ISSN 2304-1579. Visnyk Odesk. Nats. Univers. Mat. i Mekh.–2013 .–V.18,Is.4(20).–P.68–75

Mathematical Subject Classification: 11K45, 11T23, 11T71
UDC 511

Tran The Vinh, P. Varbanets
Odesa I. I. Mechnikov National University

INVERSIVE CONGRUENTIAL GENERATOR OF THE COMPLEX PSEUDO-RANDOM NUMBERS

Тран Тхе Вінь, Варбанець П. Д. Інверсний конгруенційний генератор комплексних псевдовипадкових чисел. Розглядається розподілення елементів послідовності псевдовипадкових комплексних чисел, породжених лінійно-інверсним генератором за модулем степені простого числа p, $p \equiv 3 \pmod 4$, в секторіальних областях одиничного кола комплексної площини. Побудовано аналог нерівності Турана–Ердьоша–Коксми, що дозволяє отримати нетривіальні оцінки дискріпантної функції $D_N^{(s)}(X_0, \dots, X_{N-1})$. Показано, що послідовність $\{\omega_n\}$, $\omega_n = \frac{z_n}{p^m}$, породжена рекурсією $z_{n+1} \equiv \alpha z_n^{-1} + \beta + \gamma z_n \pmod{p^m}$, $n = 0, 1, 2, \dots$ за відповідних умов на коефіцієнти α, β, γ і ініціальне значення z_0, має максимальний період $\tau = 2p^{m-\nu}$, $\nu = \nu_p(\beta)$ і проходить s-мірний тест на рівнорозподіленість та непередбачуваність.
Ключові слова: псевдовипадкові числа, дискріпансія, експоненційні суми.

Тран Тхе Винь, Варбанец П. Д. Инверсный конгруентный генератор комплексных псевдослучайных чисел. Рассматривается распределение элементов последовательности псевдослучайных комплексных чисел, порожденных линейно-инверсным генератором по модулю степени простого числа p, $p \equiv 3 \pmod 4$, в секториальных областях единичного круга комплексной плоскости. Построен аналог неравенства Турана–Эрдёша–Коксмы, позволяющий получить нетривиальные оценки дескрипантной функции $D_N^{(s)}(X_0, \dots, X_{N-1})$. Показано, что последовательность $\{\omega_n\}$, $\omega_n = \frac{z_n}{p^m}$, порожденная рекурсией $z_{n+1} \equiv \alpha z_n^{-1} + \beta + \gamma z_n \pmod{p^m}$, $n = 0, 1, 2, \dots$ при определенных условиях на коэфициенты α, β, γ и инициальное значение z_0, имеет максимальный период $\tau = 2p^{m-\nu}$, $\nu = \nu_p(\beta)$ и проходит s-мерный тест на равнораспределенность и непредсказуемость.
Ключевые слова: псевдослучайные числа, дескрипансия, экспоненциальные суммы.

Tran The Vinh, Varbanets P. Inversive congruential generator of the complex pseudo-random numbers. Consider the distribution of elements of the sequence on pseudo-random complex numbers generated by linear-inversive generator modulo prime power number p, $p \equiv 3 \pmod 4$, in sectorial regions from unit ball of complex plane. We constructed an analogue of Turan-Erdos-Koksma inequality that make it possible to derive non-trivial bounds for discrepancy $D_N^{(s)}(X_0, \dots, X_{N-1})$. It is shown that the sequence $\{\omega_n\}$, $\omega_n = \frac{z_n}{p^m}$, produced by the recursion $z_{n+1} \equiv \alpha z_n^{-1} + \beta + \gamma z_n \pmod{p^m}$, $n = 0, 1, 2, \dots$ under certain conditions to coefficients α, β, γ and initial value z_0, has maximal period $\tau = 2p^{m-\nu}$, $\nu = \nu_p(\beta)$, and it passes the s-dimensional test on equidistribution and unpredictability.
Key words: pseudo-random numbers, discrepancy, exponential sum.

Introduction. Let p be a prime number, $m > 1$ be a positive integer. Consider the following recursion

$$y_{n+1} \equiv a y_n^{-1} + b \pmod{p^m}, (a, b \in \mathbb{Z}), \tag{1}$$

© Tran The Vinh, Varbanets P., 2013

where $\overline{y}_n$ is a multiplicative inversive modulo p^m for y_n if $(y_n, p) = 1$. The parameters a, b, y_0 we called the multiplier, shift and initial value, respectively.

In [4] there was constructed the linear-inversive congruential generator

$$y_{n+1} \equiv ay_n^{-1} + b + cy_n \pmod{p^n} \tag{2}$$

with $(a, p) = 1$, $b \equiv c \equiv 0 \pmod{p}$, such that the sequence $\{\frac{y_n}{p^m}\}$ passes serial test on equidistribution and statistical independence (unpredictability as well).

Our purpose in this work is to show a passing the tests on equidistribution and unpredictability for sequence $\{\omega_n\}$, $\omega_n = \frac{z_n}{p^m}$, where z_n produced by the recursion

$$z_{n+1} \equiv \alpha z_n^{-1} + \beta + \gamma z_n \pmod{p^m}, \tag{3}$$

α, β, γ are the Gaussian integers, p is a prime rational integer, $p > 2$, $m \in \mathbb{N}$, $m \geqslant 3$.

Hence, the main point to be shown is the possibility for such sequences of complex numbers to be used in the problem of modeling the real processes and in cryptography.

We consider the sequence of complex numbers $\{z_n\}$, $|z_n| \leqslant 1$. Let $0 \leqslant \xi_1 < \xi_2 \leqslant 1$, $0 \leqslant \varphi_1 < \varphi_2 \leqslant 2\pi$ and let $P(\xi, \varphi)$ denotes the sectorial region of unit ball $|z| \leqslant 1$

$$P(\xi, \varphi) := \{z \in \mathbb{C} : \ \xi_1 < N(z) \leqslant \xi_2, \ \varphi_1 < \arg z \leqslant \varphi_2\}. \tag{4}$$

Denote by $\mathfrak{F}$ the collection of sectorial region $P(\xi, \varphi)$ for all ξ and φ.

The sequence $\{z_n\}$ calls the pseudo-random in unit circle if it induces by a determinative algorithm, and its statistic properties are "similar" on property of sequence of the random numbers. The "similarity" means that this sequence closely adjacent to uniformly distributed in the disk $|z| \leqslant 1$, and its elements are uncorrelated. On these properties of the sequence of pseudo-random numbers (abbreviation: PRN's) can destine by value of discrepancy D_N of the points $z_1, z_2, \ldots, z_N$:

$$D_N(z_1, z_2, \ldots, z_N) := \sup_{P \subset \mathbb{C}} \left| \frac{A_N(P)}{N} - |P| \right|, \tag{5}$$

where $A_N(P)$ is the number of points among $z_1, \ldots, z_N$ falling into P, $|P|$ denotes the volume P; supremum is extended over all sectorial region P of unit circle $|z| \leqslant 1$.

The similar definition of discrepancy D_N has for the s-dimensional sequence of complex points $Z_n^{(s)} = \left(z_1^{(s)}, \ldots, z_n^{(s)}\right)$, $z_j \in \mathbb{C}$.

We say that the sequence $\{z_n\}$ passes s-dimensional test on uncorrelatedness if it passes ℓ-dimensional test on equidistribution, i.e.

$$D_N^{(\ell)}\left(z_1^{(\ell)}, \ldots, z_N^{(\ell)}\right) \to 0 \ at \ N \to \infty,$$

for $\ell = 1, 2, \ldots, s$.

Notation. Let G denotes the ring of the Gaussian integers, $G := \{a + bi : \ a, b \in \mathbb{Z}\}$; $N(z) = |z|^2$ calls the norm of $z \in G$. For $\gamma \in G$ denote G_γ (respectively, G_γ^*) the complete system of residues (respectively, reduced residue system) in G modulo γ; p is a prime number in $\mathbb{Z}$; $\mathfrak{p}$ is a Gaussian prime number. If q is a positive integer, $q > 1$, then we write $e_q(x) = e^{2\pi i \frac{x}{q}}$ for $x \in \mathbb{R}$. Symbols "O" and "$\ll$" are equivalent;

$\nu_p(\alpha) = k$ if $p^k|\alpha$, $p^{k+1} \not| \alpha$.

Let $M > 1$ be a positive integer and let $y_1, y_2, \dots, y_N$ be some sequence of points form G_M and let $Y_M = \{\frac{y_n}{M}\}$, $n = 0, \dots, N-1$. For $P \in \mathfrak{F}$ denote $A(P, Y_M)$ the number of points from Y_M contained in P.

We will adapt the proof from [2] for a construction of an analogue of the Turan-Erdös-Koksma inequality.

We define the adequate approximation of sectorial region $P \in \mathfrak{F}$,

$$P := \left\{ \frac{z}{q} : \ N_1 \leqslant N(z) \leqslant N_2, \ 0 \leqslant \varphi_1 < \arg z \leqslant \varphi_2 < 2\pi \right\}, \ q \in \mathbb{N}.$$

The set $S(P)$ calls the adequate approximation of P if

(i) $A(P, Y_N(M)) = A(S(P), Y_N(M)) + O\left(N^{\frac{1}{2}}\right)$,

(ii) volumes $|P|$ and $|S(P)|$ are "similar",

(iii) $A(S(P), Y_N(M))$ has a representation by an exponential sum.

Let N_1, N_2, φ_1, φ_2 are the parameters in the definition of P. For $r, s \in \mathbb{Z}_M$ we set $\overline{r} = \frac{r}{M}$, $\overline{s} = \frac{s}{M}$.

Determine

$$S_{\overline{r},\overline{s}} : \left\{ \beta = \frac{\alpha}{M} : \ \alpha \in G_M, \overline{r} < N(\beta) \leqslant \overline{r} + \frac{1}{M}, \ 2\pi\overline{s} < \arg\alpha \leqslant 2\pi\left(\overline{s} + \frac{1}{M}\right) \right\}. \quad (6)$$

Put

$$S(P) := \bigcup_{\substack{\overline{r},\overline{s}, \\ S_{\overline{r},\overline{s}} \subset P}} S_{\overline{r},\overline{s}}.$$

It is obvious that $S(P) = P(\overline{N}_1, \overline{N}_2, \psi_1, \psi_2)$, where

$$\begin{aligned}
\overline{N}_1 &= \min\{\frac{a}{M}, \ a \in \mathbb{Z}_M : \ N_1 \leqslant \frac{a}{M}\}, \\
\overline{N}_2 &= \min\{\frac{b}{M}, \ b \in \mathbb{Z}_M : \ N_2 \leqslant \frac{b}{M}\}, \\
\psi_1 &= \min\{\frac{2\pi a}{M}, \ a \in \mathbb{Z}_M : \ \psi_1 \leqslant \frac{2\pi a}{M}\}, \\
\psi_2 &= \min\{\frac{2\pi b}{M}, \ b \in \mathbb{Z}_M : \ \psi_2 \leqslant \frac{2\pi b}{M}\}.
\end{aligned}$$

We proved the following analogue of the Turan-Erdös-Koksma inequality (see,[3])

Auxiliary arguments.

Theorem 1. *Let $M > 1$ be integer. Then for any sequence $\{y_n\}$, $y_n \in G_M$, the discrepancy D_N of points $\{\frac{y_n}{M}\}$ satisfies to inequality*

$$\begin{aligned}
D_N \leqslant 2 &\left(1 - \left(1 - \frac{2\pi}{M}\right)^2\right) + \\
&+ \frac{1}{M} \sum_{\substack{h \in G_M \\ h \neq 0}} \min\left(\frac{1}{|\sin \pi\Re h|}, \frac{1}{|\sim \pi\Im h|}\right) \frac{1}{N} \left(|S_N| + O\left(N^{\frac{1}{2}}\right)\right),
\end{aligned}$$

where $S_N = \sum\limits_{n=0}^{N-1} e_M(\Re(hy_n))$.

Proof. By an analogue with the work[2] we infer

$$R_N(S(P)) := \frac{A(S(P))}{N} - |S(P)| = \frac{1}{N}\sum_{n=0}^{N-1} \chi_{S(P)}(x_n) - |S(P)|, \tag{7}$$

where $x_n = \frac{y_n}{M}$, χ_Δ is the characteristic function of the set Δ.

By the equality

$$\chi_{S_{\overline{r},\overline{s}}}(x) = \sum_{\alpha \in S_{\overline{r},\overline{s}}} \frac{1}{M^2} \sum_{h \in G_M} e_M(h(\alpha - x))$$

we get

$$|R_N(S(P))| \leqslant$$
$$\leqslant \sum_{0 \neq h \in G_M} \frac{1}{M^2} \left| \sum_{z(r,s) \in S_{\overline{r},\overline{s}}} e_M(-\Re(hz(r,s))) \right| \cdot \left| \frac{1}{N} \sum_{n=0}^{N-1} e_M(\Re(hy_n)) \right|, \tag{8}$$

where $z(r,s)$ is the complex number such that

$$N(z(r,s)) = \frac{r}{M},\ \arg z(r,s) = \frac{2\pi s}{M}.$$

In order to calculate the first inner sum over $S_{\overline{r},\overline{s}}$ one needs an estimate of the sum

$$\sum_M = \sum_{\substack{N_1 < N(\omega) < N_2, \\ \varphi_1 < \arg\omega \leqslant \varphi_2}} e_M(\Re(h\omega)), \quad (0 \neq h \in G_M). \tag{9}$$

The sum $\sum_M$ can be considered as asum of coeficients of Dirichlet series for the Hecke Z-function over the Gaussian field $\mathbb{Q}(i)$:

$$Z_m(s, \delta_0, \delta_1) = \sum_{0 \neq \omega \in G} \frac{e^{2\pi i \Re(\omega\delta_1)}}{N(\omega + \delta_0)^s} e^{4mi \arg\omega}, (\Re s > 1).$$

Putting $\delta_0 = 0$, $\delta_1 = \frac{h}{M}$, we obtain for any $T > 1$ by a standard way the following estimates:

$$\begin{aligned} \sum_{N(\omega) \leqslant x} e_M(h\omega) = (\varphi_2 - \varphi_1) \sum N(\omega) \leqslant x e_M(h\omega) + O\left(\frac{1}{T} \sum_{N(\omega) \leqslant x} 1 \right) + \\ + O\left((\varphi_2 - \varphi_1) \sum_{m=1}^{T} \left| \sum_{N(\omega) \leqslant x} e_M(h\omega) e^{4mi \arg\omega} \right| \right). \end{aligned} \tag{10}$$

$$\sum_{N(\omega) \leqslant x} e_M(h\omega) e^{4mi \arg\omega} \ll_\varepsilon \frac{x^{\frac{1}{2}+\varepsilon}}{M^{\frac{1}{4}}} + M^{\frac{1}{2}} (|m| + 3)^{1+\varepsilon} \tag{11}$$

(for the details, see Chapter 2 of [1], for example).

Next, we have a simple analogue of the estimate of linear exponential sum over G

$$\begin{gathered}\left|\sum_{N_1<N(\omega)<N_2} 2^{2\pi i\Re(\alpha\omega)}\right| \leqslant \\ \leqslant (N_2-N_1)^{\frac{1}{2}} \min\left((N_2-N_1)^{\frac{1}{2}}, \frac{1}{|\sin\pi\Re\alpha|}, \frac{1}{|\sin\pi\Im\alpha|}\right).\end{gathered} \tag{12}$$

Now by (6)-(11), putting $T = x^{\frac{2}{3}}$ and taking into account that $|P| = \frac{\varphi_2-\varphi_1}{2}(N_2-N_1)$, we obtain our assertion. ■

Theorem 1 shows that the estimates of discrepancy are essentially depended on estimate of the special exponential sum on the sequence of pseudo-random numbers $\{\omega_n\}$.

To construct such estimate we need the following lemmas.

Lemma 1. *Let $f(x) = A_1x + A_2x^2 + p(A_3x^3 + \cdots)$ be a polynomial over G, and let $(A_2, p) = 1$. Then, for any $A \in G$, we have*

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

where x^{-1} denotes the multiplicative inverse of x in R_n^*.

Lemma 2. *Let $\{y_n\}$ is the sequence of PRN's generated by the recursion (3) with conditions $(y_0, p) = (\alpha, p) = 1$, $0 < \nu_p(\beta) < \nu_p(\gamma)$. There exist the polynomials $F_0(u,v,w)$, $G_0(u,v,w)$ over $\mathbb{Z}$ such that for any $k \geqslant 2m+1$ the relations*

$$\begin{aligned}y_{2k} = {} & k\beta + k\alpha\gamma y_0^{-1} + (1-k(k-1)\alpha^{-1}\beta^2)y_0 + (-k\alpha^{-1}\beta)y_0^2 + \\ & + (-k\alpha^{-2}\gamma + k^2\alpha^{-2}\beta^2)y_0^3 + p^\alpha F_0(k, y_0, y_0^{-1}),\end{aligned} \tag{13}$$

$$\begin{aligned}y_{2k+1} = {} & (k+1)\beta + (\alpha - k(k+1)\beta^2)y_0^{-1} + (-k\alpha\beta)y_0^{-2} + \\ & + (-k\alpha^2\gamma + k^2\alpha\beta^2)y_0^{-3} + (k+1)\gamma y_0 + p^\alpha G_0(k, y_0, y_0^{-1}),\end{aligned} \tag{14}$$

where $\alpha := \min(\nu_p(\beta^3), \nu_p(\beta\gamma))$; $F_0(u,v,w)$, $G_0(u,v,w) \in \mathbb{Z}[u,v,w]$, and furthermore, the coefficients of the polynomials F_0, G_0 depend only on α^i, β^i, γ^i, $(\alpha^{-1})^i$, $i = 1, 2, \ldots, 2m+1$, hold.

Corollary 1. *For the sequence $\{y_n\}$ generated by (3) we have*

$$\begin{aligned}y_{2k} = {} & y_0 + k\left[\beta(1-\alpha^{-1}y_0^2) + \alpha^{-1}\beta^2 y_0 + \alpha\gamma y_0^{-1}(1-\alpha^{-2}y_0^4)\right] + \\ & + k^2\left[-\alpha^{-1}\beta^2 y_0(1-\alpha^{-1}y_0^2)\right] + p^\alpha F_0(k, y_0),\end{aligned}$$

$$\begin{aligned}y_{2k+1} = {} & (\beta + \gamma y_0 - \alpha y_0) + k\left[\beta + \gamma y_0 - \beta^2 y^{-1} - \alpha\beta y_0^{-2} - \alpha^2\gamma y_0^3\right] + \\ & + k^2\left[-\beta^2 y_0^{-1} + \alpha^2\beta^2 y_0^3\right] + p^\alpha G_0(k, y_0, y_0^{-1})\end{aligned}$$

where $k \geqslant 2m+1$, $\alpha := \min(\nu_p(\beta^3), \nu_p(\beta\gamma))$, and the coefficients of polynomials F_0, G_0 depend only on α^i, β^i, γ^i, $(\alpha^{-1})^i$, $i = 1, \ldots, 2m+1$.

Corollary 2. *The maximal period of the sequence of PRN's $\{y_n\}$ produced by (3) is equal to $\tau = 2p^{m-\nu}$ if and only if $y_0^2 \not\equiv \alpha \pmod p$.*

Main Results. Having prepared the necessary background presented above, we can obtain the main result of our paper.

Let $\{z_n\}$ be the sequence produced by the recursion 3. For $h \in \mathbb{Z}$, we denote

$$S_N(h, z_0) := \sum_{n=0}^{N-1} e^{2\pi i \frac{hz_n}{p^m}}$$

Theorem 2. *Let the linear-inversive congruential sequence generated by the recursion 3 has the period τ, and let $\nu_p(\beta) = \nu$, $\nu_p(\alpha - z_0^2) = \nu_0$, $\nu_p(h) = s$ $2\nu \leqslant m$. Then we have the following bounds*

$$|S_\tau(h, z_0)| \leqslant \begin{cases} O(m) & if \quad p > 2 \text{ and } \nu_0 < \nu,\ s < m - \nu - \nu_0 \\ & or \quad p = 2,\ \nu_0 < \nu,\ \nu_2(h) < m - 2\nu; \\ 4 \cdot p^{\frac{m+s}{2}} & if \quad \nu_0 \geqslant \nu,\ s < m - 2\nu; \\ \tau & else. \end{cases}$$

Proof. Lemma 2 and its corollaries show that the behavior of the exponential sums on the sequences of PRN's are identical. Thus we consider the sequence generated by 3. And without loss of generality we can assume that $\tau = 2p^{m-\nu}$. By the Corollary 1 we have

$$|S_\tau(h, z_0)| = \left|\sum_{n=0}^{\tau-1} e\left(\frac{hz_n}{p^m}\right)\right| = \left|\sum_{n=0}^{p^\ell-1} e\left(\frac{hz_n}{p^m}\right)\right| \leqslant$$

$$\leqslant \left|\sum_{\substack{k_1=0 \\ k=2k_1}}^{p^\ell-1} e\left(\frac{hz_{2k_1}}{p^m}\right)\right| + \left|\sum_{\substack{k_1=0 \\ k=2k_1+1}}^{p^\ell-1} e\left(\frac{hz_{2k_1+1}}{p^m}\right)\right| = \tag{15}$$

$$= \left|\sum_{k=0}^{p^\ell-1} e\left(\frac{hF(k)}{p^m}\right)\right| + \left|\sum_{k=0}^{p^\ell-1} e\left(\frac{hG(k)}{p^m}\right)\right| + O(m).$$

where

$$z_{2k} = F(k) := A_0 + A_1 k + A_2 k^2 + A_3 k^3,$$

$$z_{2k+1} = G(k) := B_0 + B_1 k + B_2 k^2 + B_3 k^3,$$

with

$$A_0 = A_0(z_0) \equiv z_0 \pmod{p^a}$$

$$A_1 = A_1(z_0) \equiv \beta(1-\alpha^{-1}z_0^2) + \alpha^{-1}\beta^2 z_0 + \alpha\gamma {z_0}^{-1}(1-\alpha^{-2}z_0^4) \pmod{p^a}$$

$$A_2 = A_2(z_0) \equiv -\alpha^{-1}\beta^2 z_0 + \alpha^{-2}\beta^2 z_0^3 \pmod{p^a} = -\alpha^{-1}\beta^2 z_0(1-\alpha^{-1}z_0^2)$$

$$B_0 = B_0(z_0) \equiv \beta + \alpha {z_0}^{-1} + \gamma z_0 \pmod{p^a}$$

$$B_1 = B_1(z_0) \equiv \beta(1-\alpha {z_0}^{-2}) - \beta^2 {z_0}^{-1} - z_0\gamma(1-\alpha^2 {z_0}^{-4}) \pmod{p^a}$$

$$B_2 = B_2(z_0) \equiv -\beta^2 {z_0}^{-1} + \alpha\beta^2 {z_0}^{-3} \pmod{p^a} = -\beta^2 {z_0}^{-1}(1-\alpha {z_0}^{-2})$$

$$A_3 = A_3(z_0,k) \equiv B_3(z_0,k) = B_3 \equiv 0 \pmod{p^a},$$

where $a := \min\{\nu_p(\beta^3), \nu_p(\beta,\gamma)\}$.

In the last part of the formula (15) we take into account that the representation z_n as a polynomial on k holds only for $k \geqslant 2m+1$.

Thus by Lemma 2 from[4] we easy obtain

$$|S_\tau(h,z_0)| \leqslant \begin{cases} O(m) & if \quad p>2,\ \nu_0<\nu,\ s<m-\nu-\nu_0, \\ O(m) & if \quad p=2,\ \nu_0<\nu,\ \nu_2(h)<m-2\nu, \\ 4p^{\frac{m+s}{2}} & if \quad \nu_0 \geqslant \nu,\ s<m-2\nu, \\ \tau & else. \end{cases}$$

The constants implied by the O-symbol are absolute. ■

As we said in above, the equidistribution and statistical independency properties of pseudo-random numbers can be analyzed based on the discrepancy of certain point sets in the unit s-dimensional ball.

Theorem 3. *Let $p \equiv 3 \pmod 4$ be a prime number, $z_0, \alpha, \beta, \gamma \in G$, $0 \leqslant \arg z_0 < \frac{\pi}{2}$, $0 \leqslant \arg\alpha, \arg\beta, \arg\gamma < \frac{\pi}{4}$, and let $0 = \nu_p(\alpha) < \nu_p(\beta) < \nu_p(\gamma)$, $\alpha \not\equiv z_0^2 \pmod p$. Then for the sequence W_k, $W_k = \frac{Z_k}{p}$, $Z_k = (z_k, z_{k+1}, \dots, z_{k+s})$, $k = 0,1,2,\dots$, where are given by recursion (3) whith period $\tau = 2p^{m-\nu}$, $\nu = \nu_p(\beta)$, the discrepancy $D_N^{(s)} = (W_0, W_1, \dots, W_{N-1})$ satisfies inequality*

$$D_\tau^{(s)} \leqslant 2p^{-m+2\nu}\left(\frac{1}{\pi}\log p^{2(m-\nu)} + \frac{3}{5}\right)^3 + 2p^{-2(m+\nu)}.$$

Proof. For $s = 1$ we apply the analogical reasoning as in the proof of Theorem 4 [4] and take into account the result from Theorem 2. Then we derive at once our assertion.

If $s \geqslant 2$ we simply get the inequality (see, the proof of Theorem 1 with $M = p^m$ in above)

$$D_N^{(s)}(X_0, X_1, \ldots, X_{N-1}) \leqslant$$

$$\leqslant \frac{s}{p^m} + \frac{1}{p^m} \sum_{\substack{\overline{h} \in G_{p^m}^s \\ \overline{h} \neq (0,\ldots,0)}} \prod_{i=1}^{s} \min\left(\frac{1}{|\sin \pi \Re h_0|}, \frac{1}{|\sin \pi \Im h_i|}\right) \leqslant$$

$$\leqslant \frac{s}{p^m} + \frac{1}{p^m} \sum_{\substack{\overline{h} \in G_{p^m}^s \\ \overline{h} \neq (0,\ldots,0)}} \min\left(\frac{1}{|\sin \pi \Re h_i|}, \frac{1}{|\sin \pi \Im h_i|}\right) \frac{1}{N} \left(|S_N^{(s)}| + O\left(N^{\frac{1}{2}}\right)\right),$$

where $S_N^{(s)} = \sum\limits_{n=0}^{N-1} e_{p^m}(\Re \sum\limits_{i=1}^{s} h_i z_{n+i-1})$.

Next, following to argument from Theorem 5[4], we derive the assertion of our theorem for $s = 2, 3, 4$. ■

Conclusion. Theorems proved above show that some methods of construction of nonlinear congruential generators of the pseudo-random real numbers can be used in problems generating of the complex pseudo-random numbers.

1. **Baker R. C.** Diophantine Inequalities / R. C. Baker. – LMS Monographs New Series, Book 1, Oxford University Press, 1986. – 250 p.
2. **Drmota M.** Sequences, discrepancies and applications / M. Drmota, R. F. Tichy. – Berlin : Springer-Verlag, 1997. – 506 p.
3. **Hellekalen P.** General discrepancy estimates the Walsh function system / P. Hellekalen // Acta Arithm. – 1994. – V. 67. – P. 209–218.
4. **Varbanets P.** Generalizations of Inversive Congruential Generator / P. Varbanets, S. Varbanets // 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.