquad \begin{cases} f(x_0) \equiv 0 \pmod{p^{r\ell}} \\ y_1 \equiv \dfrac{f(x_0)}{p^{r\ell}} + f'(x_0)x_1 + \dfrac{f'(x_0)}{2!}p^{r\ell}x_1^2 + \cdots \\ \qquad\qquad \cdots + \dfrac{f^{(m)}(x_0)}{m!}p^{(m-1)r\ell} \pmod{p^{n-r\ell}-1} \end{cases}$$

relatively $y_1 \in G^*_{p^{n-r}}$, $x_0 \in G_{p^{r\ell}}$, $x_1 \in G_{p^{n-r\ell}}$.

The description of the solutions of the system (12) may be obtained from Corollary.

We are now in a position to investigate the sum $S_\ell(f, \chi, p^n)$.

## 3. Estimation of the twisted exponential sum $S_\ell(f, \chi, p^m)$

In order to investigate a twisted exponential sum we give the following preliminary lemma

**Lemma 2.** *Let $p \equiv 3 \pmod 4$ be a prime, $n \geq 3$ be a positive integer. There exists the polynomial $f(u)$ with coefficients from $G$*

$$(13) \qquad f(u) = u + a_2u^2 + \cdots + a_{N-1}p^{N-1},$$

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

$$(14) \qquad \chi(1+pu) = e_{p^{n-1}}(\Lambda f(u)),$$

*where $\Lambda \in G_{p^{n-1}}$ depends only on $\chi$, and the coefficients $a_\ell$ satisfy by the inequalities*

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

**Proof.** Well-known that the multiplicative group $G^*_p$ is a cyclic group. We may select a generator $g$ of $G^*_p$ 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

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

and

$$1+pu_k,\ \textit{for any } k\in G_{p^{n-1}},$$

where $n_0=\left[\frac{n}{p-1}\right]+1$,
we conclude that the multiplicative group $U_n$ and the additive group $G_{p^{n-1}}$ are isomorphic (for a detail, see [7], pp. 375-376).

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

$$1+pu\to e_{p^{n-1}}(\Re(\Lambda u)),\ \Lambda\in G_{p^{n-1}} \tag{15}$$

defines a character of the group $U_n$. ■

From the definition of $S_\ell(f,\chi,p^m)$ it follows that we can concede $f(x)\not\equiv 0 \pmod p$, i.e. we will consider only such $(x,y)\in C(\ell,f,p^m)$ for which $(y,p)=$ $=(f(x),p)=1$.

Let $x_0$ run over all such elements from $G_p$ for which

$$S(f,\chi,p^n)=\sum_{x_0}\sum_{y(0)}\chi(y(0))e_{p^n}(\alpha x_0+\beta y(0))\sum_t e_{p^{n-1}}(\Re(B(t))), \tag{16}$$

where

$$\begin{aligned} B(t)&=(\alpha+\lambda\Phi_1+\beta y(0)\Phi_1)t+p(\lambda\Phi_2+\lambda\overline{g}_2\Phi_1^2+\beta y(0)\Phi_2)t^2+\\ &+p^2(\lambda\Phi_3+2\lambda\Phi_1\Phi_2+\lambda\overline{g}_3\Phi_1^3+\beta y(0)\Phi_3)t^3+\cdots=\\ &=B_0+B_1t+B_2t^2+\cdots. \end{aligned} \tag{17}$$

The coefficients $B_j$ of the polynomial $B(t)$ are Gaussian integers. Moreover, denoting $B_j=p^{\mu_j}\overline{B}_j$, $(\overline{B}_j,p)=1$, we have: $2\le\mu_3\le\mu_4\le\cdots$.

For an estimate of $S(f,\chi,p^n)$ we can use the following well-known lemma.

**Lemma 3.** *Let $\mathfrak{p}$ be the Gaussian prime "odd" number, $m$ be a positive integer, $\alpha_1\ldots,\alpha_k\in G$, $(\alpha_j,\mathfrak{p})=1$, $j=2,3,\ldots$; $\nu_3,\ldots,\nu_k\ge 2$. Then*

$$\left|\sum_{x\in G_{p^m}}\exp\left(2\pi i\Re\left(\frac{\alpha_1x+\alpha_2\mathfrak{p}x^2+\alpha_2\mathfrak{p}^{\nu_3}x^3+\cdots+\alpha_k\mathfrak{p}^{\nu_k}x^k}{\mathfrak{p}^m}\right)\right)\right|=$$
$$=\begin{cases}0 & if\quad \alpha_1\not\equiv 0 \pmod{\mathfrak{p}},\\ N(\mathfrak{p})^{\frac{m+1}{2}} & if\quad \alpha_1\equiv 0 \pmod{\mathfrak{p}}.\end{cases}$$

In particular, we have

**Theorem 1.** *Let $\alpha, \beta, \gamma \in G_{p^n}$ and let us assume that for all pairs $(x_0, y(0))$, $x_0 \in C_0$, $y(0) = D(x_0)$ we have $2(\lambda + \beta y(0))\Phi_2(x_0) \not\equiv \lambda\Phi_1^2(x_0) \pmod p$. Then*

$$S(f, \chi, p^n) = \begin{cases} N(p^n)^{\frac{1}{2}} & if \quad \alpha + (\lambda + \beta y(0))\Phi_1(x_0) \equiv 0 \pmod p, \\ 0 & otherwise. \end{cases}$$

Consider the congruence

$$y^4 \equiv a + bx^3 \pmod{p^n},\ (b, p) = 1,\ p > 2, \tag{18}$$

Let $k(x_0)$ be the number of solutions of the congruence

$$y^4 \equiv a + bx_0^3 \pmod{p^n},\ (a + bx_0^3, p) = 1.$$

We have

$$\Phi(x_0) = 1,$$
$$\Phi_1(x_0) = 3 \cdot 4^{-1} b x_0^2 (a + bx_0^3)^{-1},$$
$$\Phi_2(x_0) = 3(32)^{-1} b x_0^2 (a + bx_0^3)^{-1}(8(a + bx_0^3) + bx_0^2).$$

From (17) it can be seen that the congruences $B_1 \equiv 0$, $B_2 \equiv 0 \pmod p$ are leading to the congruence $\lambda\Phi_1^3(x_0) \equiv 2\alpha\Phi_2(x_0)$. If the last congruence disturbs for all $x_0 \in C_0$ and $y(0) \in D(x_0)$, we obtain by Lemma 3

$$|S(f, \chi, p^n)| \le \sum_{x_0 \in C_0} |D(x_0)| \cdot p^n = \sum_{x_0 \in C_0} |D(x_0)| \cdot N(p^n)^{\frac{1}{2}}.$$

So we must consider four cases:

a) $(x_0, p) = (a + bx_0^3, p) = 1$

b) $(x_0, p) = 1$, $a + bx_0^3 \equiv 0 \pmod p$

c) $x_0 \equiv 0 \pmod p$, $a + bx_0^3 \not\equiv 0 \pmod p$

d) $x_0 \equiv 0 \pmod p$m $a + bx_0^3 \equiv 0 \pmod p$

For a principal character $\chi$ and the case a) we have $|C_0| \le 3$, $|D(x_0)| \le 4$ (if $x_0 \in C_0$) (here, $|V|$ means the cardinality of $V$). Hence,

$$\left| \sum_{\substack{x_0 \in C_0 \\ (a + bx_0^3, p)}} \sum_{y(0) \in D(x_0)} \sum_t \chi(y(0)\varphi(t)) e_{p^n}(\alpha(x_0 + pt) + \beta y(0)\varphi(t)) \right| \le 12p^n.$$

Similar estimate can be done in the case c).

The contribution in the estimate of $S(f,\chi,p^n)$ for the cases b) and d) are the same.

Hence, we proved the theorem

**Theorem 2.** *Let $p \equiv 3 \pmod 4$ be a prime number. Then*

$$\left| \sum_{\substack{x,y \in G_{p^n}^2 \\ y^4 \equiv a+bx^3 \pmod{p^n}}} \chi_0(y) e_{p^n}(\alpha x + \beta y) \right| \ll N(p^n)^{\frac{1}{2}}$$

*with an absolute constant in symbol "$\ll$".*

The description of solutions of the congruence

$$y^\ell \equiv f(x) \pmod{p^n}$$

can be applied for investigation of the distribution of solutions in $G^2$ of the congruences of type considered above.

Authors are grateful to referee for a careful reading of our paper and his suggestions which improved its quality.

## References

[1] **Bombieri, E.,** On exponential sums in finite fields, *Amer. J. Math.*, **88** (1966), 71–105.

[2] **Cochrane, T.,** *Exponential Sums and the Distribution of Solutions of Congruences*, Institute of Math., Academia Sinica, Taipei, Taiwan, 1994.

[3] **Mordell, L.J.,** A finite evaluation of a special exponential sum, *Proc. Cambribge Philos. Soc.*, **71** (1972), 75–78.

[4] **Perelmuter, G.,** Estimate of sum over algebraic curve, *Mat. Zametki*, **5** (1969), 373–380 (in Russian).

[5] **Postnikov, A.G.,** On sum of characters modulo of prime power, *Izvestiya. Akad. Nauk USSR, Ser. Math.*, **19(1)** (1955), 11–16 (in Russian).

[6] **Postnikova, L.P.,** Distribution of the solutions of congruence $x^2+y^2 \equiv \ell \pmod{p^n}$, *Sb. Math.*, **65(2)** (1964), 228–238 (in Russian).

[7] **Shafarevich, I.R.,** *Number Theory*, Academic Press. Inc., London, 1966.
[8] **Varbanets, P.D.,** Problem of circle in arithmetic progression, *Mat. Zametki*, **8(6)** (1970), 787–798 (in Russian).
[9] **Weil, A.,** On some exponential sums, *Proc. Nat. Acad. Sci. U. S. A.*, **34** (1948), 204–207.
[10] **Williams, K.S.,** A class of character sums, *J. London Math. Soc.*, **(2)(3)** (1971), 67–72.

**L. Balyas and P. Varbanets**
I.I. Mechnikov Odessa National University
Odessa
Ukraine
balyas@ukr.net
varb@sana.od.ua