Mathematical Subject Classification: 11N25, 11S40
UDC 511

S. Varbanets
I. I. Mechnikov Odessa National University

PARITY OF THE NUMBER OF PRIMES IN A GIVEN INTERVAL AND ALGORITHMS OF THE SUBLINEAR SUMMATION

Варбанець С. Лінійно-інверсний генератор псевдовипадкових чисел за модулем ступеня двійки. Розглянуто узагальнення інверсного конгруентного генератора псевдовипадкових чисел за модулем ступеня простого числа. Отримані оцінки експоненційних сум на послідовності псевдовипадкових чисел.
Ключові слова: інверсні конгруентні псевдовипадкові числа, експоненційна сума, дискрепансія.

Варбанец С. Линейно-инверсный генератор псевдослучайных чисел по модулю степени двойки. Рассмотрено обобщение инверсного конгруэнтного генератора псевдослучайных чисел по модулю степени простого числа. Даны оценки экспоненциальных сумм на последовательности псевдослучайных чисел.
Ключевые слова: инверсные конгруэнтные псевдослучайные числа, экспоненциальная сумма, дискрепансия.

Varbanets S. Linear-inversive prn's generator with power of two modulus. Generalization of the inversive congruential generator of pseudorandom numbers with prime-power modules is considered and the trigonometrical sums on sequence of pseudorandom numbers are estimated.
Key words: inversive congruential pseudorandom numbers, exponential sum, discrepancy.

Introduction. Nonlinear methods of generating uniform pseudorandom numbers in the interval $[0, 1)$ have been introduced and studied during the last twenty five years. The development of this attractive fields of research is described in the works of Lehn, Eichenauer, Niederreiter, Emmerich etc. A particularly promising approach is the inversive congruential method. Four types of inversive congruential generators can be distinguished, depending on whether the modulus is a prime, an odd prime power, a power of two or a product of distinct prime numbers. In the case of prime-power modulus the inversive congruential generator is defined in the following way:

Let p be a prime, $p \geq 3$, m be a natural number. For given $a, b \in \mathbb{Z}$ we take an initial value y_0, and let y_n^{-1} denotes a multiplicative inverse for y_n in $\mathbb{Z}^*_{p_m}$ if $(y_n, p) = 1$, and $y_n^{-1} = 0$ if $m = 1$ and $y_n \equiv 0(mod\ p)$. Then the recurrence relation

$$y_{n+1} \equiv a y_n^{-1} + b (mod\ p^m) \tag{1}$$

generates a sequence $y_0, y_1, \ldots$ which we call the inversive congruential sequence modulo p^m.

The case $p \geq 3$, $m = 1$ studied in [2],[6]. For the case $p = 2$, $m > 3$ the relevant investigation presented in [1, 3, 4].

In 1996 T. Kato, L.-M. Wu and N. Yanagihara[4] studied a non-linear congruential generator for the modulus $M = 2^m$ defined by the congruence

$$y_{n+1} \equiv a\overline{y}_n + b + cy_n \pmod{M},\ n = 0, 1, \dots \tag{2}$$

with the conditions

$$(y_0, 2) = (a, 2) = 1,\ b \equiv c \equiv 2 \pmod{2}. \tag{3}$$

Note that the conditions (3) guarantee infinity of the process of generation. This authors obtained the condition whereby the recursion (2) generates the sequence $\{y_n\}$ with the maximal period $\tau = 2^{m-1}$. They also give the estimate for the discrepancy of the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$.

In the present note we give the representation of elements y_n as polynomials of n and y_0 and that permits to improve the results from [7].

The essential nature of our method consists in the construction of representations of y_n as the polynomial on initial value y_0 and number n.

It is purpose of the present work to demonstrate that the sequence of PRN's $\{x_n\} = \left\{\frac{y_n}{2^m}\right\}$, $n = 0, 1, \dots$, generated by the recursion (2), satisfies the requirements of equidistribution on $[0, 1)$ and passes the serial test on unpredictability.

Notation. Variables of summation automatically range over all integers satisfying the condition indicated. For $m \in \mathbb{N}$ and $M = 2^m$ the notation $\mathbb{Z}_M$(respectively, $\mathbb{Z}_M^*$) denotes the complete(respectively, reduced) system of residues modulo M. We write $gcd(a, b) = (a, b)$ for notation a great common divisor of a and b. For $z \in \mathbb{Z}$, $(z, 2) = 1$ let z^{-1} be the multiplicative inverse of a modulo M. We write $\nu_2(A) = \alpha$ if $2^\alpha | A$, $2^{\alpha+1} \not| A$. For real t, the abbreviation $e(t) = e^{2\pi i t}$ is used.

Auxiliary results. We need the following two simple statements.

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

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

Lemma 1. *In above notations we have*

$$|S_N(f)| \le \max_{1 \le n \le \tau} \left| \sum_{x=1}^{\tau} e\left(f(x) + \frac{nx}{\tau}\right) \right| \cdot (1 + \log \tau). \tag{4}$$

This lemma is well-known.

Lemma 2 ([7]). *Let p be a prime number and let $f(x)$, $g(x)$ be polynomials over* $\mathbb{Z}$

$$f(x) = A_1 x + A_2 x^2 + 2(A_3 x^3 + \cdots),$$
$$g(x) = B_1 x + +2(B_2 x^2 + \cdots),$$

and let, moreover, $\nu_2(A_2) = \alpha > 0$, $\nu_2(A_j) \ge \alpha$, $j = 3, 4, \dots$.
Then we have the following estimates

$$\left|\sum_{x\in\mathbb{Z}_{2^m}} e\left(\frac{f(x)}{2^m}\right)\right| \leq \begin{cases} 2^{\frac{m+\alpha}{2}+1} & \text{if} \quad \nu_2(A_1)\geq\alpha, \\ 0 & \text{else;} \end{cases} \tag{5}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{2^m}} e\left(\frac{f(x)+g(x^{-1})}{2^m}\right)\right| \leq \begin{cases} 2^{\frac{m}{2}+1} & if \quad B_1 \text{ is odd}, \\ 2^{\frac{m+\alpha+4}{2}} & if \quad \nu_2(A_1)\geq\ell, \\ & \qquad \nu_2(B_j)\geq\alpha,\ldots, \\ 0 & if \quad \nu_2(A_1)<\alpha\leq\nu_2(B_j), \\ & \qquad j=1,2,3,\ldots, \end{cases} \tag{6}$$

Now we will obtain the representation of y_n in the form of rational function on y_0.
Let $n=2k$. We put

$$y_{2k}=\frac{\sum\limits_{\ell\geq 0} A_\ell^{2k} y_0^\ell}{\sum\limits_{\ell\geq 0} B_\ell^{2k} y_0^\ell}, \quad A_\ell^{2k}, B_\ell^{2k}\in\mathbb{Z}. \tag{7}$$

After simple calculations by recursion (2) we infer

$$y_{2(k+1)}=\frac{\sum\limits_{\ell\geq 0} A_\ell^{2(k+1)} y_0^\ell}{\sum\limits_{\ell\geq 0} B_\ell^{2(k+1)} y_0^\ell},$$

where

$$\begin{aligned} A_\ell^{2(k+1)} &= \sum_{s+t=\ell}\sum_{i=0}^{s}\sum_{j=0}^{t}(aA_iB_{s-i}A_jB_{t-j}+abB_iA_jB_{s-i}B_{t-j}+ \\ &\quad + b^2A_iA_jB_{s-i}B_{t-j}+bcA_iA_jA_{s-i}B_{t-j}+a^2cB_iB_jB_{s-i}B_{t-j}+ \\ &\quad + abcB_iA_jB_{s-i}B_{t-j}+ac^2B_iB_{s-i}A_jA_{t-j}+abcA_iB_jB_{s-i}B_{t-j}+ \\ &\quad + b^2cA_iA_jB_{s-i}A_{t-j}+bc^2A_iA_jB_{s-i}A_{t-j}+ac^2A_iB_jA_{s-i}B_{t-j}+ \\ &\quad + bc^2A_iA_jA_{s-i}B_{t-j}+c^3A_iA_jA_{s-i}A_{t-j}\ ); \\ B_\ell^{2(k+1)} &= \sum_{\substack{s,t\geq 0\\ s+t=\ell}}\sum_{i=0}^{s}\sum_{j=0}^{t}(aB_iA_jB_{s-i}B_{t-j}+A_iA_jB_{t-j}(bB_{s-i}+cA_{s-i})) \end{aligned}$$

(Here, for the sake of comfort we write A_j, B_j instead $A_i^{(2k)}$, $B_j^{(2k)}$).

Let j'_n (respectively, j''_n) be a exponent of y_0, for which $\left(A_{j'_n}^{(2k)},2\right)=1$ (respectively, $\left(A_{j''_n}^{(2k)},2\right)=1$).
By induction we infer easy

$$i'_{2k}=\frac{2^{2k}+2}{3}, \quad j''_{2k}=j'_{2k}-1.$$

Moreover,

$$\nu_2\left(A_\ell^{(2k)}\right) \geq \left|\frac{j'_{2k}-\ell}{2}\right| \cdot \nu_2(b),$$

$$\nu_2\left(B_\ell^{(2k)}\right) \geq \left|\frac{j''_{2k}-\ell}{2}\right| \cdot \nu_2(b).$$

Thus, the numerator and the denominator of fraction in (7) for $k \geq 2m_0+1$, $m_0 = \left[\frac{m}{\nu_2(b)}\right]$, over $\mathbb{Z}_{2^m}$ contain at the most $4m_0+1$ summands, i.e.

$$y_{2k}\frac{\left(\sum\limits_{\ell=j'_n-2m_0}^{j'_n+2m_0} A_\ell^{(2k)} y_0^\ell\right)}{\left(\sum\limits_{\ell=j''_n-2m_0}^{j''_n+2m_0} B_\ell^{(2k)} y^\ell\right)}. \tag{8}$$

Divide on a^k the numerator and the denominator in (8). Then we obtain the following representation

$$y_{2k} = \frac{\sum \overline{A}_\ell y^\ell}{\sum \overline{B}_\ell y^\ell},\ \overline{A}_\ell \equiv a^{-k}A_\ell,\ \overline{B}_\ell \equiv a^{-k}B_\ell (mod\ 2^m). \tag{9}$$

Now the coefficients $\overline{A}_\ell$, $\overline{B}_\ell$ are polynomials on k with coefficients, which depend only on a, b_0, c_0, m, where $b = 2^{\nu_2(b)}b_0$, $c = 2^{\nu_2(b)}c_0$, and these coefficients have the indicated above properties of divisibility on power of 2.

By the congruence for every $t \in \mathbb{Z}$

$$\frac{1}{1-2t} \equiv 1 + 2t + 2^2t^2 + \cdots + 2^{m-1}t^{m-1} (mod\ M)$$

and taking into account that in denominator of y_{2k} it has only one power y_0 (just $y_0^{i''_{2k}}$) with coefficient $B_{j''_{2k}}$, $(B_{j''_{2k}}, 2) = 1$, we may write

$$y_{2k} \equiv F(k, y_0, y_0^{-1}) (mod\ 2^m),\ \ F(u, v, w) \in \mathbb{Z}[u, v, w]. \tag{10}$$

The analogous representation holds for y_{2k+1}

$$y_{2k+1} \equiv G(k, y_0, y_0^{-1}) (mod\ M). \tag{11}$$

Let $\nu_2(b) \leq \nu_2(c)$. We make more precise the representations (10), (11). Using the principle of mathematical induction it is not difficult to check the correctness of the following relations for $k \geq 2m+1$:

$$\begin{aligned} y_{2k} &= kb + kacy_0^{-1} + (1 - k(k-1)a^{-1}b^2)y_0 + (-ka^{-1}b)y_0^2 + \\ &+ (-ka^{-1}c + k^2a^{-2}b^2)y_0^3 + 2^\alpha F_0(k, y_0, y_0^{-1}), \end{aligned} \tag{12}$$

$$\begin{aligned} y_{2k+1} &= (k+1)b + (a - k(k+1)b^2)y_0^{-1} + (-kab)y_0^{-2} + \\ &+ (-ka^2c + k^2ab^2)y_0^{-3} + (k+1)cy_0 + 2^\alpha G_0(k, y_0, y_0^{-1}), \end{aligned} \tag{13}$$

where $\alpha := \min(\nu_2(b^3), \nu_2(bc))$;

$F_0(u, v, w)$, $G_0(u, v, w) \in \mathbb{Z}[u, v, w]$, $F_0(0, v, w) = G_0(0, v, w) = 0$.

Thus, we get the following result.

Lemma 3. *Let $\{y_n\}$ is the sequence of PRN's generated by the recursion (2) with conditions $(y_0, 2) = (a, 2) = 1$, $0 < \nu_2(b) < \nu_2(c)$. There exist the polynomials $F_0(u, v, w)$, $G_0(u, v, w)$ over $\mathbb{Z}$, $F_0(0, v, w) = G_0(0, v, w) = 0$ such that the relations (12) and (13) are right for any $k \geq 2m + 1$.*

Corollary 1. *Let $m \geq 3$. Then the sequence $\{y_n\}$ defined by recursion (2) is purely periodic, where $b = 2^\nu b_0$, $(b_0, 2) = 1$, $c = 2^\mu c_0$, $(c_0, 2) = 1$, $\mu > \nu > 0$; $\nu_2(a - y_0^2) = \nu_0 \geq 1$. And its period τ is equal*

$$\begin{array}{lll} (i) & 2^{m-2\nu+1} & if \quad m \geq 2\nu,\ \nu_0 > \nu; \\ (ii) & 2^{m-2\nu-\beta_0+1} & if \quad m > 2\nu,\ \nu_0 = \nu, \beta_0 = \nu_2\left(\frac{y_0^2-a}{2^{\nu_0}} + b_0\right); \\ (iii) & 2^{m-\nu-\nu_0+1} & if \quad m \geq \nu + nu_0,\ \nu_0 < \nu. \end{array}$$

Proof. The first part of corollary follows as in [7].
To prove the second part, we have

$$\begin{gathered} y_{2k} \equiv y_0 (mod\ 2^m) \Longleftrightarrow \\ kb(1 - a^{-1}y_0^2) - k(k-1)a^{-1}b^2 y_0 + \\ + ka^{-1}cy_0^{-1}(a^2 - y_0^4) + 2^\alpha F_0(k) \equiv 0 (mod\ 2^m). \end{gathered} \tag{14}$$

It follows that k must be a least positive integer for which the congruence $k \equiv 0(mod\ 2^\ell)$ holds, where

$$\ell = \begin{cases} \nu_2(b) + \nu_2(a - y_0^2) & if \quad \nu_2(a - y_0^2) < \nu_2(b) \leq \frac{1}{2}m; \\ 2\nu_2(b) & if \quad \nu_2(b) \leq \frac{1}{2}m,\ \nu_2(a - y_0^2) > \nu_2(b). \end{cases}$$

□

Remark 1. *From (i), (ii) of Corollary 2 we obtain that for $\nu_0 \geq \nu$ the maximal period $\tau = 2^{m-2\nu+1}$ achieves, if and only if, $\nu_0 > \nu$ and $m \geq 2\nu$. In the work [4] this assertion was obtained only for $\nu = 1$.*

Exponential sums on sequence of PRN's. In this section we determine the estimates of certain exponential sums over the linear-inversive congruential sequence $\{y_n\}$ which was defined in (2).
For $h_1, h_2 \in \mathbb{Z}$ we denote

$$\sigma_{k,\ell}(h_1, h_2; M) := \sum_{y_0 \in \mathbb{Z}_M^*} e\left(\frac{h_1 y_k + h_2 y_\ell}{M}\right), \ (h_1, h_2 \in \mathbb{Z}). \tag{15}$$

Here we consider y_k, y_ℓ as a functions at y_0 generated by (2) (see, formula (13)).

Theorem 1. *Let $(h_1, h_2, 2) = 1$, $\nu_2(h_1 + h_2) = \beta$, $\nu_2(h_1 k + h_2 \ell) = \gamma$. The following estimates*

$$|\sigma_{k,\ell}(h_1, h_2; M)| \leq \begin{cases} 2^{\frac{m+2}{2}} & if \quad k \not\equiv \ell (mod\ 2); \\ 0 & if \quad k \equiv \ell (mod\ 2) \\ & and \quad \beta < \gamma + \nu,\ m - \beta - \nu > 0; \\ 2^{m-1} & if \quad k \equiv \ell (mod\ 2) \\ & and \quad \beta \geq \gamma + \nu,\ m - \nu - \gamma \leq 0; \\ 2^{\frac{m+\nu+\gamma+2}{2}} & if \quad k \equiv \ell (mod\ 2) \\ & and \quad \beta \geq \gamma + \nu,\ m - \nu - \gamma > 0. \end{cases}$$

hold.

Proof. We consider two cases:
(I) If k and ℓ be non-negative integers of different parity, we obtain the statement of theorem by (12), (13) and Lemma 2.

(II) Let k and ℓ be integers of identical parity. Then for $k := 2k$, $\ell := 2\ell$, we have modulo M:

$$h_1 y_{2k} + h_2 y_{2\ell} =$$
$$= B_0 + B_1 y_0 + B_2 y_0^2 + B_3 y_0^3 + B_{-1} y_0^{-1} + 2^\alpha K(y_0, y_0^{-1}) := F_2(y_0, y_0^{-1}),$$

where $B_1 = h_1 + h_2 + 2^{2\nu} B_1'$,
$B_2 = -ab(h_1 k + h_2 \ell) + 2^\alpha B_2'$,
$B_3 = -a^{-2} b^2 (h_1 k^2 + h_2 \ell^2) - a^{-1} c(h_1 k + h_2 \ell) + 2^\alpha B_3'$,
$B_{-1} = ac(h_1 k + h_2 \ell) + 2^\alpha B_{-1}'$,
moreover, B_1', B_2', B_3', B_{-1}' and coefficients of $K(y_0, y_0^{-1})$ contain multipliers of form $h_1 k^j + h_2 \ell^j$, $j \geq 0$.

Let $\nu_2(h_1 + h_2) = \beta \geq \nu$, $\nu_2(h_1 k + h_2 \ell) = \gamma \geq 0$, $\delta = \min(\beta, \gamma)$.
The application of Lemma 1 gives

$$|\sigma_{2k,2\ell}(h_1, h_2; M)| \leq \begin{cases} 0 & if \quad \beta < \gamma + \nu, \ m - \beta - \nu > 0, \\ 2^{\frac{m+\nu+\gamma+2}{2}} & if \quad \beta \geq \gamma + \nu, \ m - \nu - \gamma > 0, \\ 2^{m-2} & if \quad \beta \geq \gamma + \nu, \ m - \nu - \gamma \leq 0, \end{cases}$$

where $\varphi(2^{m-1})$ is the totient Euler function.
For $k \equiv \ell \equiv 1 (mod\ 2)$ we have the analogous result.
This finishes the proof of Theorem 1. □

Remark 2. *The case* $\nu_2((h_1, h_2, M)) > 1$ *reduces easily to the case* $\nu_2((h_1, h_2, 2)) = 0$.

Let h be integer, $(h, M) = 2^s$, $0 \leq s < m$, and let τ be a least period length of the sequence of PRN's $\{y_n\}$, $n = 0, 1, \ldots$, defined in (2). For $1 \leq N \leq \tau$ we denote

$$S_N(h, y_0) = \sum_{n=0}^{N-1} e\left(\frac{h y_n}{M}\right). \tag{16}$$

The sum $S_N(h, y_0)$ calls the exponential sum on the sequence of PRN's $\{y_n\}$.
We shall obtain the bound for $S_N(h, y_0)$.
By the relation (12)-(13) we get for $k \geq 2m + 1$:

$$y_{2k} = A_0 + A_1 k + A_2 k^2 + A_3 k^3 := F(k), \tag{17}$$
$$y_{2k+1} = B_0 + B_1 k + B_2 k^2 + B_3 k^3 := G(k), \tag{18}$$

where

$$
\begin{aligned}
&A_0 = A_0(y_0) \equiv y_0 (mod\ 2^\alpha)\\
&A_1 = A_1(y_0) \equiv b(1 - a^{-1}y_0^2) + a^{-1}b^2 y_0 + acy_0^{-1}(1 - a^{-2}y^4)(mod\ 2^\alpha)\\
&A_2 = A_2(y_0) \equiv -a^{-1}b^2 y_0 + a^{-2}b^2 y_0^3 (mod\ 2^\alpha) = -a^{-1}b^2 y_0 (1 - a^{-1}y_0^2)\\
&B_0 = B_0(y_0) \equiv b + ay_0^{-1} + cy_0 (mod\ 2^\alpha)\\
&B_1 = B_1(y_0) \equiv b(1 - ay_0^{-2}) - b^2 y_0^{-1} - y_0 c(1 - a^2 y_0^{-4})(mod\ 2^\alpha)\\
&B_2 = B_2(y_0) \equiv -b^2 y_0^{-1} + ab^2 y_0^{-3} (mod\ 2^\alpha) = -b^2 y_0^{-1}(1 - ay_0^{-2})\\
&A_3 = A_3(y_0, k) \equiv B_3(y_0, k) \equiv B_3 \equiv 0 (mod\ 2^\alpha),\\
&\alpha = \min(3\nu, \nu + \mu).
\end{aligned}
\tag{19}
$$

After all this preliminary work, it is straightforward to prove two main result of this section:

Theorem 2. *Let the linear-inversive congruential sequence generated by the recursion (2) has the period* τ, *and let* $\nu_2(b) = \nu$, $\nu_2(c) = \mu$, $\nu < \mu$, $\alpha = \min(3\nu, \nu + \mu)$, $\nu_2(a - y_0^2) = \nu_0$, $2\nu \le m$. *Then the following bounds*

$$
|S_\tau(h, y_0)| \le \begin{cases} O(m) & if \quad p = 2,\ \nu_0 < \nu,\ \nu_2(h) < m - 2\nu; \\ 4 \cdot 2^{\frac{m+\nu_2(h)}{2}} & if \quad \nu_0 \ge \nu,\ \nu_2(h) < m - 2\nu; \\ \tau & else, \end{cases}
$$

hold.

Proof. From the formulas (17)-(18) we have

$$
\begin{aligned}
|S_\tau(h, y_0)| &= \left| \sum_{n=0}^{\tau-1} e\left(\frac{hy_n}{M}\right) \right| = \left| \sum_{n=0}^{2^\ell-1} e\left(\frac{hy_n}{M}\right) \right| \le \\
&\le \left| \sum_{\substack{k_1=0\\k=2k_1}}^{2^\ell-1} e\left(\frac{hy_{2k_1}}{M}\right) \right| + \left| \sum_{\substack{k_1=0\\k=2k_1+1}}^{2^\ell-1} e\left(\frac{hy_{2k_1+1}}{M}\right) \right| = \\
&= \left| \sum_{k=0}^{2^\ell-1} e\left(\frac{hF(k)}{M}\right) \right| + \left| \sum_{k=0}^{2^\ell-1} e\left(\frac{hG(k)}{M}\right) \right| + O(m).
\end{aligned}
\tag{20}
$$

In the last part of the formula (20) we into account that the representation y_n as a polynomial on k holds only for $k \ge 2m + 1$.

By (18), the Corollaries 1 and Lemma 2 (from (5)) we easy obtain

$$
|S_\tau(h, y_0)| \le \begin{cases} O(m) & if \quad p = 2,\ \nu_0 < \nu,\ \nu_2(h) < m - 2\nu, \\ 2^{\frac{m+\nu_2(h)+4}{2}} & if \quad \nu_0 \ge \nu,\ \nu_2(h) < m - 2\nu, \\ \tau & else. \end{cases}
$$

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

Corollary 2. *Let* $1 \le N < \tau$. *Then in the notations of Theorem 2 we have*

$$
|S_N(h, y_0)| \le \begin{cases} N & if \quad \nu + \nu_2(h) \ge m, \\ 2^{\frac{m+\nu(h)+4}{2}} \log \tau & if \quad \nu + \nu_2(h) < m. \end{cases}
$$

□

This statement follows from Theorem 2 and Lemma 1.

Let $N \le 2^{m-1}$.

We will study $S_N(h, y_0)$ at the average over $y_0 \in \mathbb{Z}_M^*$.

Theorem 3. *Let a, b, c be parameters of the linear-inversive congruential generator (2) and let $(a, 2) = 1$, $0 < \nu = \nu_2(b) < \nu_2(c)$, $1 \le N \le 2^{m-1}$, $\nu_2(h) = 2^s$, $s < m$. Then the average value of the $S_N(h, y_0)$ over $y_0 \in \mathbb{Z}_M^*$ satisfies*

$$\overline{S}_N(h) = \frac{1}{2^{m-1}} \sum_{y_0 \in \mathbb{Z}_M^*} |S_N(h, y_0)| \le N^{\frac{1}{2}} 2^{-\frac{m}{4}} 2\sqrt{10} \cdot 2^{\frac{\nu+s}{4}},$$

where $s = \nu_2((h, M))$, $h = h_0 2^s$.

Proof. First we will consider the case $s = 0$, i.e. $(h, 2) = 1$. By the Cauchy-Schwarz inequality we get for $\sigma_{k,\ell} = \sigma_{k,\ell}(h, -h; M)$

$$|\overline{S}_N(h)|^2 \le \tfrac{1}{2^{m-1}} \sum_{y_0 \in \mathbb{Z}_M^*} |S_N(h, y_0)|^2 = \tfrac{1}{2^{m-1}} \sum_{k,\ell=0}^{N-1} \sum_{y_0 \in \mathbb{Z}_M^*} e\left(\tfrac{h(y_k - y_\ell)}{M}\right) \le$$

$$\le \tfrac{1}{2^{m-1}} \sum_{k,\ell=0} |\sigma_{k,\ell}| = \tfrac{1}{2^{m-1}} \sum_{r=0}^{\infty} \sum_{\substack{k,\ell=0 \\ \nu_2(k-\ell)=r}}^{N-1} |\sigma_{k,\ell}| = \tfrac{1}{2^{m-1}} \sum_{\gamma=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_2(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}| +$$

$$+ \tfrac{1}{2^{m-1}} \sum_{\substack{k=0 \\ k=\ell}}^{N-1} |\sigma_{k,k}| = N + \tfrac{1}{2^{m-1}} \sum_{\gamma=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_2(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}|.$$

Using Theorem 1 we, after simple calculations, obtain

$$|\overline{S}_N(h)|^2 \le N + \frac{1}{2^{m-1}} \sum_{\gamma=0}^{m-1} \left(\sum_{\substack{k,\ell=0 \\ k \not\equiv \ell (mod\ 2) \\ \nu_2(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}| + \sum_{\substack{k,\ell=0 \\ k \equiv \ell (mod\ 2) \\ \nu_2(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}| \right) \le \tag{21}$$

$$\le N^{\frac{1}{2}} 2^{-\frac{m}{4}} \left(2 + \sqrt{10} \cdot 2^{\frac{\nu}{4}}\right).$$

Now an argument similar to the one used to prove (21) leads to general bound

$$|S_N(h)| \le N^{\frac{1}{2}} 2^{-\frac{m-s}{4}} \left(2 + \sqrt{10} \cdot 2^{\frac{\nu}{4}}\right). \tag{22}$$

□

The estimates of exponential sums obtained in this section we will use for study of properties of the sequence PRN's $\{y_n\}$.

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

For N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1} \in [0, 1)^s$, the discrepancy is defined by

$$D_N^{(s)}(\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1}) := \sup_I \left| \frac{A_N(I)}{N} - |I| \right|,$$

where the supremum is extended over all subintervals I of $[0, 1)^s$, $A_N(I)$ is the number of points among $\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1}$ falling into I, and $|I|$ denotes the s-dimensional volume I.

Let $\{y_n\}$ be the sequence of PRN's generated by (2) and let $x_n = \frac{y_n}{M}$, $n = 0, 1, \ldots$. From our sequence $\{x_n\}$ we derive the sequence $\{X_n^{(s)}\}$ of points in $[0,1)^s$ putting $X_n^{(s)} := (x_n, x_{n+1}, \ldots, x_{n+s-1})$.

We will say the sequence $\{x_n\}$ passes d-dimensional serial test on independence if for every $s \le d$ the sequence $\{X_n^{(s)}\}$ has uniform distribution.

Theorem 4. *The discrepancy $D_N^{(s)}$, $s = 1, 2, 3, 4$, of points constructed by linear-inversive congruential generator (2) with parameters a, b, c, which satisfy the condition*

$$0 < \nu_2(b) = \nu,\ 2\nu < \mu = \nu_2(c),\ \nu_2(a - y_0^2) = \nu_0 \ge 1,\ m \ge 2\nu,\ \nu_0 > \nu,$$

the following bound

$$D_\tau^{(s)} \le \frac{s}{2^{m-\nu+1}} + 2^{-\frac{m-2\nu}{2}} \log^s M. \tag{23}$$

holds.

Proof. Consider only the case $s = 3$ (This case is the most complex). In order to apply Turan-Erdös-Koksma inequality in the Niederreiter's form[6] we must have an estimate for sum

$$\sum_{n=0}^{\tau-1} e\left(\frac{h_1 y_n + h_2 y_{n+1} + h_3 y_{n+2}}{M}\right).$$

Without loss of generality, we can suppose that $(h_1, h_2, h_3, 2) = 1$. From (17)-(19) we can write

$$\begin{array}{c} h_1 y_{2k} + h_2 y_{2k+1} + h_3 y_{2k+2} = \\ = (h_1 y_0 + h_2(a y_0^{-1} + b + c y_0) + h_3 y_0) + \\ +k\left[h_1((1 - a^{-1} y_0^2) b + a y_0^{-1} c(1 - a^{-2} y_0^4) + y_0 b^2) + \right. \\ +h_2(-((1 - a^{-1} y_0^2) b + b y_0^{-1} + a^2 c y_0^{-1})) + \\ +h_3(b(1 - a^{-1} y_0^2) + b a y_0^{-1}(1 - a^{-1} y_0^2) + \\ \left. +y_0 b^2 + 2a^{-1} y_0 b^2 (1 - a^{-1} y_0^2))\right] + \\ +k^2 b^2 (h_1 a^2 - h_2 y_0 (a^{-1} - a^{-2} y_0^2) + h_2 a^2) + 2^\alpha L(h_1, h_2, h_3, k) = \\ = C_0 + C_1 k + C_2 k^2 + 2^\alpha L(h_1, h_2, h_3, k), \end{array} \tag{24}$$

say.

Since the congruences

$$C_1 \equiv 0 (mod\ 2^{2\nu+1})$$

$$C_2 \equiv 0 (mod\ 2^{2\nu+1})$$

cannot be held simultaneously (taking into account that $1 - a^{-1} y_0^2 \not\equiv 0 \pmod{2^{\nu_0}}$) we obtain (by Lemma 2)

$$|\textstyle\sum_1| \le \begin{cases} 2^{\frac{m+\nu}{2}+1} & if \quad A_1(h_1, h_2, h_3) \equiv 0(mod\ 2^{2\nu}), \\ 0 & else. \end{cases} \tag{25}$$

Similarly, we have

$$|\textstyle\sum_2| \le \begin{cases} 2^{\frac{m+\nu}{2}+1} & if \quad B_1(h_1, h_2, h_3) \equiv 0(mod\ 2^{2\nu}), \\ 0 & else, \end{cases} \tag{26}$$

where $B_1(h_1, h_2, h_3)$ defined by the representation

$$h_1 y_{2k+1} + h_2 y_{2k+2} + h_3 y_{2k+3} = B_0 + B_1 k + B_2 k^2 + 2^\alpha M(h_1, h_2, h_3, k).$$

Now, Lemma 4 and simple calculations give

$$D_\tau^{(3)} \le \frac{3}{2^{m-\nu+1}} + 2^{-\frac{m-2\nu}{2}} \log^3 M.$$

□

The assertions of theorem 4 stay held if write N instead τ for $N \leq \tau$.

The Theorem 4 shows that the sequence of PRN's $\{x_n\}$ passe the s-dimensional test on unpredictability (for $s \leq 4$) if this sequence generated by the linear-inversive generator (2) under indicated conditions on the parameters a, b, c, y_0.

Conclusion. Since every nonlinear congruential generator passes also the s-dimensional lattice test for all $s \leq 4$ we conclude that the sequence of PRN's $\{x_n\}$ generated by (2) may be use in applications.

1. **Eichenauer-Herrmann J.** 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.
2. **Eichenauer J.** A non-linear congruential pseudorandom number generator / Eichenauer J., Lehn J. // Statist. Hefte. – 1986. – 27. – P. 315-326.
3. **Eichenauer J.** A nonlinear congruential pseudorandom number generator with power of two modulus / Eichenauer J., Lehn J., Topuzoğlu A. // Math. Comp. – 1988. – 51. – P. 757-759.
4. **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.
5. **Niederreiter H.** Recent trends in random number and random vector generation / Niederreiter H. // Ann. Oper. Res. – 1991. – 31. – P. 323-345.
6. **Niederreiter H.** Random Number Generation and Quasi-Monte Carlo Methods / Niederreiter H. – SIAM, Philadelphia, Pa., 1992.
7. **Varbanets P.** On a nonlinear congruential pseudorandom number generator / Varbanets P., Varbanets S. // Analytic and Probabilistic Methods in Number Theory, Proc. Fifth. International Conference in Honour of J. Kubilius, Palanga, Lithuania, 04-10 Semtember 2011. – 2012. – 17. – P. 265-282.