ISSN 2304-1579. Visnyk Odesk. Nats. Univers. Mat. i Mekh.–2014 .–V.19,Is.1(21).–P.71–80

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

S. Varbanets
I. I. Mechnikov Odesa National University

SEQUENCES OF PRN'S PRODUCED BY CIRCULAR GENERATOR

Варбанець С. П. Послідовності ПВЧ, породжені циклічним генератором. Ми досліджуємо послідовність псевдовипадкових чисел (абревіатура: ПВЧ), породжену конгруентним генератором, ассоційованим із групою точок цілих гаусових чисел, норми яких порівняні (конгруентні) з $\pm 1 \pmod{p^m}$, де $p \equiv \pmod 4$ — просте число. Ці точки утворюють "нормену" підгрупу у групі класів вичитів $\mathbb{Z}[i]/p^m$ і ця група циклічна. Породжувальна послідовність ПВЧ проходить s-мірний тест на рівномірність та статистичну незалежність.
Ключові слова: псевдовипадкові числа, дискріпансія, експоненціальні суми.

Варбанец С. П. Последовательности ПСЧ, порождённые циклическим генератором. Мы исследуем последовательность псевдослучайных чисел (аббревиатура: ПСЧ), порождённую конгруэнтным генератором, ассоциированным с группой точек целых гауссовых чисел, нормы которых сравнимы (конгруэнтны) с $\pm 1 \pmod{p^m}$, где $p \equiv \pmod 4$ — простое число. Эти точки образуют "норменную"подгруппу в группе классов вычетов $\mathbb{Z}[i]/p^m$ и эта группа циклична. Порождаемая последовательность ПСЧ проходит s-мерный тест на равномерность и статистическую независимость.
Ключевые слова: псевдослучайные числа, дескрипансия, экспоненциальные суммы.

Varbanets S. Sequences of PRN's produced by circular generator. We investigate the sequence of pseudorandom numbers (abbreviation: PRN) produced by congruential generator that associated with the group of points of the gaussian integers with norms comparing (congruent) with $\pm 1 \pmod{p^m}$, where $p \equiv \pmod 4$ is a prime number. These points produce norm subgroup over the residue classes group $\mathbb{Z}[i]/p^m$ and this group is a cyclic. The generated sequence of PRN's passes s-dimensional test on equidistribution and statistical independency.
Key words: pseudo-random numbers, discrepancy, exponential sum.

Introduction. The sequence of real numbers $\{a_n\}$, $0 \leqslant a_n < 1$, we call the sequence of pseudorandom numbers (arbitrary, 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 $[0, 1)$. More acceptable sequences of PRN's generate by the congruential recursion

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

where $y_0, y_1, \dots, y_{k-1} \in \{0, 1, \dots, m-1\}$, $f(u_1, \dots, u_k)$ is integer function over $\mathbb{Z}_m^k$.

In case $f \in \mathbb{Z}_m[u_1, \dots, u_k]$ we have the congruential polynomial generator of periodical sequence $\{y)n\}$ with a period τ, $\tau \leqslant m$.

It emerged that linear function $f(u) = au + b$ does not supply requirements of "affinity" to statistical independency (unpredictability) (see, for example [11]).

But quadratic function $f(u) = au^2 + bu + c$ satisfies to condition of "practical" unpredictability (see [8]).

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

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

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

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

The inversive generator (2) and its generalization was being investigated by many authors (see [3]–[10], [14]–[18]). Starting out from our reasoning we will call such inversive generator as hyperbolical.

To apply the sequence $\{y_n\}$ in cryptography it is necessary to carry-out the requirement of secrecy as well. That means providing the impossibility to restore the generator parameters by single values of sequence elements. There are some interesting researches about this area (see, [1]–[4], [9], [10]). In the paper [18] there are being investigated the analogues of inversive congruential generators, that without any increases of computational complexity of finding the elements of sequence $\{y_n\}$, get essential complexity for intruder's work around parameters of inversive or linear generator to be recovered.

Let $p \equiv 3 \pmod 4$ be a prime rational number, m be a natural. Denote G the ring of gaussian integers, $G = \{a + bi : a, b \in \mathbb{Z},\ i^2 = -1\}$, and G_{p^m} (accordingly, $G^*_{p^m}$) the ring of residue classes (accord., multiplicative group of this ring modulo p^m) over G.

Let

$$E_m := \left\{\alpha \in G^*_{p^m} :\ N(\alpha) \equiv \pm 1 \pmod{p^m}\right\}.$$

It easy to check, that E_m is a subgroup in $G^*_{p^n}$ with order $2(p+1)p^{m-1}$, that we call the norm group over the ring G_{p^m}. As far as E_m is a cyclic group, it means that every generated element $u + iv$ defines two sequences of integer numbers modulo p^m:

$$Z_n = \Re((u+iv)^n) \qquad and \quad W_n = \Im((u+iv)^n),\ \ n = 1, 2, \ldots.$$

We considered in [19] the sequence $\left\{\frac{aZ_n + bW_n}{p^m}\right\}$, $n = 1, 2, \ldots$, and there were shown that this congruence are uniformly distributed on $[0, 1)$. The main point of this work is to prove that the sequence $\left\{\frac{\Re(u+iv)^{2(p+1)n+k} \cdot \Im(u+iv)^{2(p+1)n+k}}{p^m}\right\}$ also is an uniformly distributed sequence on $[0, 1)$.

Auxiliary arguments. Before studying the sequences of PRN's produced by circular generator, we standardize some notations to be used throughout this paper.

Lower case Roman (respectively, Greek) letters usually denote rational (respectively, Gaussian) integers; inparticular, m, n, k are positive integers and p is always a rational prime number $p \equiv 3 \pmod 4$, γ stands for the Gaussian odd prime number. We also define a *norm* over $\mathbb{Q}(i)$ 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_γ) denotes the ring of residue classes modulo q (respectively, $\gamma \in G$), and $\mathbb{Z}_q^*$ (or G_γ^*) denotes the multiplicative group in $\mathbb{Z}$ (or G_γ). If $x \in G_\gamma^*$ we write x^{-1} for the multiplicative inverse of

$x \bmod \gamma$, i. e. x^{-1} is an arbitrary Gaussian integer sutysfying the condition $xx^{-1} \equiv 1 \pmod{\gamma}$. As usual, $gcd(a,b)$ or (a,b) stand for the greater common divisor of 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 $p^{\nu(a)} | a$, $p^{\nu(a)+1} \not| a$.

Before starting out the study of the sequences $\{Z_n\}$ and $\{W_n\}$ we need several lemmas being used in sequel.

Lemma 1. *Let* $f(\xi) = \alpha_1\xi + \alpha_2\xi^2\mathfrak{p} + \alpha_3\xi^3\mathfrak{p}^{\nu_3} + \cdots + \alpha_k\xi^k\nu_{\mathfrak{k}}$, *where* $\nu_3, \nu_4, \ldots, \nu_k, n \geqslant 2$ *be positive integers,* $\alpha_1, \ldots, \alpha_k \in G$, $(\alpha_2, \mathfrak{p}) = \cdots = (\alpha_k, \mathfrak{p}) = 1$. *Then we have*

$$|S(f, \mathfrak{p}^n)| \leqslant \begin{cases} 0 & if \quad \mathfrak{p} \neq 1+i, \ (\alpha_1, \mathfrak{p}) = 1 \\ & or \quad \mathfrak{p} = 1+i, \ \alpha_1 \not\equiv 0 \pmod{\mathfrak{p}^2}, \\ N(\mathfrak{p})^{\frac{n+1}{2}} & if \quad \mathfrak{p} \neq 1+i, \ \alpha_1 \equiv 0 \pmod{\mathfrak{p}}, \\ 2^{\frac{n+3}{2}} & if \quad \mathfrak{p} = 1+i, \ \alpha_1 \equiv 0 \pmod{2}. \end{cases}$$

Proof. For $n = 2$ the estimated sum is the Gaussian sun, and thus in such case our assertion holds.

For $n \geqslant 3$, $\mathfrak{p}$ be a odd prime. We put

$$\xi = \eta + \mathfrak{p}^{n-1}\zeta, \ \eta \in G_{\mathfrak{p}^{n-1}}, \ \zeta \in G_{\mathfrak{p}}.$$

Taking into account that $\xi^k = \eta^k + k\eta^{k-1}\zeta \pmod{\mathfrak{p}^{n-1}}$, we get

$$S(f, \mathfrak{p}^n) = \sum_{\eta \in G_{\mathfrak{p}^{n-1}}} e^{2\pi i \Re\left(\frac{f(\eta)}{\mathfrak{p}^n}\right) \Re\left(\frac{\alpha_1 + 2\alpha_2\eta}{\mathfrak{p}}\zeta\right)} = N(\mathfrak{p}) \sum_{\substack{\eta \in G_{\mathfrak{p}^{n-1}} \\ \alpha_1 + 2\alpha_2\eta \neq 0 \pmod{\mathfrak{p}}}} e^{2\pi i \Re\left(\frac{f(\eta)}{\mathfrak{p}^n}\right)}.$$

Let $\alpha_1 + 2\alpha_2\eta_0 \equiv 0 \pmod{\mathfrak{p}}$, $\eta_0 \in G_{\mathfrak{p}}^*$. We put $\eta = \eta_0 + \mathfrak{p}\xi$, $\xi \in G_{\mathfrak{p}^{n-2}}$. Then we infer

$$f(\eta_0 + \mathfrak{p}\xi) = f(\eta_0) + \mathfrak{p}(\alpha_1 + 2\alpha_2\eta_0)\xi + \mathfrak{p}^2\alpha_2'\xi^2 + \cdots = f(\eta_0) + \mathfrak{p}^2 f_1(\xi),$$

where the polynomial $f_1(\xi)$ has such type as $f(\xi)$.

So, after $\left[\frac{n}{2}\right]$ steps we obtain

$$|S(f, \mathfrak{p}^n)| = \begin{cases} N(\mathfrak{p})^{\frac{n}{2}} & if \quad n \ is \ even, \\ N(\mathfrak{p})^{\frac{n-1}{2}} \left| \sum\limits_{\xi \in G_{\mathfrak{p}}} e^{2\pi i \Re\left(\frac{\beta_1 + \beta\xi^2}{\mathfrak{p}}\right)} \right| & if \quad n \ is \ odd. \end{cases}$$

By the estimate of the Gauss sum we have the assertion of Lemma.

The case $\mathfrak{p} = 1 + i$ can be considered similarly. ■

Corollary 1. *Let* $f(\xi) = \alpha\xi + \beta\xi^2 + \mathfrak{p}(\gamma\xi^2 + \cdots)$ *be a polynomial over* G, *and let* $(\beta, \mathfrak{p}) = 1$. *Then for any* $\delta \in G$, *we have*

$$\left| \sum_{\xi \in G_{\mathfrak{p}^n}^*} e^{2\pi i \Re\left(\frac{f(\xi) + \delta\xi^{-1}}{\mathfrak{p}^n}\right)} \right| \leqslant 2N(\mathfrak{p})^{\frac{n}{2}}.$$

Indeed, putting $\xi = \eta + \mathfrak{p}^{n-1}\zeta$, $\eta \in G^*_{\mathfrak{p}^{n-1}}$, $\zeta \in G_{\mathfrak{p}}$, and observing that $\xi^{-1} = \eta^{-1} - \mathfrak{p}^{n-1}\xi(\eta^{-1})^2$, where η^{-1} be a multiplicative inverse mod$\mathfrak{p}^n$ for η, we immediately infer that inequality holds by Lemma 1.

Similarly, assertion holds for the same exponential sums over $\mathbb{Z}_{p^n}$.

Let us denote by E_m the following subgroup of $G^*_{p^m}$, $p \equiv 3 \pmod 4$, p be a prime number in $\mathbb{Z}$:

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

The subgroup E_m^+ we will call the norm group in $G^*_{p^m}$.

Take into account that the multiplicative group of the field G_p is a cyclic group. It is easy to prove (as in $\mathbb{Z}^*_{p^m}$) that it exists a generating element of the group E_1^+, such that it will generate every group E_m^+, $m > 1$.

In order to find that element, we take such generating element g_0 of group G_p^* for which $g_0^{(p+1)p} = 1 + hp^2$ with $(h, p) = 1$. Then g_0^{p-1} is revealed generating element of group E_m^+, $m = 1, 2, \ldots$.

Moreover, we have

Lemma 2. *Let us $u+iv \in E_m$ be a generating element of E_m. Then* $\operatorname{ord}(u+iv) = |E_m| = 2(p+1)p^{m-1}$ *and*

$$\begin{aligned} &(u+iv)^{2(p+1)} = 1 + p^2 x_0 + ipy_0, \\ &x_0 + 2y_0^2 \equiv 0 \pmod p, \ (x_0, p) = (y_0, p) = 1, \end{aligned}$$

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

$$\begin{aligned} \Re(u+iv)^{2(p+1)t} &= A_0 + A_1 t + A_2 t^2 + \cdots + A_{m-1} t^{m-1}, \\ \Im(u+iv)^{2(p+1)t} &= B_0 + A_1 t + B_2 t^2 + \cdots + B_{m-1} t^{m-1}, \end{aligned} \tag{3}$$

where

$$\begin{cases} A_0 \equiv 1 \pmod{p^4}, \ B_0 \equiv 0 \pmod{p^4}, \\ A_1 \equiv p^2 x_0 + \frac{1}{2} p^2 y_0^2 \equiv 0 \pmod{p^3}, \ B_1 \equiv py_0 \pmod{p^3}, \\ A_2 \equiv -\frac{1}{2} p^2 y_0^2 \pmod{p^3}, \ B_2 \equiv 0 \pmod{p^3}, \\ A_j \equiv B_j \equiv 0 \pmod{p^3}, \ j = 3, 4, \ldots m-1. \end{cases} \tag{4}$$

■

Denote

$$\begin{aligned} (u+iv)^{2k} &= u(k) + iv(k), \ 0 \leqslant k \leqslant p, \\ (u+iv)^{2(p+1)t+2k} &\equiv \sum_{j=0}^{m-1} (A_j(k) + iB_j(k))\, t^j \pmod{p^m}. \end{aligned}$$

It is clear

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

Thus from Lemma 1 we have

Corollary 2. *For $k = 1, 2, \ldots, p$, we have*

$$u(k) \equiv u(-k),\ v(k) \equiv -v(-k) \pmod{p^m},$$
$$(u(k), p) = (v(k), p) = 1,\ \textit{if } k \neq \frac{p+1}{2}, \frac{3(p+1)}{2},$$
$$u(0) = 1,\ v(0) = 0,$$
$$u(k) \equiv 0 \pmod{p},\ (v(k), p) = 1,\ \textit{if } k = \frac{p+1}{2}, \frac{3(p+1)}{2}.$$

Moreover, for $k \neq \frac{p+1}{2}, \frac{3(p+1)}{2}$

$$A_0(k) \equiv u(k),\ B_0(k) \equiv v(k) \pmod{p},$$
$$p||A_1(k),\ p||B_1(k),\ p^2||A_2(k),\ p^2||B_2(k)$$

and

$$A_0(0) \equiv 1,\ B_0(0) \equiv 0,$$
$$A_1(0) \equiv 0 \,(\mathrm{mod}\ p^4),\ B_1(0) \equiv py_0 \,(\mathrm{mod}\ p^4),\ p^2||A_2(0),\ B_2(0) \equiv 0 \,(\mathrm{mod}\ p^3),$$
$$A_0(p+1) \equiv -1 \pmod{p^3},\ B_0(p+1) \equiv 0 \pmod{p^3},$$
$$A_0(k) \equiv 0,\ B_0(k) \equiv 0 \pmod{p},$$
$$p||A_1(k),\ p^2||B_1(k),\ p^2||A_2(k),\ B_2(k) \equiv 0 \pmod{p^3}\ \textit{if } k = \frac{p+1}{2}, \frac{3(p+1)}{2},$$

moreover,

$$A_j(k) \equiv B_j(k) \equiv 0 \pmod{p^3},\ k = 0, 1, \ldots, 2p+1,\ j \geqslant 3.$$

In view the congruence

$$(u + iv)^{p+1} = 1 + p^2 x_0 + iy_0,$$
$$(x_0, p) = (y_0, p) = 1,$$
$$2x_0 + y_0^2 \equiv 0 \pmod{p},$$
$$u^2 + v^2 \equiv +1 \pmod{p^m},$$

the proof of Corollary 2 is a simple exercise and we omit.

Main Results

Circular generator of PRN's. We select a random number k from $\{0, 1, 2, \ldots, p-1\}$ and consider the sequence $\{(u + iv)^{2(p+1)n+2k}\}$, $n = 0, 1, \ldots, p^{m-1} - 1$, where $u + iv$ is a generating element of E_m.

Denote

$$Z_n(k) = Z_n = \Re\Big((u + iv)^{2(p+1)n+2k}\Big),$$
$$W_n(k) = W_n = \Im\Big((u + iv)^{2(p+1)n+2k}\Big).$$

The description of this sequences there is in Lemma 2. We saw that $(u + iv)^{2(p+1)} = u_0 + iv_0$, where $u_0 = 1 + p^2 x_0$, $v_0 = y_0$, $(x_0, p) = (y_0, p) = 1$ and $x_0 + 2y_0^2 \equiv 0 \pmod{p}$.

Hence,

$$\begin{aligned} Z_{n+1} &\equiv \Re((u_0+iv_0)^n\cdot(u_0+iv_0)\cdot(u(k)+iv(k)))\equiv \\ &\equiv Z_nu_0-W_tv_0 \pmod{p^m}, \end{aligned} \tag{5}$$

$$W_{n+1}\equiv Z_tv_0+W_tu_0 \pmod{p^m} \tag{6}$$

for $n=0,1,\dots,p^{m-1}-1$.

The sequence (5) and (6) satisfies that condition

$$Z_n^2+W_n^2\equiv 1 \pmod{p^n}$$

for any $n\in\mathbb{Z}_{p^{n-1}}$ and $k\in\{0,1,\dots,p\}$.

Thus we call the sequences (5) and (6) circular sequences of PRN's.

Let $X_n^{(k)}:=X_n=\frac{Z_n}{W_n}$.

Theorem 1. *For* $k\in\{0,1,\dots,2p+1\}\diagdown\left\{0,\frac{p+1}{2},p+1,\frac{3(p+1)}{2}\right\}$ *we have*

$$S_X(A,p^m)=\sum_{n\in\mathbb{Z}_{p^m-1}} e_{p^m}(AX_n)\ll 2p^{\frac{m}{2}} \tag{7}$$

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

Proof. From Corollary we infer

$$X_n=c_0(k)+c_1(k)n+c_2(k)n^2+\cdots,$$

where

$$\begin{aligned} c_1(k)&=py_0(1-2v^2(k))=py_0(3+2u^2(k)),\\ c_2(k)&\equiv x_0(p^2)-\frac{5}{3}u(k)v^{-1}(k)x_0y_0p^3-u(k)v(k)^{-2}p^2y_0^2\equiv\\ &\equiv p^2x_0(-1+2u-u^2)\equiv -p^2x_0(1-u)^2 \pmod{p^3},\\ c_j(k)&\equiv 0 \pmod{p^3},\ j\geqslant 3. \end{aligned} \tag{8}$$

Noting that the congruences

$$\begin{aligned} 3+2u^2(k)&\equiv 0 \pmod p,\\ 1-u(k)&\equiv 0 \pmod p, \end{aligned}$$

cannot be realized simultaneously, we, by Lemma 1 (for rational case), obtain the statement of theorem. ■

Corollary 3. *For* $1<N<p^{m-1}$ *and any* $k\in\{0,1,\dots,p\}$

$$\left|\sum_{n=0}^{N-1} e^{2\pi i\frac{aZ_n(k)+bW_n(k)}{p^m}}\right|\leqslant 2p^{\frac{m}{2}}\log p^m. \tag{9}$$

Indeed, the inequality (9) is consequence of well-known estimate of incomplete sum by complete sum. ■

Theorem 2. *Let s be positive integer, $h_1, \dots, h_s \in \mathbb{Z}_{p^m}$, $(h_1, \dots, h_s, p) = 1$. Then for $s \in \{1, 2, \dots, p-1\}$ the following estimate*

$$S(h_1, \dots, h_s) = \sum_{n=0}^{p^{m-1}-1} e_{p^m}(h_1 X_n + h_2 X_{n+1} + \dots + h_s X_{n+s-1}) \ll p^{\frac{m}{2}}$$

holds (with an absolute constant depending only on s).

Proof. Using (8) and calculating coefficients for n and n^2 in presentation $h_1 x(n) + h_2 x(n+1) + \dots + h_s x(n+s-1)$ as a polynomial of n or $(n+1)$,..., or $n+s-1$, we obtain (by Lemma 1) that $S(h_1, \dots, h_s) \neq 0$ only if $3 + 2u^2(k) \equiv 0 \pmod p$. In such case we estimate the sum $S(h_1, \dots, h_s)$ as $O\left(p^{\frac{m}{2}}\right)$ with the absolute constant in symbol "O". In other cases this sum is zero. ■

Corollary 4. *In the conditions of Theorem 2 we have*

$$\sum_{n=0}^{N-1} e_{p^m}(h_1 X_n + h_2 X_{n+1} + \dots h_s X_{n+s-1}) \ll p^{\frac{m}{2}} \log p^m.$$

Discrepancy bound. Consider the sequence $\{X_n\}$, $n = 0, 1, 2, \dots$ of the elements of $\mathbb{Z}_{p^m}$ defined above. Let $\{Y_n\}$ be a sequence of PRN's in interval $[0, 1)$ obtained by the normalization $Y_n = \frac{X_n}{p^m}$,

The sequence $\{y(n)\}$, $n = 0, 1, \dots$, is purely periodic with the period length $\tau = p^{m-1}$.

Equidistribution and statistical independency properties of pseudorandom numbers can be analyzed based on the discrepancy of certain point sets in $[0, 1)^s$.

Besides the discrepancy, there exist other important criteria for the uniformity and independence of PRN's. We will restrict our attention to the discrepancy, since it is the most important measure of uniformity and independence in connection with PRN's.

For N arbitrary points, $x_0, x_1, \dots, x_{N-1} \in [0, 1)^d$, the discrepancy is defined by

$$D_N(x_0, x_1, \dots, x_{N-1}) = \sup_{I \subset [0,1)^d} \left| \frac{A_N(I)}{N} - |I| \right|, \tag{10}$$

where the supremum is extended over all subintervals I of $[0, 1)^d$, $A_N(I)$ is the number of points among $x_0, x_1, \dots, x_{N-1}$ falling into I, and $|I|$ denotes the d-dimensional volume of I.

Our goal is to obtain a nontrivial discrepancy estimate for a part of period for the circular generators of pseudorandom numbers. In particular, we shall estimate discrepancy for the sequence $\{\omega_\ell\}$, $\omega_\ell = \frac{x_\ell}{p^m}$, $\ell \geqslant 0$ and for the sequence $\{\Omega_\ell\}$, $\Omega_\ell = (\omega_\ell, \omega_{\ell+1}, \dots, \omega_{\ell+s-1})$, $\ell \geqslant 0$, $s \geqslant 2$. Well-known that a small value $D(\omega_0, \omega_1, \dots, \omega_{N-1})$ guarantees an uniform distribution $\{\omega_\ell\}$, $\ell \geqslant 0$ on $[0, 1)$, and a small value $D(\Omega_0, \Omega_1, \dots, \Omega_{N-1})$ means that the sequence $\{\omega_\ell\}$, $\ell \geqslant 0$, pass the two-dimensional serial test on the statistical independence properties of this sequence. In the cryptographical applications the property of statistical independence means that the circulate congruential pseudorandom sequence $\{x_\ell\}$, $\ell \geqslant 0$, is unpredictable.

In the following, some further notation is necessary.

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

$$r(h,q) = \begin{cases} 1 & if\ h = 0, \\ q \sin(\pi \frac{|h|}{q}) & if\ h \neq 0, \end{cases}$$
$$r(\mathbf{h},q) = \prod_{j=1}^{d} r(h_j, q). \tag{11}$$

Moreover, several auxiliary results are given.

Lemma 3. *Let $N \geqslant 1$ and $q \geqslant 2$ be integers. Suppose that $\mathbf{y_0}, \mathbf{y_1}, \dots, \mathbf{y_{N-1}} \in \mathbb{Z}_q^d$. Then the discrepancy of the points $\mathbf{t}_\ell = \frac{\mathbf{y}_\ell}{q} \in [0,1)^d$, $\ell = 0, 1, \dots, N-1$, satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \leqslant \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \frac{1}{r(\mathbf{h},q)} \left| \sum_{\ell=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_\ell) \right| \tag{12}$$

(Proof see in [13], Theorem 3.1).

Lemma 4. *Let T be the period of the sequence $\{\mathbf{y_k}\}$, $T \geqslant N \geqslant 1$ and $q \geqslant 2$ be integers, $\mathbf{y_k} \in \{0, 1, \dots, q-1\}^d$ for $k = 0, 1, \dots, N-1$; $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0,1)^d$. Then*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \leqslant \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(\mathbf{h},q) r(h_0, T)} \times$$
$$\times \left| \sum_{k=0}^{T} e(\mathbf{h} \cdot \mathbf{t_k} + \frac{k h_0}{T}) \right|. \tag{13}$$

This assertion follows from Lemma 3 and from an estimate of uncomplete exponential sum through complete exponential sum.

Now it easy to prove the following theorems.

Theorem 3. *Let $p \equiv 3 \pmod 4$ be a prime number and let the sequence produced by circular generator (5)–(6) has a view $X_n = \frac{\Re\left((u+iv)^{2(p+1)n+k}\right)}{\Im\left((u+iv)^{2(p+1)n+k}\right)}$. Then we have for $k \not\equiv 0 \pmod{\frac{p+1}{2}}$*

$$D_N\left(\frac{X_0}{p^m}, \frac{X_1}{p^m}, \dots, \frac{X_{N-1}}{p^m}\right) \leqslant \frac{1}{p^m} + \frac{2p^{\frac{m}{2}}}{N} \left(\frac{1}{p}\left(\frac{2}{\pi} \log p^m + \frac{7}{5}\right)^2 + 1\right),$$

where $1 \leqslant N \leqslant p^{m-1} - 1$.

Theorem 4. *Let T_n, $n = \{0, 1, \dots, p^{m-1}+1\}$ be a sequence of points $T_n \in [0,1)^s$, $T_n = (X_n^{(k)}, X_{n+1}^{(k)}, \dots, X_{n+s-1}^{(k)})$. Then for $N \leqslant p^{m-1}-1$, $k \not\equiv 0 \pmod{\frac{p+1}{2}}$, $s \leqslant p-1$*

$$D_N^{(s)} := D_N(T_0, T_1, \dots, T_{N-1}) \leqslant \frac{s}{p^m} + \frac{1}{p^{\frac{m-1}{2}}} \left(1 + \frac{1}{p}\left(\frac{2}{\pi} \log p^m + \frac{7}{5}\right)^s\right).$$

The proof of these theorems follow from the estimates of theorems 1 and 2 and their corollaries.

From Theorem 3 and 4 it follows that the sequences $\{\Re\big((u+iv)^{2(p+1)\ell+2k}\big)\}$ and $\{\Im\big((u+iv)^{2(p+1)\ell+2k}\big)\}$ are equidistributed and pass s-dimensional test on unpredictability.

Conclusion. By congruence $N(w) \equiv 1 \pmod{p^m}$ over the ring of Gaussian integers $\mathbb{Z}[w]$, we obtained the circle that produces a big family of circular generators. The description of solution obtained above for such congruence allows to construct new types of congruential generators. Also, this solution make possible to investigate quite efficiently the related sequences of PRN's on equidistribution and unpredictability in terms of exponential sums.

1. **Blackburn S. R.** Predicting nonlinear pseudorandom number generators / S. R. Blackburn, D. Gomez-Peres, I. Gutierrez, I. Shparlinski // Math. Comp. – 2004. – Vol. 74 (251). – P. 1471–1494.
2. **Blackburn S. R.** Reconstructing noisy polynomial evaluation in residue rings / S. R. Blackburn, D. Gomez-Peres, I. Gutierrez, I. Shparlinski // J. of Algorithm. – 2006. – Vol. 61 (2). – P. 47–59.
3. **Eichenauer-Herrmann J.** Inversive congruential pseudorandom numbers: a tutorial / J. Eichenauer-Herrmann // Internat. Statist. Rev. – 1992. – Vol. 60. – P. 167–176.
4. **Eichenauer-Herrmann J.** Pseudorandom number generation by nonlinear methods / J. Eichenauer-Herrmann // Internat. Statist. Rev. – 1995. – Vol. 63. P. 247–255.
5. **Eichenauer-Herrmann J.** A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus / J. Eichenauer-Herrmann, H. Grothe // ACM Transactions of Modelling and Computer Simulation. – 1992. – Vol. 2(1). – P. 1–11.
6. **Eichenauer J.** A non-linear congruential pseudorandom number generator / J. Eichenauer, J. Lehn // Statist. Hefte. – 1986. – Vol. 27. – P. 315–326.
7. **Eichenauer J.** A nonlinear congruential pseudorandom number generator with power of two modulus / J. Eichenauer, J. Lehn, A. Topuzoğlu // Math. Comp. – 1988. – Vol. 51. – P. 757–759.
8. **Eichenauer-Herrmann J.** A survey of quadratic and inversive congruential pseudorandom numbers / J. Eichenauer-Herrmann, E. Herrmann, S. Wegenkittl // Monte Carlo and Quasi-Monte Carlo Methods, H. Niederreiter et al (eds.), Lecture Notes in Statist. – 127, Springer, New York, 1998. – P. 66–97.
9. **Eichenauer-Herrmann J.** On the period of congruential pseudorandom number sequences generated by inversions / J. Eichenauer-Herrmann J., A. Topuzoğlu // J. Comput. Appl. Math. – 1990. – Vol. 31. P. 87–96.
10. **Kato T.** On a nonlinear congruential pseudorandom number generator / T. Kato, L. M. Wu, N. Yanagihara // Math. of Comp. – 1996. – Vol. 65. (213). – P. 227–233.
11. **Knuth D. E.** The Art of Computer Programming, Vol. 2: Seminumerical algorithms, Addison-Wesley, 1998.

12. **Niederreiter H.** Nonlinear methods for pseudorandom number and vector generation, Simulation and Optimization (G. Pflug and U. Dieter, eds.) // Lecture Notes in Econom. and Math. Systems, Springer, Berlin, – 1992. – Vol. 374. – P. 145–153.

13. **Niederreiter H.** Random Number Generation and Quasi-Monte Carlo Methods. SIAM, Philadelphia, Pa., 1992.

14. **Niederreiter H.** Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus / H. Niederreiter, I. Shparlinski // Acta Arith. – 2000. – Vol. 90 (1). P. 89–98.

15. **Varbanets S.** Exponential sums on the sequences of inversive congruential pseudorandom numbers / S. Varbanets // Šiauliai Math. Semin. – 2008. – Vol. 3 (11). P. 247–261.

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

17. **Varbanets P.** Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus / P. Varbanets, S. Varbanets // Voronoy's Impact on modern science, Proceedings of the 4^{th} International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine. – September 22–28, 2008. – P. 112–130.

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

19. **Varbanets P.** Circular generator of PRN's / P. Varbanets, S. Varbanets // Proceedings, The 7th CHAOS2014 International Conference, 7–10 June 2014, Lisbon Portugal, 2014, to appear.