ISSN 2304-1579. Visnyk Odesk. Nats. Univers. Mat. i Mekh.–2014 .–V.19,Is.2(22).–P.87–??

Mathematical Subject Classification: 11L07, 11K45, 11T23, 11T71, 45B67
UDC 511

Tran The Vinh
Odesa I. I. Mechnikov National University

LINEAR-INVERSIVE CONGRUENTIAL GENERATOR OF PRN'S

Чан Тхе Вінь. Лінійно-інверсний конгруентний генератор ПВЧ. Інверсний конгруентний метод генерування рівномірно розподілених псевдовипадкових чисел є особливо привабливою альтернативою лінійним конгруентним генераторам, які володіють низкою небажаних закономірностей. В даній статті розглядається новий лінійно-інверсний конгруентний генератор за модулем степеню простого числа. Даються оцінки тригонометричних сум для лінійно-інверсних конгруентних псевдовипадкових чисел. Результати показують, що ці інверсні конгруентні псевдовипадкові числа проходять s-мірний серіальний тест на статистичну незалежність.
Ключові слова: інверсні конгруентні псевдо-випадкові числа, експоненційні суми, дискріпансія.

Чан Тхе Винь. Линейно-инверсный конгруэнтный генератор ПСЧ. Инверсный конгруэнтный метод генерирования равномерно распределённых псевдослучайных чисел является особенно привлекательной альтернативой линейным конгруэнтным генераторам, которые обладают рядом нежелательных закономерностей. В настоящей статье рассматривается новый линейно-инверсный конгруэнтный генератор по модулю степени простого числа. Даются оценки тригонометрических сумм для линейно-инверсных конгруэнтных псевдослучайных чисел. Результаты показывают, что эти инверсные конгруэнтные псевдослучайные числа проходят s-мерный сериальный тест на статистическую независимость.
Ключевые слова: инверсные конгруэнтные псевдо-случайные числа, экспоненциальные суммы, дескрипансия.

Tran The Vinh. Linear-inversive congruential generator of PRN's. The inversive congruential method for generating uniform pseudorandom numbers is a particulary attractive alternative to inversive congruential generators, which show many undesirable regularities. In the present paper a new linear-inversive congruential generator with prime-power modulus is introduced. Exponential sums on linear-inversive congruential pseudorandom numbers are estimates. The results show that these inversive congruential pseudorandom numbers pass s-dimensional serial tests on the statistical independence.
Key words: inversive congruential pseudorandom numbers, exponential sum, discrepancy.

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

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

where y_n^{-1} 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 the works of Eichenauer, Lehn, Topuzoğlu [5], Niederreiter, Shparlinski [9], Eichenauer, Grothe [4] ets. were proved that the inversive congruential generator (1) produces the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$, $n = 0, 1, 2, \ldots$, which passes s-dimensional serial tests on equidistribution and statistical independence for $s = 1, 2, 3, 4$ if the defined conditions on relative parameters a, b, y_0 are accomplishable.

It was proved that this generator is extremely useful for Quasi-Monte Carlo type application (see, [7–9]). The sequences of PRN's can be used for the cryptographic applications. Now the initial value y_0 and the constants a and b are assumed to be secret key, and then we use the output of the generator (1) as a stream cipher. By the works [1], [2] it follows that we must be careful in the time of using the generator (1).

In the current paper we give generalization of the generator (1). This generalization is based on the recurrence relation

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

under conditions

$$(c_n, p) = (y_0, p) = 1, \ \ b \equiv a \equiv 0 \pmod{p}.$$

We call the generator (2) the linear-inversive congruential generator. The computational complexity of generator (2) is the same as that for the generator (1), but the reconstruction of parameters a, b, c, y_0 is a tricky problem even if several consecutive values $y_n, y_{n+1}, \ldots, y_{n+N}$ are revealed. Thus the generator (2) can be used in cryptographical applications. Notice that the conditions $(c_n, p) = (y_0, p) = 1$, $b \equiv a \equiv 0 \pmod{p}$ guarantee that the recursion (2) produces an infinite sequence $\{y_n\}$.

T. Kato, L.-M. Wu and N. Yanagihara [6] studied a nonlinear congruential pseudorandom numbers generator with modulus 2^m of the form

$$y_{n+1} \equiv ay_n^{-1} + b + cy_n \,(mod\ 2^m), \ (y_n, 2) = 1, \ n = 0, 1, 2, \ldots \tag{3}$$

They have obtained a condition at which sequences of the maximal length of the period are generated.

P. Varbanets and S. Varbanets [12] considered the generator (2) with conditions $(a, p) = (y_0, p) = 1$, $b \equiv c \equiv 0 \pmod{p}$ and showed that the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$ passes tests on equidistribution and statistical independence.

In present paper we investigate generator (2) under conditions $a \equiv b \equiv 0 \pmod{p}$, $(c_n, p) = 1$, $n = 1, 2, \ldots$ and show that for the sequence $\{c_n\}$ of special type according sequence $\{x_n\}$ passes tests on equidistribution and statistical independence (say, unpredictability).

It will be observed that W.-S. Chou [3] showed that for generator (1) the conditions $a \equiv 0 \pmod{p}$, $(b, p) = 1$ produce according sequence $\{y_n\}$ with a period $\tau = 1$. It is not alright for applications. Thus in our paper we introduced additional summand in order extend the period of PRN's. We will prove that the sequence $\{y_n\}$produced by (2) has reasonably large period. As well, we give the description of y_n, as the polynomial on n and initial value y_0. It makes possible to obtain an acceptable estimate for the discrepancy function D_N.

Notation. The letter p denotes a prime number, $p \geqslant 3$. For an integer $q > 1$ we denote by $\mathbb{Z}_q$ the residue ring of integers modulo q. Also, we denote $\mathbb{Z}_q^*$ the set

of invertible elements of $\mathbb{Z}_q$. We write $gcd(a,b) = (a,b)$ for notation a great common divisor of a and b. For $z \in \mathbb{Z}$, $gcd(z,p) = 1$ let z^{-1} be the multiplicative inverse of a modulo p^m. We write $\nu_p(A)$ if $p^{\nu_p(A)} | A$, $p^{\nu_p(A)+1} \nmid A$. For any $t \in \mathbb{R}$ and $q \in \mathbb{N}$ we write $exp(t) = e^t$, $e(t) = e^{2\pi i t}$, $e_q(t) = e\left(\frac{t}{q}\right)$. We denote an integer part of x by symbol $[x]$.

Auxiliary arguments. In this section we shall gather some auxiliary results which we use during the course of proof the main theorems.

Lemma 1. *Let p be a prime number and let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n, $n \geqslant 2$,*

$$f(x) = a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n,$$

where $\nu_p(a_j) \geqslant \nu_p(a_2) > 0$, $j \geqslant 3$.

Then the following estimates

$$\left| \sum_{x \in \mathbb{Z}_{p^m}} e_{p^m}(f(x)) \right| = \begin{cases} 0 & if \quad \nu_p(a_1) < \nu_p(a_2), \\ 2p^{\frac{m+\nu_p(a_2)}{2}} & if \quad \nu_p(a_1) \geqslant \nu_p(a_2) \end{cases}$$

hold.

This assertion is a corollary of the estimate of Gauss sum.

We will study the statistical properties of the sequences of PRN's by the discrepancy of the sequence of points $X_n^{(s)} = \left(\frac{y_n}{p^m}, \frac{y_{n+1}}{p^m}, \ldots, \frac{y_{n+s-1}}{p^m}\right)$, $n = 0, 1, \ldots, N-1$; $s = 1, 2, \ldots$.

For the sequence of N points $P_s = \{(\gamma_{1,n}, \ldots, \gamma_{s,n})\}$, $n = 0, 1, \ldots, N-1$ on the half-opened interval $[0,1)^s$ we denote the discrepancy $D^{(s)}(P_s)$ as

$$D^{(s)}(P_s) = \sup_{\Delta \subseteq [0,1)^s} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

where $A_N(\Delta)$ is the number of points of the sequence P_s that hits the box

$$\Delta = [\alpha_1, \beta_1) \times \cdots \times [\alpha_s, \beta_s) \subseteq [0,1)^s,$$

$|\Delta|$ is the volume of Δ and the supremum is taken over all boxes Δ.

Let $\{x_n\}$ is a sequence of numbers from $[0,1)$. Form the sequence of s-dimensional points $X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n = 1, 2, \ldots, N$. We say that $\{x_n\}$ passes s-dimensional discrepancy test if for every $j = 1, 2, \ldots, s$ the sequence $\{X_n^j\}$ has a discrepancy which tends to zero for $N \to \infty$.

Consider a point set P_s from $[0,1)^s$ for which all coordinates of all points are rational numbers of the form $\frac{a}{q}$, $0 \leqslant a < q$. Let us denote $C(q) = \left(-\frac{a}{2}, \frac{a}{2}\right] \cap \mathbb{Z}$, $C^*(q) = \{a \in C(q) | (a,q) = 1\}$. Let $C_s(q)$ (respectively, $C_s^*(q)$) be the inner product of s copies of $C(q)$ (respectively, $C^*(q)$).

Lemma 2. *(Niederreiter, [8]). For an integer $M \geqslant 2$ and $y_0, \ldots, y_{N-1} \in \mathbb{Z}^s$, let P be the point set consisting of the fractional parts $\left\{M^{-1} y_0\right\}, \ldots, \left\{M^{-1} y_{N-1}\right\}$.*

Then

$$D_N(P) \leqslant 1 - \left(1 - \frac{1}{M}\right)^s + \sum_{h \in C_s^*(M)} \frac{1}{r(h,M)} \left| \frac{1}{N} \sum_{n=0}^{N-1} e\left(\frac{1}{M} h \cdot y_n\right) \right|.$$

From this lemma it is seen the the non-trivial estimates of exponential sums over the sequence $\left\{X_n^{(s)}\right\}$ are important for the further investigation we presented.

Next assertion has the paramount importance for estimation of such exponential sums.

Proposition 1. *Let $\{y_n\}$ be the sequence produced by the recursion (2) with the parameters $a \equiv b \equiv 0 \pmod p$, $(c,p) = (y_0,p) = 1$. Denote $m_0 = 2\nu_p(a) + \nu_p(b)$, $m_1 = \left[\frac{m}{\nu_p(a\cdot b)}\right]$. There are exist the polynomial $F_n(u,v) \in \mathbb{Z}[u,v]$ such that for $n \geqslant m+1$ we have*

$$\begin{aligned} y_n &\equiv F_n(y_0, y_0^{-1}) := A_{0n} + A_{1n} y_0 + B_{1n} y_0^{-1} + \\ &\quad + B_{2n} y_0^{-2} + B_{3n} y_0^3 + \cdots + B_{m_1 n} y_0^{-m_1} \pmod{p^m}, \\ B_{jn} &\equiv 0 \pmod{p^{m_0}},\ j \geqslant 4, \end{aligned} \tag{4}$$

where the coefficients A_{jn}, B_{jn} defined by the following relations

$$\begin{cases} A_{0,n+1} = b + c_{n+1}(b + c_n A_{0,n-1}) = \\ \qquad = b(1 + c_{n+1}) + c_{n+1}c_n(b + c_{n-1}A_{0,n-2}) = \\ \qquad = b(1 + c_{n+1} + c_{n+1}c_n + c_{n+1}c_nc_{n-1}A_{0,n-1}) = \\ \qquad = b(1 + c_{n+1} + c_{n+1}c_n + c_{n+1}c_nc_{n-1} + \cdots \\ \qquad \cdots + c_{n+1}c_n \cdots c_2 A_{0,1}) = bA_0'(n) \\ A_{1,n+1} = c_{n+1}c_n \cdots c_2 c_1. \end{cases} \tag{5}$$

$$\begin{aligned} B_{1,n+1} &= aA_{1n}^{-1} + c_{n+1}B_n = aA_{1n}^{-1}(1 + c_{n+1}c_n + c_{n+1}c_n^2c_{n-1} + \cdots + \\ &\quad + c_{n+1}c_n^2 \cdots c_2^2 c_1) = aB_{1,n+1}', \\ B_{2,n+1} &= ab\sum_{j=1}^{n+1} \frac{A_{0,j}'}{A_{1j}^2}, \\ B_{3,n+1} &= a^2 B_3'(n) + ab^2 B_3''(n), \\ B_{j,n+1} &\equiv 0 \pmod{p^{m_0}},\ j \geqslant 4, \end{aligned} \tag{6}$$

where $B_3'(n)$, $B_3''(n)$ have the simple description in terms of coefficients $c_1, c_2, \ldots$.

Proof. By (2) we infer consequently

$$\begin{aligned} y_1 &\equiv ay_0^{-1} + b + cy_0 \pmod{p^m}, \\ y_2 &= \frac{a}{ay_0^{-1} + b + y_0c_1} + b_2 + c_2(ay_0^{-1} + b_1 + c_1y_0) = \\ &= ac_1^{-1}y_0^{-1}(1 - ac_1^{-1}y_0^{-2} - bc_1^{-1}y_0^{-1} + a^2c_1^{-2}y_0^{-4} + 2abc_1^{-2}y_0^{-3} + b^2c_1^{-2}y_0^{-2} + \cdots) + \\ &+ b_2 + c_2(ay_0^{-1} + b_1 + c_1y_0) = A_{02} + A_{12}y_0 + B_{12}y_0^{-1}B_{22}y_0^{-2} + B_{32}y_0^{-3} + \cdots, \end{aligned}$$

where

$$\begin{aligned}
&A_{02} = b(1 + c_2),\\
&A_{12} = c_1 c_2,\\
&B_{12} = ac_1^{-1} + ac_2 = a(c_1^{-1} + c_2),\\
&B_{22} = -abc_1^{-2},\\
&B_{32} = -a^2 c_1^{-2} + ab^2 c_1^{-3},\\
&B_{42} = 2a^2 bc_1^{-3} - ab^3 c_1^{-4},\\
&B_{j2} \equiv 0 \pmod{p^{\min(2a+b,a+3b)}}.
\end{aligned}$$

In general case

$$y_n = A_{0n} + A_{1n} y_0 + B_{1n} y_0^{-1} + B_{2n} y_0^{-2} + \cdots, \ \ (A_{1n}, p) = 1.$$

$$\begin{aligned}
\Rightarrow y_{n+1} = {} & aA_{1n}^{-1} y_0^{-1} \left[1 - A_{0n} A_{1n}^{-1} y_0^{-1} - B_{1n} A_{1n}^{-1} y_0^{-2} - \right.\\
& \left. - B_{2n} A_{1n}^{-1} y_0^{-3} - A_{0n}^2 A_{1n}^{-2} y_0^{-2} + B_{1n}^2 A_{1n}^{-2} y_0^{-4} + \cdots\right] +\\
& + b + c_{n+1}(A_{0n} + A_{1n} y_0 + B_{1n} y_0^{-1} + B_{2n} y_0^{-2} + B_{3n} y_0^{-3} + B_{4n} y_0^{-4} + \cdots) =\\
& = A_{0,n+1} + A_{1,n+1} y_0 + B_{1,n+1} y_0^{-1} + B_{2,n+1} y_0^{-2} + B_{3,n+1} y_0^{-3+\cdots},
\end{aligned}$$

where

$$\begin{aligned}
&A_{0,n+1} = b + c_{n+1} A_{0n};\\
&A_{1,n+1} = c_{n+1} A_{1n};\\
&B_{1,n+1} = aA_{1n}^{-1} + c_{n+1} B_{1n};\\
&B_{2,n+1} = aA_{0n} A_{1n}^{-2} + B_{2n};\\
&B_{3,n+1} = -aB_{1n} A_{1n}^{-2} - aA_{2n}^2 A_{1n}^{-3} + c_{n+1} B_{3n};\\
&B_{jn} \equiv 0 \pmod{p^{m_0}}, \ \ j \geqslant 4.
\end{aligned}$$

Hence, we have

$$\begin{cases}
\begin{aligned}
A_{0,n+1} &= b + c_{n+1}(b + c_n A_{0,n-1}) = b(1 + c_{n+1}) + c_{n+1} c_n (b + c_{n-1} A_{0,n-2}) =\\
&= b(1 + c_{n+1} + c_{n+1} c_n + c_{n+1} c_n c_{n-1} A_{0,n-1}) =\\
&= b(1 + c_{n+1} + c_{n+1} c_n + c_{n+1} c_n c_{n-1} + \cdots + c_{n+1} c_n \cdots c_2 A_{0,1}) = bA_0'(n)
\end{aligned}\\
A_{1,n+1} = c_{n+1} c_n \cdots c_2 c_1.
\end{cases}$$

$$\begin{aligned}
B_{1,n+1} &= aA_{1n}^{-1} + c_{n+1} B_n = aA_{1n}^{-1}(1 + c_{n+1} c_n + c_{n+1} c_n^2 c_{n-1} + \cdots +\\
&\quad + c_{n+1} c_n^2 \cdots c_2^2 c_1) = aB_{1,n+1}',\\
B_{2,n+1} &= ab \sum_{j=1}^{n+1} \frac{A_{0,j}'}{A_{1j}^2},\\
B_{3,n+1} &= a^2 B_3'(n) + ab^2 B_3''(n),\\
B_{j,n+1} &\equiv 0 \pmod{p^{m_0}}, \ \ j \geqslant 4.
\end{aligned}$$

■

Corollary 3. *Let $\{y_n\}$ be the sequence produced by the recursion (2) with $\nu_p(b) = \beta < \nu_p(a) = \alpha$ and let $c_j = c$, $i = 1, 2, \ldots$. Then we have modulo p^m*

$$\begin{aligned} y_n = {} & y_0 + n(b + p^{\alpha} H_1(y_0^{-1})) - n^2 ab(1 + p^{\alpha-\beta} H_2(y_0^{-1})) + \\ & + n^3 p^{\min(2\alpha+\beta, \alpha+3\beta)} H_3(y_0^{-1}, n), \quad if \quad c \equiv 1 \pmod{p^m}, \end{aligned} \tag{7}$$

$$\begin{aligned} y_n = {} & y_0 + n(b + p^{\alpha} G_1(\delta, z, y_0^{-1})) - n^2 ab(1 + p^{\alpha-\beta} G_2(\delta, z, y_0^{-1})) + \\ & + n^3 p^{\min(2\alpha+\beta, \alpha+3\beta)} G_3(\delta, z, y_0^{-1}, n), \quad if \quad c \not\equiv 1 \pmod{p^m}, \end{aligned} \tag{8}$$

where H_i, G_j are polynomials on its own variables with integer coefficients.

Proof. For $c \equiv 1 \pmod{p^m}$ we obtain

$$\begin{cases} A_{0,n} \equiv nb, \ A_{1,n} \equiv 1 \pmod{p^m}, \\ B_{1,n} \equiv na, \ B_{2n} \equiv -ab\frac{n(n+1)}{2} \pmod{p^m} \\ B_{3,n} \equiv -ab\frac{n(n+1)}{2} - a^2(n-1) \pmod{p^m} \\ B_{jn} \equiv a^2 b \cdot g_1(n) + ab^3 \cdot g_2(n), \ g_1(n), g_2(n) \in \mathbb{Z}[n]. \end{cases} \tag{9}$$

From this follows that there are polynomials H_i, $i = 1, 2, 3$, such that the relation (7) holds.

If $c \not\equiv 1 \pmod{p^m}$ we denote throughout δ an index $c \pmod{p}$. Let us assume that $n = \delta\ell + z$, $0 \leqslant z \leqslant \delta - 1$, $\ell \equiv n\delta^{-1} + z\delta^{-1} \pmod{p}$.

Mindful that

$$\begin{aligned} c^n &\equiv (1 + pu)^{\ell} c^z \equiv (1 + pu\ell + p^2 u^2 \frac{\ell(\ell-1)}{2} + \cdots) c^z, \\ c^{-n} &\equiv (1 - pu\ell + p^2 u^2 \frac{\ell(\ell-1)}{2} + \cdots) c^{-z}, \end{aligned}$$

we also obtain

$$\begin{aligned} y_n \equiv {} & y_0 + n(b + p^{\alpha} G_1(\delta, z, y_0^{-1})) - n^2 ab(1 + G_2(\delta, z, y_0^{-1}) p^{\alpha}) + \\ & + n^3 p^{\gamma} G_3(\delta, z, y_0^{-1}), \end{aligned} \tag{10}$$

where $\gamma = \min(2\alpha + \beta, \alpha + 3\beta)$.

The corollary is established. ■

Corollary 4. *In notation above with $c_n = c + np$, $n = 1, 2, \ldots$, we have modulo p^m*

$$\begin{aligned} y_n = {} & b(n + pf_0(n)) + y_0(1 + pnf_1(n)) + \\ & + y_0^{-1} \left(n + p \left(\frac{n(n-1)(2n-1)}{6} + 2n^2 - n \right) + p^2 f_{21}(n) \right) + \\ & + y_0^{-2}(abf_{22}(n)) + y_0^{-3}(-ab^2 f_3(n)) + p^{\gamma} f_4(n), \end{aligned} \tag{11}$$

where $f_0, f_1, f_{21}, f_{22}, f_3, f_4 \in \mathbb{Z}[n]$.

Proof. In virtue of Proposition 1 we can write

$$\begin{aligned} A_{0n} &= b[1+(c+np)+(c+np)(c+(n-1)p)+\cdots \\ &\quad \cdots+(c+np)(c+(n-1)p)\cdots(c+p)c] = \\ &= b\left(1+c^n+pc^{n-1}\frac{n(n-1)}{2}+p^2c^{n-2}\sum_{\substack{i,j=1\\ i\neq j}}^{n} ij+\cdots\right) = \\ &= b(1+c^np^nF_1(n)) = bA'_{0n}, \end{aligned} \tag{12}$$

where $F_1(n) = 1 + a_1n + a_2n^2 + \cdots$, $a_i \equiv 0 \pmod{p^i}$, $i = 1, 2, \ldots$.

$$\begin{aligned} A_{1n} &= (1+p)(1+2p+\cdots+1+np) = \\ &= 1+p\frac{n(n+1)}{2}+p^2\frac{n(n+1)(6n^2-n-2)}{6}+p^3F_2(n),\ F_2(n)\in\mathbb{Z}. \end{aligned} \tag{13}$$

The similar reasoning shows that

$$B_{1n} = aA_{1n}^{-1}(1+d_1n+d_2n^2+\cdots),\quad (d1,p)=1,\ \nu_p(d_j)\geqslant 1,\ j=2,3,\ldots. \tag{14}$$

Further we have

$$B_{2n} = \begin{cases} ab\left(\frac{c-c^n}{1-c}+pF_3(n)\right) & if \quad c\not\equiv 1 \pmod{p^m} \\ ab(n+nF_4(n)) & if \quad c\equiv 1 \pmod{p^m}, \end{cases} \tag{15}$$

$$\begin{aligned} B_{3n} &= -a^2\left[\frac{c_n^2}{A_{1n}^4}(1+(c+np)(c+(n-1)p))+\right. \\ &\quad \left.+\frac{c_{n-1}^2}{A_{1,n-1}^4}(1+(c+(n-1)p+\cdots))+\cdots\right]- \\ &\quad - ab^2\frac{{A_{0n}}'^2}{A_{1n}^3}(n+pg(n))+\cdots = \\ &= -a^2(2c^2+c^3pn+c^4p^2n^2(1+pg_1(n)))- \\ &\quad - ab^2(n+2c^n+c^{2n})(1+png_2(n)), \end{aligned} \tag{16}$$

$$B_{jn} \equiv p^\gamma g_j(n) \pmod{p^m},\ j\geqslant 4, \tag{17}$$

where $g_1(n)$, $g_2(n)$, $g_j(n)$, $j \geqslant 4$, are polynomials with integer coefficients.

Hence, by Proposition 1 we obtain Corollary 2. ■

From Proposition 1, Corollaries 1 and 2 we deduce

Corollary 5. *Let τ be the least of periods for the sequence $\{y_n\}$ generated by the congruential recursion (2) with $\nu_p(b) = \beta < \nu_p(a) = \alpha$. Then $\tau = p^{m-\beta}$, if $c_n = c$ or $c_n = c + np$, $(c, p) = 1$.*

Proof. Indeed, from formulas for A_{0n}, A_{1n}, B_{jn}, $j = 1, 2, \ldots$, we can conclude that

$$A_{i,n+3} \equiv A_{i,3},\quad B_{j,n+3} \equiv B_{j,3} \pmod{p^m},\ i=0,1;\ j=1,2,\ldots,$$

if and only if $n \equiv 0 \pmod{p^{m-\beta}}$. ■

Let $\{y_n\}$ be the sequence produced by (2). For $h, h_1, h_2 \in \mathbb{Z}$ and $k, \ell \in \mathbb{N} \cup \{0\}$, we denote

$$S_N(h, y_0) = \sum_{n=0}^{N-1} e^{2\pi i \frac{hy_n}{p^m}},$$

$$\sigma_{k,\ell}(h_1, h_2; p^m) = \sum_{y_0 \in \mathbb{Z}_{p^m}^*} e\left(\frac{h_1 y_k + h_2 y_\ell}{p^m}\right).$$

Proposition 2. *Let we have the linear-inversive congruential generator produced by relation (2) with $\beta = \nu_p(b) < \nu_p(a) = \alpha$, $2\beta \leqslant m$, and let $(h, p^m) = s$. The we have the following estimates*

$$|S_N(h, y_0)| \leqslant \begin{cases} 0 & if \quad N = \tau,\ m > \beta + s, \\ N & if \quad m \leqslant \beta + s, \\ 2p^{\frac{m+s+\beta}{2}}(1 + \log p^{m-\beta}) & if \quad m > \beta + s. \end{cases}$$

Proof. First we assume that $N = \tau = p^{m-\beta}$, i.e. N is a period of the sequence $\{y_n\}$. The Corollaries 1 and 2 from Proposition 1 show that the behavior of the exponential sum $S_\tau(h, y_0)$ on the sequences of PRN's for the cases $c_n = c$ and $c_n = c + np$ are identical. Thus, we consider the sequence generated by (2) with $c_n = c$.

By Corollary 1 we have

$$|S_\tau(h, y_0)| = \left|\sum_{n=0}^{p^{m-\beta}-1} e\left(\frac{hy_n}{p^{m-\beta}}\right)\right| = \left|\sum_{n=0}^{p^{m-\beta}-1} e\left(\frac{h_0 F(n)}{p^{m-s-\beta}}\right)\right|,$$

where $h = h_0 p^s$, $F(n) = C_0 + C_1 n + \cdots + C_m n^m$,

$$\begin{aligned} C_1 &\equiv b \pmod{p^{\beta+1}}, \\ C_2 &\equiv -ab \pmod{p^{\alpha+\beta+1}}, \\ C_j &\equiv 0 \pmod{p^\gamma}, \end{aligned}$$

moreover,

$$\alpha = \nu_p(a),\ \ \beta = \nu_p(b),\ \ \gamma = \min(2\alpha + \beta, \alpha + 3\beta) > \alpha.$$

Now, applying Lemma 1 we obtain

$$|S_\tau(h, y_0)| = \begin{cases} \tau & if \quad m \leqslant \beta + s, \\ 0 & if \quad m > \beta + s. \end{cases}$$

In the case $N < \tau$ we use the well-known estimate of uncomplete exponential sum by means of the complete exponential sum (see, [7], Ch. 1, Th. 2)

$$|S_N(h, y_0)| \leqslant \max_{1 \leqslant t \leqslant \tau} \left|\sum_{n=0}^{\tau-1} e^{2\pi i\left(\frac{hF(n)}{\tau} + \frac{tn}{\tau}\right)}\right| (1 + \log \tau).$$

By virtue of the fact that the congruence

$$hb + t \equiv 0 \pmod{p^{\alpha+\beta}}$$

have only one solution under condition $1 \leqslant t \leqslant \tau$, we deduce (by Lemma 1), that

$$|S_N(h, y_0)| \leqslant p^s \cdot 2p^{\frac{m+\beta-s}{2}}(1 + \log p^{m-\beta}) = 2p^{\frac{m+\beta+s}{2}}(1 + \log p^{m-\beta}).$$

■

Remark. *Similar bound for $S_N(h, y_0)$ is valid for case $c_n = c + np$.*

Proposition 3. *Let $(h_1, h_2, p) = 1$, $\nu_p(h_1+h_2) = s_1$, $\nu_p(h_1k+h_2\ell) = s_2$ and let $\{y_n\}$ be the sequence produced by (2) with $c_n = c$ or $c_n = c + np$. The following estimates*

$$\left|\sum_{y_0 \in \mathbb{Z}^*_{p^m}} e\left(\frac{h_1y_k + h_2y_\ell}{p^m}\right)\right| \leqslant \begin{cases} 0 & if \quad s_1 < s_2 + \beta,\ m - s_1 - s_2 > 0, \\ 2p^{\frac{m+\beta+s_2}{2}} & if \quad s_1 \geqslant s_2 + \beta,\ m - s_1 - s_2 > 0, \\ p^{m-1}(p-1) & otherwise, \end{cases}$$

hold.

Proof. Let $c = 1 + pu$, $u \not\equiv 0 \pmod{p^{m-1}}$. By Corollary 2 we have modulo p^m

$$h_1y_k + h_2y_\ell = B_0 + B_1y_0 + B_{-1}y_0^{-1} + B_{-2}y_0^{-2} + \cdots,$$

where

$$\begin{aligned}
B_0 &= b\left[(h_1 + h_2) + (h_1c^kp^kF_1(k) + h_2c^\ell p^\ell F_1(\ell))\right] = bB_0',\ \ (B_0', p) = 1; \\
B_1 &= (h_1 + h_2) + p\left(h_1\frac{k(k+1)}{2} + h_2\frac{\ell(\ell+1)}{2} + \cdots\right); \\
B_{-1} &= a[(h_1 + h_2) + d_1(h_1k + h_2\ell) + d_2(h_1k^2 + h_2\ell^2) + \cdots]; \\
B_{-2} &= ab\left[\frac{c(h_1 + h_2) - (h_1c^k + h_2c^\ell)}{c-1} + p(h_1F_3(k) + h_2F_3(\ell))\right]; \\
B_{-3} &\equiv -a^2\left(2c^2(h_1 + h_2) + c^3p(h_1k + h_2\ell) + \right. \\
&\quad + c^4p^2(h_1(k^2 + pg(k)) + h_2(\ell^2 + pg(\ell)))\big) - \\
&\quad - ab^2\left[h_1k + h_2\ell + 2(h_1c^k + h_2c^\ell) + (h_1c_1^{2k} + h_2c^{2\ell})(h_1 + h_2) + \right. \\
&\quad + p(h_1kg(k) + h_2\ell g(\ell))\big]; \\
B_{-j} &\equiv 0 \pmod{p^\gamma},\ \ j = 4, 5, \ldots.
\end{aligned}$$

Substituting c^k and c^ℓ by the polynomials on k and ℓ and applying Lemma 1 we obtain requisite statement. ■

This conclusion of Proposition 3 stays behind also for $c_n = c+pn$, $c \not\equiv 1 \pmod{p^m}$.

Main Results. The properties of equidistribution and statistical independency of sequences of PRN's $\{y_n\}$ generated by (2) we will study using bounds for the discrepancy of certain points produced by the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$. We say that the sequence $\{x_n\}$ passes the s-dimensional test on equidistribution and statistical independency if every sequence $\{X_n^{(j)}\}$, $X_n = (x_n, \ldots, x_{n+j-1})$, $j = 1, \ldots, s$ has the discrepancy $D_N(X_n^{(j)})$ such that $D_N(X_n^{(j)}) \to 0$ for $N \to \infty$. From Lemma 2 it follows that we should have non-trivial estimates for sum

$$\sum_{n=0}^{N-1}\left(\frac{h_1y_n + \cdots + h_jy_{n+j-1}}{p^m}\right),\ \ j = 1, 2, \ldots, s.$$

Theorem 1. *Let $\{X_n^{(j)}\}$, $n = 0, 1, \ldots, N-1$, $X_n^{(j)} = (x_n, \ldots, x_{n+j-1})$ be the sequence of points $X_n^{(j)} \in [0,1)^j$ produced by (2). Then for every j, $1 \leqslant j \leqslant 4$, the following estimate*

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

holds.

Proof. Let $h \cdot X_n^{(j)}$ denote the inner dot of h and $X_n^{(j)}$, i.e.

$$h \cdot X_n^{(j)} = h_1 x_n + h_2 x_{n+1} + \cdots + h_j x_{n+j-1}.$$

In order to apply Lemma 2, we should have an estimate for the sum

$$\sum_{n=0}^{\tau-1} e\left(\frac{h_1 y_n + h_2 y_{n+1} + \cdots + h_j y_{n+j-1}}{p^m}\right).$$

Without loss of generality, we can suppose that $(h_1, h_2, \ldots, h_j, p) = 1$. From the representation y_n as a polynomial on n (by Corollaries 1 and 2) we have

$$h_1 y_n + \cdots + h_j y_{n+j-1} = (h_1 y_0 + \cdots h_j y_0) +$$

$$+ (h_1 n + h_2(n+1) + \cdots + h_j(n+j-1))b + np^{\alpha+\beta} G^{(1)}(y_0^{-1}) -$$

$$- ab(1 + p^{\alpha-\beta} G^{(2)}(y_0^{-1})) \sum_{i=1}^{j} h_i (n+i-1)^2 +$$

$$+ \left(\sum_{i=1}^{j} h_i (n+i-1)^3\right) p^\gamma G^{(3)}(y_0, h_i).$$

Hence, the sum $h_1 y_n + \cdots + h_j y_{n+j-1}$ represents a polynomial of special type $f(n)$ such that the exponential sum $\sum\limits_{n=1}^{p^m} e\left(\frac{f(n)}{p^m}\right)$ is appreciable by Lemma 1:

$$\left|\sum_{n=0}^{\tau-1} e\left(\frac{h_1 y_n + \cdots + h_j y_{n+j-1}}{p^m}\right)\right| \leqslant 2p^{\frac{m+\beta+\ell}{2}},$$

if $(h_1 + h_2 + \ldots + h_j, p^m) = p^\ell$.

Now, using the connection between complete and uncomplete exponential sums and Lemma 2, we deduce the assertion of theorem. ■

Corollary 6. *The sequence of PRN's produced by (2) passes s-dimensional test on equidistibution and statistical independency for $s = 1, 2, \ldots, p-1$.*

Theorem 2. *Let the sequence $\{y_n\}$ be produced by (2) with $(c, p) = (y_0, p) = 1$, $0 < \beta = \nu_p(b < \alpha = \nu_p(a))$. Then for $h \in \mathbb{Z}$, $\nu_p(h) = s$, we have*

$$\overline{S}_N(h) = \frac{1}{\varphi(p^m)} \sum_{y \in \mathbb{Z}_{p^m}^*} |S_N(h, y_0)| \leqslant N^{\frac{1}{2}} + Np^{-\frac{m+s}{4}} (2 + \sqrt{5} p^{\frac{\beta}{4}}).$$

Proof. Without loss of generality we will assume that $s = 0$. By the Cauchy-Schwarz inequality we obtain

$$|\overline{S}_N(h)|^2 \leqslant \frac{1}{\varphi(p^m)} \sum_{y_0 \in \mathbb{Z}_{p^m}^*} |S_N(h, y_0)|^2 = \frac{1}{\varphi(p^m)} \sum_{k,\ell=0}^{N-1} \sum_{y_0 \in \mathbb{Z}_{p^m}^*} e\left(\frac{h(y_k - y_\ell)}{p^m}\right) \leqslant$$

$$\leqslant \frac{1}{\varphi(p^m)} \sum_{k,\ell=0} |\sigma_{k,\ell}(h, -h; p^m)| = \frac{1}{\varphi(p^m)} \sum_{r=0}^{\infty} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=r}}^{N-1} |\sigma_{k,\ell}(h-h; p^m)| =$$

$$= \frac{1}{\varphi(p^m)} \sum_{\gamma=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}(h, -h; p^m)| + \frac{1}{\varphi(p^m)} \sum_{\substack{k=0 \\ k=\ell}}^{N-1} |\sigma_{k,k}(h, -h; p^m)| =$$

$$= N + \frac{1}{\varphi(p^m)} \sum_{\gamma=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}(h, -h; p^m)|.$$

Using Proposition 3 we infer

$$|\overline{S}_N(h)|^2 \leqslant N + \frac{1}{\varphi(p^m)} \sum_{\gamma=0}^{m-1} \left(\sum_{\substack{k,\ell=0 \\ k \not\equiv \ell (mod\ 2) \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell(h,-h;p^m)}| + \right.$$

$$\left. + \sum_{\substack{k,\ell=0 \\ k \equiv \ell (mod\ 2) \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}(h, -h; p^m)| \right) \leqslant N + \frac{1}{\varphi(m)} \left[2p^{\frac{m}{2}} \sum_{\gamma=0}^{m-1} \frac{N}{p^\gamma} + \right.$$

$$\left. + \left(\sum_{\gamma < m-\beta} + \sum_{m-\beta \leqslant \gamma \leqslant m-1} \right) \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h, -h; p^m)| \right] \leqslant$$

$$\leqslant N + \frac{1}{\varphi(m)} \left\{ 2p^{\frac{m}{2}} \sum_{\gamma=0}^{m-1} \frac{N}{p^\gamma} + \right.$$

$$\left. + \left(\sum_{\gamma < m-\beta} + \sum_{m-\beta \leqslant \gamma \leqslant m-1} \right) \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}(h, -h; p^m)| \right\} \leqslant$$

$$\leqslant N + \frac{1}{\varphi(m)} \left\{ 2Np^{\frac{m}{2}} + 2 \sum_{\gamma < m-\beta} p^{\frac{m+\beta+\gamma}{2}} \frac{N}{p^\gamma} + p^m \sum_{\gamma \geqslant m-\beta} \frac{N}{p^\gamma} \right\} \leqslant$$

$$\leqslant N + \frac{1}{\varphi(m)}\left(2Np^{\frac{m}{2}} + 2Np^{\frac{m+\beta}{2}} + Np^m p^{-m+\beta}\right) \leqslant$$

$$\leqslant Np^{-\frac{m}{2}}\left(4 + 5p^{\frac{\beta}{2}}\right).$$

Thus, for $(h,p) = 1$:

$$|\overline{S}_N(h)| \leqslant N^{\frac{1}{2}} + Np^{-\frac{m}{4}}\left(2 + \sqrt{5}p^{\frac{\beta}{4}}\right).$$

If $(h,p^m) = p^s$, $s < m$, then similarly to the previous, we have

$$|\overline{S}_N(h)| \leqslant N^{\frac{1}{2}} + Np^{-\frac{m+s}{4}}\left(2 + \sqrt{5}p^{\frac{\beta}{4}}\right).$$

■

Theorem 3. *Let $D_N(y_0)$ denotes the mean of discrepancy of the sequence points $\left\{\frac{y_n}{p^m}\right\}$ produced by the recursion (2) with initial value y_0. Then the following bound for value averaged over all $y_0 \in \mathbb{Z}_{p^m}^*$*

$$\overline{D}_N = \frac{1}{\varphi(p^m)} \sum_{y_0 \in \mathbb{Z}_{p^m}^*} D_N(y_0) \leqslant \frac{1}{p^m} + 3p^{-\frac{m-\beta}{4}} \log p^m$$

holds.

This assertion follows immediately from Theorem 2 and Lemma 2.

The last theorem shows that for $\beta > \frac{2}{3}m$ upon the average an estimate of $D_N(y_0)$ it is preferable than individual estimate $D_N(y_0)$ given by Theorem 1.

Conclusion. In the presented paper a new linear-inversive congruential generator with prime-power modulus was introduced. Exponential sums on linear-inversive congruential pseudorandom numbers were estimated. The obtained results show these inversive congruential pseudorandom numbers pass s-dimensional serial tests on the statistical independence.

1. **Blackburn S. R.** Predicting nonlinear pseudorandom number generators / S. R. Blackburn, D. Gomez-Peres, I. Gutierrez, I. Shparlinski // Math. Comp. – 2004. – V. 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. – V. 61(2). – P. 47–59.
3. **Chou W.-S.** The period lengths of inversive congruential recursions / W.-S. Chou // Acta Arith. – 1995. – V. 73(4). – P. 325–341.
4. **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. – V. 2(1). – P. 1–11.
5. **Eichenauer J.** A nonlinear congruential pseudorandom number generator with power of two modulus / J. Eichenauer, J. Lehn, A. Topuzoğlu // Math. Comp. – 1988. – V. 51. – P. 757–759.

6. **Kato T.** On a nonlinear congruential pseudorandom number generator / T. Kato, L.-M. Wu, N. Yanagihara // Math. of Comp. – 1996. – V. 65(213). – P. 227–233.

7. **Korobov N. M.** Trigonometric Sums and Their Applications. – Moscow, Nauka, 1989.

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

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

10. **Niederreiter H.** On the Distribution of Compound Inversive Congruential Pseudorandom Numbers / H. Niederreiter, A. Winterhof // Monatsh. Math. – 2001. – V. 132. – P. 35-–48.

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

12. **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, 2012. – P. 265–282.