Researches in Mathematics and Mechanics. — 2020. — V. 25, Is. 2(36). — P. 26–39

UDC 511.32

P. Fugelo, S. Varbanets
State Agrarian and Engineering University in Podilia
Odessa I.I. Mechnikov National University

GENERATOR OF PRN'S ON THE NORM GROUP

Let p be a prime number, $d \in \mathbb{N}$, $\left(\frac{-d}{p}\right) = -1$, $m > 2$, and let E_m denotes the set of of residue classes modulo p^m over the ring of Gaussian integers in imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with norms which are congruented with 1 modulo p^m. In present paper we establish the polynomial representations for real and imagimary parts of the powers of generating element $u+iv\sqrt{d}$ of the cyclic group E_m. These representations permit to deduce the "rooted bounds" for the exponential sum in Turan-Erdös-Koksma inequality. The new family of the sequences of pseudo-random numbers that passes the serial test on pseudorandomness was being buit.
MSC: 11L07, 11T23, 11T71, 11K45.
Key words: imaginary quadratic field, norm group, pseudorandom numbers, discrepancy.
DOI: 10.18524/2519-206X.2020.2(36).233737.

1. Introduction

The sequence of real numbers $\{a_n\}$, $0 \le a_n < 1$ we call the sequence of pseudorandom numbers (abbreviation, PRN's) if it is produced by deterministic generator and, being a periodical sequence, has the statistical properties such that it looks like to implementation of the sequence of random numbers with independent and uniformly distributed values on $[0, 1)$. Primary sequences of PRN's are the sequences of PRN's which generated by the congruential recursion of the type

$$y_{n+1} \equiv f(y_n, y_{n-1}, \dots, y_{n-k+1}) \pmod m$$

with some initial values $y_0, y_1, \dots, y_{k-1} \in \{0, 1, \dots, m-1\}$, where $f(u_1, \dots, u_k)$ is integer-valued function over $\mathbb{Z}_m^k$. Such sequences have been studied with many results (see, survey [12]).

Because it emerged that linear function $f(u) = au + b$ does not supply requirements of "affinity" to statistical independent (unpredictable) sequence (see, [10]), this motivated the creation of nonlinear congruential pseudorandom sequences having an unpredictability property.

Received 07.10.2020
© Fugelo P., Varbanets S. 2020

The generator produced by the quadratic function $f(u) = au^2 + bu + c$ satisfies to condition of "practical" unpredictability (see, [6]).

The generator associated with quadratic function $f(c)$ we call parabolical.

In 1989 J. Eichenauer and J. Lehn[4] and H. Niederreiter[13] have studied the sequences generated by the congruential relation modulo p

$$x_{n+1} = \begin{cases} ax_n^{-1} + b & if \quad x_n \neq 0, \\ b & if \quad x_n = 0. \end{cases}$$

with some coefficients $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$.

In the paper [18] there are investigated the analogous of inversive congruential generators, that without any increases of computational complexity of finding the elements of sequence $\{y_n\}$, have got an essential complexity for intruder's to work around the parameters of inversive or linear generator to be recovered.

The requirements to uniform distribution and unpredictability is satisfied the following inversive generator

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m},$$

where p is a prime number, $a, b \in \mathbb{Z}$, y_n^{-1} is a multiplicative inverse to y_n (mod p^m).

The inversive generator and its generalization was being investigated by many authors (see, [1], [2], [3], [5], [6], [7], [8], [11], [15], [16], [17], [18]).

Starting out from our reasoning, we will call such inversive generator as hyperbolical.

In [19] there have been studied the statistical properties of sequences of PRN's produced by a number generator, which determines by the norm group of the ring of residue classes of modulus p^m of the ring of Gaussian integers. That generator we call circular generator.

In present paper we consider the generalization of generator from [19] and study the statistical properties of the sequences of PRN's produced by this generator.

Our main aim here is to elucidate the motivation for constructing circular generator of the sequences of PRN's with some specific properties that be faster of its usage in cryptography. Our exposition focuses on some special measures of "randomness" with respect to which "the good" sequences have

been produced by using of norm group E_m. A quantive measure of uniformity of distribution of a sequence may be the so-called discrepancy. Originated from a classical problem in Diophantine approximations this concept has found applications in the analysis of PR sequences on uniformity and unpredictability. From the well-known Turan-Erdös-Koksma inequality it is evident that the main tool in estimating discrepancy is the use of bounds on exponential sums over on elements of the sequence of PRN's. This motivates a construction this paper.

Before we proceed further we will fix the notation that will be used throughout this paper.

Notation.

- Lower case Roman (respectively, Greek) letters usually denote rational (respectively, nonrational) integers of field $\mathbb{Q}$ (respectively, field $\mathbb{Q}(\sqrt{-d})$, d is a free-square natural number); in particular, m, n, k are positive integers and p is a rational prime number.
- We also define a *norm* over $\mathbb{Q}(\sqrt{-d})$ into $\mathbb{Q}$ by $N(\alpha) = a^2 + db^2$ for $\alpha = a + b\sqrt{-d}$, $a, b \in \mathbb{Q}$.
- For the sake of convenience, we suppose $d \equiv 1 \pmod 4$ and denote by G the set of integer elements of $\mathbb{Q}(\sqrt{-d})$.
- Let $\mathbb{Z}_q$ (or G_q) denotes the ring of residue classes modulo q, and $\mathbb{Z}_q^*$ (or G_q^*) denotes 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 an arbitrary integer of $\mathbb{Q}(\sqrt{-d})$ satisfying the condition $x \cdot x^{-1} \equiv 1 \pmod q$.
- For $a \in \mathbb{Z}$ the symbol $\left(\frac{a}{p}\right)$ denotes a symbol of Legendre.
- As usual, (a, b) stand for the greater common divisor of integer rational a and b (or, respectively, α and β in G).
- Through $\mathbb{Z}[x]$ (or $G[x]$) we denote the polynomial ring over $\mathbb{Z}$ (or G).
- For $a \in \mathbb{Z}$ ($\alpha \in G$) stand $\nu_p(a)$ (or $\nu_p(\alpha)$) if $p^{\nu(a)} | a$ and $p^{\nu(a)+1} \nmid a$.

- The fraction $\frac{a}{b}$, $(b,q)=1$, of modulus q means as ab^{-1}, where b^{-1} is a multiplicative inverse modulo q.
- At last, $e_q(x)$ denotes $e^{2\pi i\frac{x}{q}}$.

2. Auxiliary arguments

We start by listing some previous estimates of exponential sums which will be used to establish our main results.

Let $f(x)$ be a periodic function with a period τ. For any $N\in\mathbb{N}$, $1\le N\le\tau$, we denote

$$S_N(f):=\sum_{x=1}^{N}e^{2\pi if(x)}$$

Lemma 1. *The following estimate*

$$|S_N(f)|\le\max_{1\le n\le\tau}\left|\sum_{x=1}^{\tau}e^{2\pi i\left(f(x)+\frac{nx}{\tau}\right)}\right|\log\tau$$

holds.

This statement is well-known lemma about an estimate of uncomplete exponential sum by means of the complete exponential sum (see, [9]).

Lemma 2. *Let p be a prime number and let $f(x)$ be a polynomial over $\mathbb{Z}$*

$$f(x)=A_1x+A_2x^2+p(A_3x^3+\cdots),$$

and, moreover, let $\nu_p(A_2)=\alpha>0$, $\nu_p(A_j)>\alpha$, $j=3,4,\ldots$. Then we have the following estimate

$$\left|\sum_{x\in\mathbb{Z}_{p^m}}e^{2\pi i\frac{f(x)}{p^m}}\right|=\begin{cases}p^{\frac{m+\alpha}{2}} & \text{if } \nu_p(A_1)\ge\alpha,\\ 0 & \text{else,}\end{cases}$$

(see, [16]).

The relevant statistical properties of any sequence of the independent and uniformly distributed random numbers are, first of all, uniformity and dependence. Departures from uniformity or independency may be detected by theoretical or empirical tests. The main tools of theoretical tests for the establishment of the uniformity or dependency of the sequence $\{x_n\}$ is the s-dimensional

discrepancy of the points $X_n^{(s)} = (x_n, x_{n+1}, \dots, x_{n+s-1})$, $s = 1, 2, \dots$, which defined by

$$D_N(X_0^{(s)}, X_1^{(s)}, \dots, X_{N-1}^{(s)}) := \sup_{\Delta \subset [0,1)^s} \left| \frac{A_N(\Delta)}{N} - vol(\Delta) \right|,$$

where $A_N(\Delta)$ is the number of points $X_n^{(s)}$ falling into $\Delta \subset [0,1)^s$, $vol(\Delta)$ is a volume of Δ, and the supremum is extended over all subintervals Δ of $[0,1)^s$.

If $D_N(X_0^{(s)}, X_1^{(s)}, \dots, X_{N-1}^{(s)}) \to 0$ for $N \to \infty$ we say that the sequence of PRN's $\{x_n\}$ passes the s-dimensional test on the pseudo-randomness.

The following two lemmas give the estimate for $D_N(X_0^{(s)}, X_1^{(s)}, \dots, X_{N-1}^{(s)})$.

Lemma 3. *Let $T \geq N \geq 1$ and $q \geq 2$ be integers, $\mathbf{y_k} \in \{0, 1, \dots, q-1\}^s$ for $k = 0, 1, \dots, N-1$; $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0,1)^s$. Then*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \leq \frac{s}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(q)} \sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(\mathbf{h}, q) r(h_0, T)} \times \left| \sum_{k=0}^{T} e(\mathbf{h} \cdot \mathbf{t_k} + \frac{k h_0}{T}) \right|$$

(see, [12])

Lemma 4. *The discrepancy of N arbitrary points $\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}} \in [0,1)^2$ satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \geq \frac{1}{2(\pi+2)|h_1 h_2| N} \left| \sum_{k=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_k}) \right|$$

for any lattice point $\boldsymbol{h} = (h_1, h_2) \in \mathbb{Z}^2$ with $h_1 h_2 \neq 0$.

(It is the special version of Niederreiter result in [13]).

For integers $s \geq 1$ and $q \geq 2$, let $C_s(q)$ be the set of all nonzero lattice points $\mathbf{h} = (h_1, \dots, h_s) \in \mathbb{Z}^s$ with $-\frac{q}{2} < h_j \leq \frac{q}{2}$ for $1 \leq j \leq s$. Define for $\mathbf{h} \in C_s(q)$

$$r(h, q) = \begin{cases} 1 & if\ h = 0, \\ q \sin(\pi \frac{|h|}{q}) & if\ h \neq 0, \end{cases}$$

$$r(\mathbf{h}, q) = \prod_{j=1}^{s} r(h_j, q)$$

Lemma 5. *Let* $\{\boldsymbol{Y}_n\}$ *be the sequence of* s*-dimensional points in* $(\mathbb{N}\cup\{0\})^s$ *with a period* τ*, and* $\boldsymbol{y}_n = \frac{\boldsymbol{Y}_n}{q} \in [0,1)^s$*. Then for any* N*,* $1 \le N \le \tau$*, we have*

$$D_N^{(s)}(\mathbf{y_0}, \mathbf{y_1}, \ldots, \mathbf{y_{N-1}}) \le \frac{s}{q} + \frac{1}{N} \sum_{\mathbf{h}\in C_s(q)} \sum_{h_0 \in \left(-\frac{\tau}{2}, \frac{\tau}{2}\right]} \frac{1}{r(\mathbf{h}, q) r(h_0, q)} \times \left| \sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{y_n} + \frac{nh_0}{\tau}) \right|,$$

where $\boldsymbol{h}\cdot\boldsymbol{y}$ *denotes the inner product of* $\boldsymbol{h}$ *and* $\boldsymbol{y}$*.*

Lemma 6. *Let* $X_0, X_1, \ldots, X_{N-1} \in [0,1)^s$*,* $s \ge 1$ *with discrepancy* D_N^s*. Then for any nonzero* $\overline{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ *we have*

$$\left| \sum_{n=0}^{N-1} e^{2\pi i \overline{h}\cdot X_n} \right| \le \frac{2}{\pi} \left(\left(\frac{\pi+1}{2} \right)^m - \frac{1}{2^m} \right) N D_N^{(s)} \prod_{j=1}^{s} \max(1, 2|h_j|),$$

where m *is the number of nonzero coordinates of* $\overline{h}$*.*

(see, [13])

Let p be a prime rational number, $\left(\frac{-d}{p}\right) = -1$. Let us denote by E_m the following subgroup of $G_{p^m}^*$

$$E_m := \{x \in G_{p^m}^* : \ N(x) \equiv \pm 1 \pmod{p^m}\}.$$

The subgroup E_m we call the norm group in $G_{p^m}^*$ of imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

The following lemma is constitutive for the sequence $\{x_n\}$ being investigated in our paper.

Lemma 7. *The norm group* E_m *is a cyclic group of order* $2(p+1)p^{m-1}$*. Let* $u+iv$ *denotes a generating element of* E_m*. Then exist* $x_0, y_0 \in \mathbb{Z}_{p^m}^*$ *such that*

$$(u+\sqrt{-d}v)^{2(p+1)} \equiv 1 + p^2 x_0 + \sqrt{-d} p y_0,$$
$$2x_0 + d y_0^2 \equiv -2p^2 x_0^2 \pmod{p^3}$$

and for any $t = 4, 5, \ldots$ *we have modulo* p^m

$$\Re((u+\sqrt{-d}v)^{2(p+1)t}) = A_0 + A_1 t + A_2 t^2 + \cdots$$
$$\Im((u+\sqrt{-d}v)^{2(p+1)t}) = \sqrt{d}\cdot(B_0 + B_1 t + B_2 t^2 + \cdots).$$

Moreover,

$$A_0 \equiv 1 \pmod{p^4},\ B_0 \equiv 0 \pmod{p^4},$$
$$A_1 \equiv p^2x_0 + \frac{1}{2}dp^2y_0^2 \equiv -\frac{5}{2}x_0^2p^4 \pmod{p^5},$$
$$B_1 \equiv py_0(1-p^2x_0) \pmod{p^4},$$
$$A_2 \equiv -\frac{5}{2}x_0^2p^2 \pmod{p^5},$$
$$B_2 \equiv \frac{5}{2}p^3x_0y_0 \pmod{p^4},$$
$$A_j \equiv B_j \equiv 0 \pmod{p^3},\ j = 3, 4, \ldots.$$

Proof. By virtue of the fact that the residue classes modulo p with $\left(\frac{-d}{p}\right) = -1$ generate a prime field G_p, it follows that the multiplicative group of this field is a cyclic group G_p^* and we always can yield a generating element of every group E_k of a reduced residue system modulo p^k, $k = 1, 2, \ldots$, in G.

Denote

$$(u + \sqrt{-d}v)^k = u(k) + \sqrt{-d}v(k),\ 0 \le k \le 2p+1,$$
$$(u + \sqrt{-d}v)^{2(p+1)t+k} \equiv \sum_{j=0}^{m-1}\left(A_j(k) + \sqrt{-d}B_j(k)\right) \pmod{p^m}.$$

It is clear, that

$$A_j(k) = A_ju(k) - dB_jv(k);\ B_j(k) = A_jv(k) + B_ju(k).$$

And now, the description of group E_m is performed by an analogue of description of the norm group E_m in case of Gaussian field $\mathbb{Q}(i)$ E_m (in greater details see [14]).

Thus from Lemma (7) we infer.

Consequence 1. *For $k = 0, 1, \ldots, 2p+1$, we have*

$$(u(k), p) = (v(k), p) = 1\ if\ k \not\equiv 0 \pmod{\frac{p+1}{2}};$$
$$u(0) = 1,\ v(0) = 0,\ (u(p+1), p) = 1,\ p \| v(p+1);$$
$$u(k) \equiv 0 \pmod{p},\ (v(k), p) = 1\ if\ k = \frac{p+1}{2}\ or\ \frac{3(p+1)}{2};$$
$$u(k) = u(-k),\ v(k) = -v(-k).$$

Hence, for $k \not\equiv 0 \pmod{\frac{p+1}{2}}$ *we have*

$$
\begin{aligned}
&A_0(k) \equiv u(k),\ B_0(k) \equiv v(k) \pmod{p},\\
&A_1(k) \equiv -pdy_0 v(k),\ B_1(k) \equiv py_0 u(k) \pmod{p^3},\\
&A_2(k) = -\frac{5}{2}x_0^2 p^2 u(k),\ B_2(k) \equiv -\frac{5}{2}x_0^2 p^2 v(k) \pmod{p^4},\\
&A_j(0) = A_j,\ B_j(0) = B_j,\ j = 3, 4, \ldots,\\
&A_0(p+1) \equiv -1,\ B_0(p+1) \equiv 0 \pmod{p^3},\\
&p^2 \| A_1(p+1),\ p \| B_1(p+1),\ p^2 \| A_2(p+1),\\
&p \| A_1(k),\ p^2 \| B_1(k),\ p^2 \| A_2(k),\ B_2(p+1) \equiv 0 \pmod{p^3},\\
&B_2(k) \equiv 0 \pmod{p^3}\ if\ k = \frac{p+1}{2}\ or\ \frac{3(p+1)}{2}.
\end{aligned}
$$

Lastly, we will make use the following sequences produced by a generating element $u + iv$ of the norm group E_m.

We select a random number $k \in \{0, 1, \ldots, 2p+1\}$ and consider the sequence $\{(u + \sqrt{-d}v)^{2(p+1)n+k}\}$, $n = 0, 1, \ldots, p^{m-1} - 1$.

Denote

$$x_n^{(k)} := \Re((u + \sqrt{-d}v)^{2(p+1)n+k}), \tag{1}$$

$$y_n^{(k)} := \Im((u + \sqrt{-d}v)^{2(p+1)n+k}). \tag{2}$$

Every sequence $\{x_n^{(k)}\}$ or $\{y_n^{(k)}\}$, $n = 0, 1, \ldots$, has a period $\tau = p^{m-1}$. From Lemma 7 and its corollary we obtain the description of elements of these sequences as the polynomials at n. Besides, taking into account, that

$$
\begin{aligned}
&(u + \sqrt{-d}v)^{2(p+1)} = u_0 + \sqrt{-d}v_0,\\
&u_0 = 1 + p^2 x_0,\ v_0 = py_0,\ (x_0, p) = (y_0, p) = 1
\end{aligned}
$$

and

$$x_n^{(k)} \equiv x_{n-1}^{(k)} u_0 - y_{n-1}^{(k)} v_0 \pmod{p^m}, \tag{3}$$

$$y_n^{(k)} \equiv x_{n-1}^{(k)} v_0 - y_{n-1}^{(k)} u_0 \pmod{p^m} \tag{4}$$

we may be achieved the representations of $x_n^{(k)}$, $y_n^{(k)}$ as the polynomials at x_0, y_0.

By virtue of the congruence $\left(x_n^{(k)}\right)^2 + d\left(y_n^{(k)}\right)^2 \equiv (-1)^k \pmod{p^m}$ and recursion (3) we call the sequences (1) and (2) as the sequences of PRN's

produced by the norm group. The recursions (3), (4) we call the generators associated with the norm group E_m.

Family of sequences of PRN's produced by circular generator It is clear to see that, without restricting the generality, we can take that $d = 1$ and, hence, $p \equiv 3 \pmod 4$.

So, finally, we generate the family of the sequences of congruential PRN's which associated with the sequences $\{x_n(k)\}$ and $\{y_n(k)\}$. Depending on a select $k \in \{0, 1, \dots, 2p+1\}$ we will construct the special sequences of PRN's. We will distinguish three cases of class sequences depend upon the values of k:

(A) $k \not\equiv 0 \pmod{\frac{p+1}{2}}$;

(B) $k = 0$ or $p+1$;

(C) $k = \frac{p+1}{2}$ or $\frac{3(p+1)}{2}$.

Firstly, we consider the class (A). The classes (B) and (C) may be consider by a similar way, but these classes have its specific.

So, for every $k \in \{0, 1, \dots, 2p+1\}$, $k \not\equiv 0 \pmod{\frac{p+1}{2}}$ we consider the sequences $\{x_n^{(k)}(t)\}$ and $\{y_n^{(k)}(t)\}$, $t = 0, 1, 2, \dots$. For such k we have

$$k \not\equiv 0 \pmod{\frac{p+1}{2}}.$$

In these cases $(u(k), p) = (v(k), p) = 1$.

We denote

$$z_n^{(k)} := \frac{x_n^{(k)}}{1 + v_0(k) y_n^{(k)}} \pmod{p^m}, \tag{5}$$

where $v_0(k) = v(k) + p^2 v_1(k)$, $(v_1(k), p) = 1$.

This definition is correct by virtue of the fact that

$$1 + v_0(k) y_n^{(k)} \equiv 1 + v_0(k) B_0(k) \equiv 1 + d v_0^2(k) \equiv -u_0^2(k) \pmod p,$$
$$v_0(k) \sum_{j=1}^{m-1} B_j(k) n^j \equiv 0 \pmod p.$$

And hence, denoting $(u(k)^{-1})^2 = u(k)^{-2} \pmod{p^m}$, we have modulo p^m

$$z_n^{(k)} \equiv -(u(k))^{-2}(A_0(k) + A_1(k)n + \cdots)\Bigg(1 + (u(k))^{-2} v_0(k) B_1(k) n$$
$$+ u^{-2}(k)\left(v_0(k) B_2(k) n^2 + u^{-2}(k) v_0^2(k) B_1(k)\right) n^2 + \cdots\Bigg).$$

Now, after simple calculations, we get

$$z_n^{(k)} = -(u(k))^{-2} \sum_{j=0}^{M} A_j^{(k)} n^j,$$

where

$$\begin{aligned} A_1^{(k)} &= pu(k)^{-1}y_0 - py_0v(k)u(k)^{-2}, \\ A_2^{(k)} &= v_0(k)A_0(k)B_2(k) + u(k)^{-2}v_0(k)^2A_0(k)B_1^2(k) \\ &\quad + v_0(k)A_1(k)B_1(k) + A_2(k), \\ A_j^{(k)} &\equiv 0 \pmod{p^3},\ j = 3, 4, \ldots. \end{aligned}$$

So, we obtain modulo p^m

$$z_n^{(k)} = F(n) \equiv (u(k))^{-1} \left[A_0^{(k)} + p^2y_0v_1(k)n + p^2c_2(k)n^2 + p^3G(n) \right], \qquad (6)$$

where

$$c_2(k) = y_0^2 \cdot (-2x_0u^{-1}(k)v^2(k) - 10x_0^2u^2(k) - 10x_0^2u^{-1}(k)v(k) - u^{-3}(k)v^2(k)), \qquad (7)$$

where $G(n) \in \mathbb{Z}_{p^m}[n]$.

The relation (6) defines the representation of $z_n^{(k)}$ as the polynomial at n.

In case of (B) we consider the sequence $\{z_n^{(k)}\}$, $z_n^{(k)} = \frac{x_n^{(k)}}{y_n^{(k)}}$.

Finally, in case of (C) we let

$$z_n^{(k)} = \frac{x_n^{(k)}}{1 + y_n^{(k)}}$$

and similarly to (A) we infer the representation $z_n^{(k)}$ as polynomial at n.

This allows us to state the following theorem.

Theorem 1. *Let $h_1, h_2, j \in \mathbb{Z}$, $(h_1, h_2, p^m) = p^\ell$. Then for the sequence of PRN's $\{z_n^{(k)}\}$ the following estimate*

$$|S_j(h_1, h_2)| := \left| \sum_{n=0}^{p^{m-1}-1} e_{p^m}(h_1z_n^{(k)} + h_2z_{n+j}^{(k)}) \right| \le p^{\frac{m+\ell}{2}}$$

holds for every $j \in \{1, \ldots, 2p+1\}$.

Proof. Without less of generality that $(h_1, h_2, p^m) = 1$, using the relations (6) we can write for $k \not\equiv 0 \pmod{\frac{p+1}{2}}$

$$h_1 z_n^{(k)} + h_2 z_{n+j}^{(k)} \equiv$$
$$\equiv (u(k))^{-2}\Bigg[A_0^{(k)} + p^2((h_1 v(k) + h_2 v(k)(1 + pO(j)))y_0 v(k) + 2{\cdot}h_2 c_2(k)(1 + pO(j)))n$$
$$+p^2(h_1 c_2(k) + h_2 c_2(k)(1 + pO(j)))n^2 + p^3 G_1(n)\Bigg] \pmod{p^m},$$

where c_2 defined in (7)

By the condition $(h_1, h_2, p^m) = 1$, it follows that the congruences

$$(h_1 v(k) + h_2 v(k)(1 + pO(j)))y_0 v(k) + 2{\cdot}h_2 c_2(k)(1 + pO(j)) \equiv 0 \pmod{p}$$
$$h_1 c_2(k) + h_2 c_2(k)(1 + pO(j)) \equiv 0 \pmod{p}$$

cannot be realized simultaneously. Thus, by Lemma 2, we infer

$$|S_j(h_1, h_2)| \le \begin{cases} 0 & if \quad h_1 + h_2 \equiv 0 \pmod{p}, \\ p^{\frac{m}{2}} & if \quad h_1 + h_2 \not\equiv 0 \pmod{p}. \end{cases} \tag{8}$$

Consequence 2. *The discrepancy of the sequence* $\left\{\frac{X_n^{(s)}}{p^{m-1}}\right\}$, $s = 1, 2$, *has the following bound*

$$D_N^{(s)} \le \frac{s}{p^{m-1}} + \frac{2p^{\frac{m-1}{2}}}{N}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^s, \ 0 < N \le \tau, \tag{9}$$

where $X_n^{(s)} = \left(z_n^{(k)}, \dots, z_{n+s-1}^{(k)}\right)$.

This assertion follows from Lemma 4 and Theorem 1. Now we prove a lower estimate $D_N^{(2)}$.

Theorem 2. *Let p be a prime number, $p \equiv 3 \pmod 4$ and let $z_n^{(k)}$ defined by the relation (5), $k \not\equiv 0 \pmod{\frac{p+1}{2}}$. Then for the sequence $\{w_n^{(k)}\}$, $w_n^{(k)} = \frac{z_n^{(k)}}{p^m}$, $n = 0, 1, \dots, \tau - 1$, we have*

$$D_\tau^{(2)}(W_0^{(k)}, W_1^{(k)}, \dots, W_{\tau-1}^{(k)}) \ge \frac{1}{4(\pi + 2)} p^{-\frac{m-1}{2}}, \tag{10}$$

where $W_n^{(k)} = (w_n^{(k)}, w_{n+1}^{(k)})$, $n = 0, 1, \dots, \tau - 1$.

Proof. We take $h_1 = h_2 = 1$. Then by Theorem 1 with $j = 1$ and Lemma 7, we at one obtain

$$D_\tau^{(2)} \ge \frac{1}{2(\pi + 2)}\tau^{-\frac{1}{2}} = \frac{1}{2(\pi + 2)} p^{-\frac{m-1}{2}}.$$

(For detailed proof, see [16]).

Theorem 1 and 2 show that, in general, the upper bound is the best possible up to the logarithmic factor for circular congruential sequence $\{(w_n^{(k)}, w_{n+1}^{(k)})\}$, $n \geq 0$, defined by congruence (5) (or (10)).

3. Conclusion

In conclusion we have the following two remarks.

Remark 1. *It is straightforward to verify that all that we said in the case the sequence produced of the relation (5) also holds for the sequence produced by the congruence*

$$z_n^{(k)} \equiv u_0(k)x_n^{(k)} + v_0(k)y_n^{(k)} \pmod{p^m} \tag{11}$$

with $u_0(k) = u(k)+p^2u_1(k)$, $v_0(k) = v(k)+p^2v_1(k)$, $(u_1(k), p) = (v_1(k), p) = 1$.

Remark 2. *Relations (3), (4) make it possible to drive the representations* $x_n^{(k)}$, $y_n^{(k)}$ *and consequently* $z_n^{(k)}$ *as polynomials at* x_0, y_0. *Thus it may be well to construct non-trivial estimates of exponential sums over generating element of the norm group* E_m.

Фугело П., Варбанець С.
Генератор ПВЧ на норменій групі

Резюме

Нехай p — просте число, $d \in \mathbb{N}$, $\left(\frac{-d}{p}\right) = -1$, $m > 2$, і нехай E_m позначає множину класів лишків за модулем p^m над кільцем цілих гаусових чисел в уявному квадратичному полі $\mathbb{Q}(\sqrt{-d})$ з нормами, що дорівнюють 1 за модулем p^m. В даній статті ми отримуємо поліноміальні зображення для дійсної та уявної частин степенів породжуючого елементу $u + iv\sqrt{d}$ циклічної групи E_m. Ці зображення дозволяють отримати "кореневі границі" експоненційної суми в нерівності Турана-Ердьоша-Коксми. Також було побудовано нове сімейство послідовностей псевдовипадкових чисел, що проходять серіальний тест на псевдовипадковість.
Ключові слова: уявне квадратичне поле, норменна група, псевдовипадкові числа, дескріпансія.

Фугело П., Варбанец С.
Генератор ПСЧ на норменой группе

Резюме

Пусть p — простое число, $d \in \mathbb{N}$, $\left(\frac{-d}{p}\right) = -1$, $m > 2$, и пусть E_m обозначает множество классов вычетов по модулю p^m над кольцом целых гауссовых чисел в мнивом квадратичном поле $\mathbb{Q}(\sqrt{-d})$ с нормами, которые сравнимы с 1 по модулю p^m. В данной статье мы получаем полиномиальные представления действительной и мномой честей степеней порождающего елемента $u + iv\sqrt{d}$ циклической группы E_m. Эти представления позволяют получить "корневые границы" экспоненциальной суммы в неравенстве Турана-Эрдёша-Коксмы. Также было построено новое симейство последовательностей псевдослучайных чисел, которые проходят сериальный тест на псевдослучайность.
Ключевые слова: мнимое квадратичное поле, норменная группа, псевдослучайные числа, дескрипансия.

References

1. **Eichenauer-Herrmann J.** Inversive congruential pseudorandom numbers: a tutorial / Eichenauer-Herrmann J. // Internat. Statist. Rev. – 1992. – 60, № 2. – P. 167–176. doi: 10.2307/1403647
2. **Eichenauer-Herrmann J.** Pseudorandom number generation by nonlinear methods / Eichenauer-Herrmann J. // Internat. Statist. Rev. – 1995. – 63, №2. – P. 247–255. doi: 10.2307/1403620
3. **Eichenauer-Herrmann J.** A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus / Eichenauer-Herrmann J., Grothe H. // ACM Transactions of Modelling and Computer Simulation. – 1992. – 2, №1. – P. 1–11. doi: 10.1145/132277.132278
4. **Eichenauer J.** A non-linear congruential pseudorandom number generator / Eichenauer J., Lehn J. // Statist. Hefte. – 1986. – 27, №1. – P. 315–326. doi: 10.1007/BF02932576
5. **Eichenauer J.** A nonlinear congruential pseudorandom number generator with power of two modulus / Eichenauer J., Lehn J. and Topuzoğlu A. // Math. Comp. – 1988. – 51, №18. – P. 757–759. doi: 10.2307/2008776
6. **Eichenauer-Herrmann J.** A survey of quadratic and inversive congruential pseudorandom numbers / Eichenauer-Herrmann J., Herrmann E. and Wegenkittl S. // Monte Carlo and Quasi-Monte Carlo Methods 1996, H. Niederreiter et al(eds.), Lecture Notes in Statist, Springer, New York. – 1998. – 127. – P. 66–97. doi: 10.1007/978-1-4612-1690-2_4
7. **Eichenauer-Herrmann J.** On the period of congruential pseudorandom number sequences generated by inversions / Eichenauer-Herrmann J. and Topuzoğlu A. // J. Comput. Appl. Math. – 1990. – 31, №1. – P. 87–96. doi: 10.1016/0377-0427(90)90339-2
8. **Kato T.** On a nonlinear congruential pseudorandom number generator / Kato T., Wu L.-M., Yanagihara N. // Math. of Comp. – 1996. – 65, №213. – P. 227–233. doi: 10.1090/S0025-5718-96-00694-1
9. **Korobov N.M.** Estimates of trigonometric sums and their applications / Korobov N.M. // Uspekhi Mat. Nauk. – 1958. – 13, №4(82). – P. 185–192. MR:106205, Zbl:0086.03803.

10. **Knuth D.E.** The Art of Computer Programming. In: Trigub S. N. (Third Eds.) Poluchislennye algoritmy / Knuth D.E. – 2. – 2000.

11. **Niederreiter H.** Nonlinear methods for pseudorandom number and vector generation / Niederreiter H. // Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems. – 1992. – 374. – P. 145–153. doi: 10.1007/978-3-642-48914-3_11

12. **Niederreiter H.** Random Number Generation and Quasi-Monte Carlo Methods / Niederreiter H. // Society for Industrial and Applied Mathematics, Philadelphia. – 1992. – P. .

13. **Niederreiter H.** Lower bounds for the discrepancy of inversive congruential pseudorandom numbers / Niederreiter H. // Math. of Comput. – 1990. – 55, №191. – P. 277–287. doi: 10.1090/S0025-5718-1990-1023766-0

14. **Varbanets S.P.** The norm Kloosterman sums over $\mathbb{Z}[i]$ / Varbanets S.P. // Anal. Probab. Methods in Number Theory. – 2008. – 3, №11. – P. 225–239.

15. **Varbanets S.** On inversive congruential generator for pseudorandom numbers with prime power modulus / Varbanets S. // Annales Univ. Sci. Budapest, Sect. Comp. – 2008. – 29. – P. 277–296.

16. **Varbanets P.** Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus / Varbanets P., Varbanets S. // VoronoÏ's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Kyiv, Ukraine, September 22-28. – 2008. – 4, №1. – P. 112–130.

17. **Varbanets S.** Exponential sums on the sequences of inversive congruential pseudorandom numbers / Varbanets S. // Siauliai Math. Semin. – 2008. – 3, №11. – P. 247–261.

18. **Varbanets P.** Generalizations of Inversive Congruential Generator / Varbanets P., Varbanets S. // Analytic and probabilistic methods in number theory, Proceedings of the 5^{th} international conference in honour of J. Kubilius, Palanga, Lithuania, September 4–10, 2011, Vilnius: TEV. – 2012. – P. 265–282.

19. **Varbanets S.** Circular generator of PRN's / Varbanets S. // 7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon, Portugal. – 2014. – P. 523–532.