Chaotic Modeling and Simulation (CMSIM) 3: 267–279, 2016

Inversive generator of the second order for the sequence of PRN's

Sergey Varbanets

Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, str. Dvoryanskaya 2, 65026 Odessa, Ukraine
(E-mail: varb@sana.od.ua)

Abstract. The new inversive congruential method for generating uniform pseudorandom numbers is a particularly attractive alternative to linear congruential generators which have many undesirable regularities. In the present paper, a new inversive congruential generator of the second order for the sequence of PRN's is introduced. Exponential sums on inversive congruential pseudorandom numbers are estimated. The results show that these inversive congruential pseudorandom numbers pass the s-dimensional serial tests for the statistical independency.
Keywords: inversive congruential pseudorandom numbers, exponential sum, discrepancy.

1 Introduction

The uniform pseudorandom numbers (abbrev., PRN's) in the interval $[0, 1]$ are basic ingredients of any stochastic simulation. Its quality is of fundamental importance for the success of the simulation, since the typical stochastic simulation essentially depends on the structural and statistical properties of the producing pseudorandom number generators. In the cryptographical applications of pseudorandom numbers the significant importance is of the availability of property of the unpredictability to generated sequence of pseudorandom numbers. The classical and most frequently used method for generation of PRN's still is the linear congruential method. Unfortunately, its simple linear nature implies several undesirable regularities. Therefore, a variety of nonlinear methods for the generation of PRN's have been introduced as alternatives to linear methods. It is particularly interesting the nonlinear generators for producing the uniform PRN's, such as the inversive generators and its generalizations. Such generators were introduced and studied in [2], [6], [7]. These generators have several attractive properties such as an uniformity, unpredictability (statistical independence), pretty large period and simple calculative complexity. The most common types of the inversive generators define by the following congruential recursions.

Received: 18 January 2016 / Accepted: 14 April 2016

ISSN 2241-0503

Let F_q be a finite field with q elements and let y_0, a, b belong F_q. Put

$$y^{-1} = \begin{cases} 0 \; if \; y = 0, \\ \text{multiplicative inverse to } y \text{ in } F_q^* \text{ if } y \neq 0. \end{cases}$$

Then the recursion

$$y_{n+1} = ay_n^{-1} + b, \; n = 0, 1, 2, \ldots. \tag{1}$$

produces the inversive congruential generator over F_q.
The generator (1) was introduced in [2], [6], [7], [11].

Other inversive generators consider over the ring Z_{p^m}.

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

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{p^m}, (a, b \in Z), \tag{2}$$

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 the works of Eichenauer, Lehn, Topuzoğlu[3]; Niederreiter, Shparlinski[10]; Eichenauer, Grothe[5] etc. were proved that the inversive congruential generator (2) 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, [9],[12]). 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 (2) as a stream cipher. At the last time it has been shown that we must be careful in the time of using the generator (2).

We call the generator (2) the inversive generator with constant shift.

In [14] we have given two generalization for the generator (2). The first generalization connects with the recurrence relation

$$y_{n+1} \equiv a\overline{y}_n + b + cF(n+1)y_0 \pmod{p^m} \tag{3}$$

under conditions

$$(a, p) = (y_0, p) = 1, \; b \equiv c \equiv 0 \pmod{p}, \; F(u) \text{ is a polynomial over } Z[u].$$

We call the generator (3) the inversive congruential generator with a variable shift $b + cF(n+1)y_0$. The computational complexity of generator (3) is the same as for the generator (2), but the reconstruction of parameters a, b, c, y_0, n and polynomial $F(n)$ is a tricky problem even if the several consecutive values $y_n, y_{n+1}, \ldots, y_{n+N}$ will be revealed (for example, even the reconstruction of three-term polynomial $F(u)$ of large unknown degree is a very hard problem). Thus the generator (3) can be used in the cryptographical applications. Notice that the conditions $(a, p) = (y_0, p) = 1$, $b \equiv c \equiv 0 \pmod{p}$ guarantee that the

recursion (3) produces the infinite sequence $\{y_n\}$.

The second congruential recursion has the form

$$y_{n+1} \equiv a\overline{y}_n + b + cy_n \pmod{p^m} \tag{4}$$

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

We call the generator (4) the linear-inversive congruential generator.

We must notice that the conditions $a \equiv b \equiv 0 \pmod{p}$, $(y_0,p)=(c,p)=1$ also give to generate the sequence of PRN's with appropriate properties for PRN's $\{x_n\}$. However, the conditions $a \equiv c \equiv 0 \pmod{p}$, $(y_0,p) > (b,p) = 1$ don't permit to construct the required sequence of PRN's.

For the case $p = 2$, Kato, Wu, Yanagihara[7] studied the generator (4). These authors proved that the appropriate sequence of PRN's $\{x_n\}$ has a period $\tau = 2^{m-1}$ if and only if $a + c \equiv 1 \pmod{4}$ and $b \equiv 3 \pmod{4}$.

The present paper deals with the congruential inversive generator of second order determined by the recursion

$$y_{n+1} \equiv a(y_{n-1}y_n)^{-1} + b \pmod{p^m}, \tag{5}$$

where $(a,p)=1$, $b \equiv 0 \pmod{p}$, $(y_0,p)=(y_1,p)=1$.

Notice that the superimposed requirements on a, b, y_0, y_1 permit to define every value y_n, $n = 2,3,\ldots$.

Our purpose in this work is to show passing the test on equidistribution and statistical independence for the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$, and hence, the main point to be shown is the possibility for such sequences to be used in the problem of real processes modeling and in the cryptography.

In the sequel we will use the following notation.

2 Notation and auxiliary results

Variables of summation automatically range over all integers satisfying the condition indicated. The letter p denotes a prime number, $p \geq 3$. For $m \in N$ the notation Z_{p^m} (respectively, $Z^*_{p^m}$) denotes the complete (respectively, reduced) system of residues modulo p^m.For $z \in Z$, $(z,p)=1$ let z^{-1} be the multiplicative inverse of z modulo p^m. We write $\nu_p(A) = \alpha$ if $p^\alpha | A$, $p^{\alpha+1} \nmid A$. For integer t, the abbreviation $e_m(t) = e^{\frac{2\pi i t}{p^m}}$ is used.

We need the following simple statements.

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

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

Lemma 1. *The following estimate*

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

holds.

This statement is well-known lemma about an estimate of uncomplete exponential sum by means of the complete exponential sum.

Lemma 2. *Let h_1, h_2, k, ℓ be positive integers and let $\nu_p(h_1 + h_2) = \alpha$, $\nu_p(h_1k + h_2\ell) = \beta$, $\delta - \min(\alpha, \beta)$. Then for every $j = 2, 3, \dots$ we have*

$$\nu_p(h_1k^{j-1} + h_2\ell^{j-1}) \geq \delta.$$

Proof. By the equality

$$h_1k^j + h_2\ell^j = (h_1k^{j-1} + h_2\ell^{j-1})(k + \ell) - k\ell(hk^{j-2} + h_2\ell^{j-2}),$$

applying the method of mathematical induction, we obtain at once $\nu_p(h_1k^j + h_2\ell^j) \geq \delta$, $j = 2, 3, \dots$ □

Lemma 3. *Let $p > 2$ be a prime number, $f(x)$, $g(x)$ be polynomials over Z*

$$f(x) = A_1x + A_2x^2 + \cdots, \ \ g(x) = B_1x + B_2x^2 + \cdots,$$

$$\nu_p(A_j) = \lambda_j, \ \ \nu_p(B_j) = \mu_j, \ \ j = 1, 2, 3, \dots$$

and, moreover, $\alpha = \lambda_2 \leq \lambda_3 \leq \cdots$, $0 = \mu_1 < \mu_2 \leq \mu_3 \leq \cdots$.

Then for $m \geq 2$ the following bounds occur

$$\left|\sum_{x \in Z_{p^m}} e_m(f(x))\right| \leq \begin{cases} 2p^{\frac{m+\alpha}{2}} & if\ \nu_p(A_1) \geq \alpha, \\ 0 & if\ \nu_p(A_1) < \alpha; \end{cases}$$

$$\left|\sum_{x \in Z^*_{p^m}} e_m(f(x) + g(x^{-1}))\right| \leq I(p^m)p^{\frac{m}{2}}$$

where $I(p^m)$ is a solution of the congruence

$$f'(y) \equiv g(y^{-1}) \cdot y^{-1} \pmod{p^{m-m_0}}.$$

Proof. Putting $x = y(1 + p^{m_0}z)$, $y \in Z^*_{p^{m_0}}$, $z \in Z_{p^{m-m_0}}$, we have modulo p^m

$$x^k = y^k + kp^{m_0}y^kz, \ \ (x^{-1})^k = y^k - kp^{m_0}y^kz.$$

And then we obtain modulo p^m

$$f(x) + g(x^{-1}) = f(y) + g(y) + p^{m_0}(f'(y) - y^{-1}g'(y^{-1}))z.$$

Hence,

$$\sum_{x \in Z^*_{p^m}} e_m(f(x) + g(x^{-1})) =$$

$$= \sum_{y \in Z^*_{p^{m_0}}} e_m(f(y) + g(y^{-1})) \sum_{z \in Z_{p^{m-m_0}}} e_m((f'(y) - y^{-1}g'(y^{-1}))z) =$$

$$= p^{m-m_0} \sum_{\substack{y \in Z^*_{p^{m_0}} \\ f'(y) \equiv y^{-1}g'(y^{-1}) \pmod{p^{m-m_0}}}} e_m(f(y) + g(y^{-1})).$$

Now, if $m = 2m_0$, we obtain

$$\left| \sum_{x \in Z_{p^m}^*} e_m(f(x) + g(x^{-1})) \right| = p^{\frac{m}{2}} I(p^m).$$

For $m = 2m_0 + 1$ we put $y = y_j + p^{m-m_0}t$, $t \in Z_p$, y_j runs all solutions of the congruence $f'(y) \equiv y^{-1}g'(y^{-1}) \pmod{p^{m-m_0}}$ over $Z_{p^{m-m_0}}^*$. Then setting $y = y_j(1 + pt)$, $t \in Z_p$, we obtain

$$\sum_{\substack{y \in Z_{p^{m_0}}^* \\ f'(y) \equiv y^{-1}g'(y^{-1}) \pmod{p^{m-m_0}}}} e_m(f(y) + g(y^{-1})) =$$

$$= \sum_{j=1}^{I(p^m)} e_m(f(y_j) + g(y_j^{-1})) \sum_{t \in Z_p} e_{m-2m_0}\left(\frac{f'(y_j) - y_j^{-1}g'(y_j^{-1})}{p^{m_0}} t + B_1 y_j^{-2} t^2 \right).$$

The inner sum in right side of last equality is the Gaussian sum. Consequently, we finally have

$$\left| \sum_{x \in Z_{p^m}^*} e_m(f(x)_g(x^{-1})) \right| \le p^{\frac{m}{2}} \cdot I(p^m).$$

□

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

$$D(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}) = \sup_I \left| \frac{A_N(I)}{N} - |I| \right|, \tag{5.1}$$

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

For study the discrepancy of points usually use the following lemmas.

For integers $q \ge 2$ and $d \ge 1$, let $C_q(d)$ denote the set of all nonzero lattice points $(h_1, \ldots, h_d) \in Z^d$ with $-\frac{q}{2} < h_j \le \frac{q}{2}$, $1 \le j \le d$. We define

$$r(h,q) = \begin{cases} q \sin \frac{\pi |h|}{q} & if\ h \in C_1(q), \\ 1 & if\ h = 0 \end{cases}$$

and

$$r(\mathfrak{h}, q) = \prod_{j=1}^{d} r(h_j, q) \quad for\ \mathfrak{h} = (h_1, \ldots, h_q) \in C_d(q).$$

Lemma 4 (Niederreiter,[9]). *Let $N \ge 1$ and $q \ge 2$ be integers. For N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1} \in [0,1)^d$, the discrepancy $D(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1})$ satisfies*

$$D_N(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}) \le \frac{d}{q} + \frac{1}{N} \sum_{\mathfrak{h} \in C_d(q)} \frac{1}{r(\mathfrak{h}, q)} \left| \sum_{n=0}^{N-1} e(\mathfrak{h} \cdot \mathfrak{t}_n) \right|.$$

Lemma 5. *Let* $\{\mathfrak{y}_k\}$, $\mathfrak{y}_k \in \{0,1,\dots,q-1\}^d$, *is a purely periodic sequence with a period* τ. *Then for the discrepancy of the points* $\mathfrak{t}_k = \frac{\mathfrak{y}_k}{q} \in [0,1)^d$, $k = 0,1,\dots,N-1$; $N \le \tau$, *the following estimate*

$$D_N(\mathfrak{t}_0,\mathfrak{t}_1,\dots,\mathfrak{t}_{N-1}) \le \frac{d}{q} + \frac{1}{N}\sum_{\mathfrak{h}\in C_d(q)}\sum_{h_0\in\left(-\frac{\tau}{2},\frac{\tau}{2}\right]} r^{-1}(\mathfrak{h},q)r^{-1}(h_0,\tau)\cdot|\mathfrak{S}|$$

holds,

where $\mathfrak{S} := \sum\limits_{k=0}^{\tau-1} e(\mathfrak{h}\cdot\mathfrak{t}_k + \frac{kh_0}{\tau})$.

This assertion follows from Lemma 4 and from an estimate of uncomplete exponential sum through complete exponential sum (see, Lemma 1).

3 Preparations

We will obtain the representation of y_n in the form of rational function on y_0.

Denote $\nu_p(b) = \nu_0$. A straightforward computation by recursion (5) shows that modulo $p^{3\nu_0}$ we have

$$y_2 = \frac{a+by_0y_1}{y_0y_1},\quad y_3 = \frac{ay_0+ab+b^2y_0y_1}{ay_0y_1+aby_0+ab^2},\quad y_4 = \frac{ay_0y_1+aby_0+ab^2}{ay_0+ab+b^2y_0y_1},$$
$$y_5 = \frac{2a^2b+a^2y_0+3ab^2y_0y_1}{a^2+2aby_0y_1+ab^2y_0},\quad y_6 = \frac{2a^2b+a^2y_0+3ab^2y_0y_1}{a^2+2aby_0y_1+ab^2y_0}.$$

These relations give rise to proposal that representation of y_n will be found in the form of

$$y_n = \frac{A_0^{(n)}+A_1^{(n)}y_0+A_2^{(n)}y_0y_1}{B_0^{(n)}+B_1^{(n)}y_0+B_2^{(n)}y_0y_1}, \tag{6}$$

where $A_j^{(n)}$, $B_j^{(n)}$ are the polynomials from $Z[n]$. From the above, for y_n we involve

$$y_{n+2} = \frac{(aB_0^{(n)}+bA_0^{(n+1)})+(aB_1^{(n)}+bA_1^{(n+1)})y_0+(aB_2^{(n)}+bA_2^{(n+1)})y_0y_0}{A_0^{(n+1)}+A_1^{(n+1)}y_0+A_2^{(n+1)}y_0y_1} \tag{7}$$

Now, a straightforward computation suggest that modulo $p^{3\nu_0}$ we have

$$\begin{cases} A_0^{(3k-1)} \equiv a^k,\ A_1^{(3k-1)} \equiv (k^2-3k+3)a^{k-1}b^2,\\ A_2^{(3k-1)} \equiv ka^{k-1}b+6(k-3)a^{k-2}b^2;\\ B_0^{(3k-1)} = \dfrac{k(k-1)}{2}a^{k-1}b^2,\ B_1^{(3k-1)} = (3k-1)-2(k-2)a^{k-1}b,\\ B_2^{(3k-1)} = a^{k-1}+6a^{k-2}b; \end{cases} \tag{8}$$

$$\begin{cases} A_0^{(3k)} \equiv ka^kb,\ A_1^{(3k)} \equiv 2a^k; A_2^{(3k)} \equiv \dfrac{k(k+1)}{2}a^{k-1}b^2;\\ B_0^{(3k)} \equiv a^k,\ B_1^{(3k)} \equiv (k^2-3k+3)a^{k-1}b^2;\\ B_2^{(3k)} \equiv ka^{k-1}b+6(k-3)a^{k-1}b^2; \end{cases} \tag{9}$$

$$\begin{cases} A_0^{(3k+1)} = a^{k+1} + ka^k b^2,\ A_1^{(3k+1)} = (k^2-3k+3)a^k b^2 + 2a^k b; \\ A_2^{(3k+1)} = ka^k b + 6(k-3)a^{k-1}b^2; \\ B_0^{(3k+1)} = ka^2 b,\ B_1^{(3k+1)} = 2a^k;\ B_2^{(3k+1)} = a^{k-1}b^2. \end{cases} \tag{10}$$

The validity of the formulas (8), (9) is not difficult establishes by the method of mathematical induction. The formula (10) follows by recursion (5). Other summands of A_j^n, $j = 0, 1, 2$; $n = \{3k-1$ or $3k$ or $3k+1\}$, which modulo $p^{3\nu_0}$ are equal to 0, be represented the polynomials from $Z[n]$ (it comes from formula (7)). So, we may write

$$A_0^{(3k-1)} = a^k + p^{3\nu_0}F_0(k), \ldots, B_2^{3k-1} = a^{k-1} + 6(k-3)a^{k-2}b^2 + p^{3\nu_0}G_2(k).$$

The number summands in any $F_j(k)$ or $G_j(k)$, $j = 0, 1, 2$ be less than $4m_0$, where $m_0 = \left[\frac{m+1}{\nu_0}\right]$ by virtue when passing from k to $k+2$ "old" coefficients gets multiplier divisible to $a \cdot b$.Therefore, appearance of the polynomials $F_j(k)$, $G_j(k)$ rallies, moreover, all summands in the polynomials $F_j(k)$, $G_j(k)$ contains factor a^ℓ, $k - m_0 \le \ell \le k$.

The relation (6) shows that for every $k = 0, 1, 2, \ldots$ the numerator and denominator contain a summand that is coprime to p, and every such summand contains the factor a^k. Multiply out numerator and denominator on multiplicative inverse modp^m to the respective summand of denominator and applying the expanding $(1+pu)^{-1} = 1 - pu + p^2u^2 - \cdots + (-1)^{m-1}(pu)^{m-1} \pmod{p^m}$, we obtain the representation of y_k power expansion of k with coefficients which depend only on y_0, y_1 and $(a^{-1})^j$, $0 \le j \le m$, where $a \cdot a^{-1} \equiv 1 \pmod{p^m}$.

So, after simple calculations we deduce modulo p^m

$$y_{3k-1} = y_0^{-1}y_1^{-1} \cdot S_1 \cdot S_2$$

where

$$S_1 = \Big[a + (k^2-3k+3)b^2y_0 + \\ + (b + 6(k-3)a^{-1}b^2)y_0y_1 + p^{3\nu_0}G(k, y_0, y_1)\Big]$$

$$S_2 = \Big[1 - 6a^{-1}by_0y_1 - \frac{k(k-1)}{2}b^2 - (2k-4)b^2 - \\ - (2k-4)by_0 + 36a^{-2}b^2(y_0y_1)^2 + (2k-4)^2b^2y_0^2 + \\ + 12(2k-4)a^{-1}b^2y_0^2y_1 + p^{3\nu_0}F(k, y_0, y_1)\Big]$$

From where we have

$$y_{3k-1} = y_0^{-1}y_1^{-1}\Big\{(a + bc_0) + kb(1 - 2ay_1^{-1}) + \\ + k^2b^2(y_0 - \frac{1}{2}ay_1^{-1} + 4ay_1^{-1}) + b^3H(k, y_0, y_1)\Big\} \tag{11}$$

where $c_0 = -6a^{-1}by_0y_1 + b^2(3y_0 + 8a + 36a^{-1}(y_0y_1)^2 + 16ay_0^2 - 48y_0^2y_1) + 4by_0a$.

Next, by analogy, we infer

$$\begin{aligned} y_{3k} = [2y_0 - 3a^{-1}b^2y_0(1 - ba^{-1}y_1)] + kb(1 + bh(k)) + \\ + k^2b^2(-\frac{1}{2}a^{-1}y_0y_1 - 2a^{-1}y_0^2) + p^{3\nu_0}L(k, y_0, y_1), \end{aligned} \tag{12}$$

where $h(k) = 6a^{-1}by_0^2 - 12a^{-1}by_0^2y_1$,

$$\begin{aligned} y_{3k+1} = 2^{-1}y_0^{-1}[a + 2by_0 + 3b^2y_0(1 - 6a^{-1}y_1)] + \\ + kb(y_0y_1 - 2^{-1}ay_0^{-1} + p^{3\nu_0}b(-3y_0)) + \\ + k^2b^2(y_0 + 2^{-1}ay_0^{-2} - 2^{-2}y_0^{-1} - 2^{-1}y_1^{-1}) + p^{3\nu_0}M(k, y_0, y_1)y_0^{-1}. \end{aligned} \tag{13}$$

From (11)-(13) we infer the following statement.

Proposition 1. *Let the sequence $\{y_n\}$ be produced by the recursion (5) with $(a, p) = (y_0, p) = (y_1, p) = 1$, $\nu_p(b) = \nu_0 > 0$. There exist the polynomials $F_{-1}(x), F_0(x), F_1(x) \in Z[x]$ with the coefficient depending on y_0, y_1, such that*

$$\begin{aligned} y_{3k-1} = y_0^{-1}y_1^{-1}((a + b(-6a^{-1}y_0y_1) + b^2B_0(y_0, y_1)) + \\ + kb(1 - 2ay_1^{-1} + bB_1(y_0, y_1)) + \\ + k^2b^2(y_0 - \frac{7}{2}ay_1^{-1} + bB_2(y_0, y_1))) + p^{3\nu_0}F_{-1}(k) \end{aligned} \tag{14}$$

$$\begin{aligned} y_{3k} = (2y_0 + b^2C_0(y_0, y_1)) + kb(1 + bC_1(y_0, y_1)) + \\ + k^2b^2(-\frac{1}{2}a^{-1}y_0y_1 - 2a^{-1}y_0^2) + p^{3\nu_0}F_0(k) \end{aligned} \tag{15}$$

$$\begin{aligned} y_{3k+1} = 2^{-1}y_0^{-1}(a + 2by_0 + 3b^2y_0(1 - ba^{-1}y_1)) + kb(y_0y_1 - 2^{-1}ay_0^{-1}) + \\ + k^2b^2(y_0 + 2^{-1}ay_0^{-2} - (2^{-1})^2y_0^{-1} - 2^{-1}y_1^{-1}) + p^{3\nu_0}F_1(k). \end{aligned} \tag{16}$$

In process of proof the Proposition 1 we obtain also the following corollaries.

Corollary 1. *For $k = 2, 3, \ldots$, we have*

$$\begin{aligned} y_{3k-1} = (a + kb + 8ab^2)y_0^{-1}y_1^{-1} + (-2akb + \frac{7}{2}ak^2b^2)y_0^{-1}y_1^{-2} + \\ + (4ab + 3b^2 + k^2b^2)y_1^{-1} + 16ab^2y_0y_1^{-1} + \\ + 48b^2y_0 - 6a^{-1}b + p^{3\nu_0}f_{-1}(y_0, y_1) \end{aligned} \tag{17}$$

$$\begin{aligned} y_{3k} = kb + (2 - 3a^{-1}b^2)y_0 + (18a^{-2}b^2)y_0y_1 + (6a^{-1}b^2k - 2a^{-1}b^2k^2)y_0^2 - \\ - 12a^{-1}kb^2y_0y_1 + p^{3\nu_0}f_0(y_0, y_1) \end{aligned} \tag{18}$$

$$\begin{aligned} y_{3k+1} = 2^{-1}ay_0^{-1} + (b + 2^{-1}k^2b + 3b^2) + (-3a^{-1}b^2 + kb)y_1 + \\ + (-2^{-2}abk - 2^{-2}k^2b^2)y_0^{-2} + (-2^{-3}k^2b^2)y_0^{-3} - 2^{-2}y_0^{-1}y_1^{-1} + \\ + p^{3\nu_0}f_1(y_0, y_1), \end{aligned} \tag{19}$$

where f_{-1}, f_0, f_1 are homographic (rational) functions at y_0, y_1.

This Corollary at once follows from (11)-(13).

Corollary 2. *Let τ be a period length of the sequence $\{y_n\}$ generated by recursion (5); y_0, y_1 be initial values, and let $\nu_p(b) = \nu_0 > 0$. Then we have*

$$\begin{array}{ll}(A)\ \tau = 3p^{m-\nu_0} & \text{if only one congruence } 4y_0^2 \equiv a \pmod p \\ & \text{or } y_1 \equiv 2 \pmod p \text{ violates;} \\ (B)\ \tau = 3p^{m-\nu_0-\delta} & \text{if } \min(\nu_p(4y_0^2 - a), \nu_p(y_1 - 2)) = \delta < m - \nu_0; \\ (C)\ \tau \le 3p^{m-\nu_0-\delta} & \text{otherwise.}\end{array}$$

Proof. Let $4y_0^2 \equiv a \pmod p$. Then, assuming $y_{3k} \equiv y_{3\ell+1} \pmod{p^m}$, we obtain $2y_0 \equiv 2^{-1}ay_0^{-1} \pmod p$. This gives a contradiction.

Similarly, from $y_{3k-1} \equiv y_{3\ell+1} \pmod{p^m}$ and $y_{3k} \equiv y_{3\ell+1} \pmod{p^m}$ we infer $y_0^{-1}y_1^{-1}a \equiv 2^{-1}ay_0^{-1} \pmod p$ and $2y_0 \equiv 2^{-1}ay_0^{-1} \pmod p$, i.e. $y_1 \equiv 2 \pmod p$ and $4y_0^2 \equiv a \pmod p$.

Let $n_1 \equiv n_2 \pmod 3$. Then from Corollary 1 we deduce that $y_{n_1} \equiv y_{n_2} \pmod{p^m}$ if and only if $n_1 \equiv n_2 \pmod{p^{m-\nu_0}}$. Hence, $\tau = 3p^{m-\nu_0}$. the second and third parts of Corollary 3 are also clear. □

4 Exponential sums over the sequence of PRN's

In this section we prove the theorems 1-3 on the estimates of exponential sums on the sequence of pseudorandom numbers $\{y_n\}$ which are generated by recursion (5).

Let

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

Here we consider y_k, y_ℓ as a functions of initial values y_0, y_1 generated by (5).

Theorem 1. *Let $(h_1, h_2, p) = 1$, $\nu_p(h_1 + h_2) = \mu_1$, $\nu_p(h_1 k + h_2 \ell) = \mu_2$, $k, \ell \in Z_{\ge 0}$ and let $\{y_n\}$ produced by (5). The following estimates*

$$|\sigma_{k,\ell}(h_1, h_2; p^m)| \le \begin{cases} 0 & if\ k \not\equiv \ell \pmod 3,\ \nu_p(h_2) > 0, \\ 4p^{m+\nu_0} & if\ \nu_p(h_2) = 0,\ k \not\equiv \ell \pmod 3, \\ 0 & if\ \mu_1 = 0,\ k \equiv \ell \pmod 3, \\ 4p^{m+\nu_0} & if\ \min(\mu_1, \mu_2) \ge \nu_0,\ k \equiv \ell \pmod 3. \end{cases}$$

hold.

Proof. Without restricting the generality it may be assumed that $(h_1, h_2, p) = 1$, $(h_1, p) = 1$. We considerate two cases:

(I) Let k and ℓ be nonnegative integers with $k \not\equiv \ell \pmod 3$, i.e. $k = 3k_1 \pm 1$, $\ell = 3\ell_1$ or $k = 3k_1 - 1$, $\ell = 3\ell_1 + 1$.
For $k = 3k_1$, $\ell = 3\ell_1 + 1$, by Corollary 1 we have

$$h_1 y_{3k_1} + h_2 y_{3\ell_1+1} = A_0 + A_1 y_0 + A_2 y_0^{-1} + bg_1(y_0^{-1}) + bB_1 y_1^{-1} + B_2 y_1^{-1} + bg_2(y_1^{-1}),$$

where modulo p^{ν_0}

$$A_1 = 2h_1,\ A_2 = 2^{-1}h_2,\ B_1 = h_2k,\ B_2 = -2^{-2}y_0^{-1}.$$

Thus, by Lemma 3, we easily infer

$$|\sigma_{3k_1-1,3\ell}(h_1,h_2)| \le \begin{cases} 0 & if\ \nu_p(h_2) > 0, \\ 4p^{m+1} & if\ \nu_p(h_2) = 0. \end{cases}$$

Such result gives the case $k = 3k_1$, $\ell = 3\ell_1 + 1$ or $k = 3k_1 - 1$, $\ell = 3\ell_1 + 1$.

(II) Let $k \equiv \ell \pmod 3$. For definiteness we will consider only the case $k \equiv \ell \equiv 0 \pmod 3$. Then we have from Corollary 1

$$\begin{aligned} h_1y_{3k} + h_2y_{3\ell} = {} & (h_1k + h_2\ell)b + (h_1 + h_2)(2 - 3a^{-1}b^2)y_0 + \\ & + (h_1 + h_2)18a^{-2}b^2y_0y_1 + 6a^{-1}b^2(h_1k + h_2\ell) - \\ & - 2a^{-1}b^2(h_1k^2 + e_2\ell^2)y_0^2 - 12a^{-1}b^2(h_1k + h_2\ell)y_0y_1 + \\ & + p^{3\nu_0}\sum_{j=0}^{m_0} a_j(h_1k^j + h_2\ell^j)f_j(y_0,y_1). \end{aligned}$$

Again, by Lemmas 2 and 3, we obtain

$$|\sigma_{3k,3\ell}(h_1,h_2)| \le \begin{cases} 0 & if\ \mu_1 = 0,\ k \equiv \ell \pmod 3, \\ 4p^{m+1} & if\ \min(\mu_1,\mu_2) \ge \nu_0,\ k \equiv \ell \pmod 3. \end{cases}$$

In the cases (I) and (II) we take into account that $I(p^m)$ (see, the notation in Lemma 3) are zero or 2. □

Let the least length of period for $\{y_n\}$ is equal to τ.

Theorem 2. *Let the linear-inversive congruential sequence generated by the recursion (5) has the period τ, and let $\nu_p(b) = \nu_0$ and $4y_0^2 \not\equiv a \pmod p$ or $y_1 \not\equiv 2 \pmod p$. Then the following bounds*

$$|S_\tau(h,y_0)| \le \begin{cases} O(m) & if \quad \delta > \nu_0,\ n_p(h) < m - 2\nu_0 - \delta, \\ 4p^{\frac{m+\nu_p(h)}{2}} & if \quad \delta \ge \nu_0,\ \nu_p(h) < m - 2\nu_0, \\ \tau & otherwise. \end{cases}$$

hold,
with the constant implied by the O-symbol is absolute.

Proof. Let we have the sequence produced by recursion (5). Without lose the generality, we cas assume that the sequence $\{y_n\}$ has a period $\tau = 3p^{m-\nu_0}$. By Corollary 2 we have

$$\begin{aligned} |S_\tau(h,y_0,y_1)| = \left|\sum_{n=0}^{\tau-1} e_m(hy_n)\right| = \left|\sum_{n=0}^{3p^{m-\nu}-1} e_m(hy_n)\right| \le \\ \le \left|\sum_{k=1}^{p^{m_1}} e_m(hy_{3k-1})\right| = \left|\sum_{k=1}^{p^{m_1}} e_m(hy_{3k+1})\right| + O(m), \end{aligned} \tag{20}$$

where $m_1 = m - \nu_0$, and

$$y_{3k-1} = F_{-1}(k) := A_0 + A_1 k + A_2 k^2 + \cdots$$
$$y_{3k} = F_0(k) := B_0 + B_1 k + B_2 k^2 + \cdots$$
$$y_{3k+1} = F_1(k) := C_0 + C_1 k + C_2 k^2 + \cdots$$

with A_i, B_i, C_i defined by Proposition 1.

The summand $O(m)$ in (20) appears in virtue of the fact that the representation y_n as a polynomial on k holds only $k \geq 2m_0 + 1$.

Thus, by Lemma 3 we easily obtain

$$|S_\tau()| \leq \begin{cases} O(m) & if\ \delta < \nu_0,\ \nu_p(h) < m - \nu_0 - \delta, \\ 4p^{\frac{m+\nu_p(h)}{2}} & if\ \delta \geq \nu_0,\ \nu_p(h) < m - 2\nu_0, \\ \tau & otherwise. \end{cases}$$

with the constant implied by the O-symbol is absolute. □

Theorem 3. *Let the sequence $\{y_n\}$ be produced by (5) with parameters a, b, y_0, y_1, $(a,p) = (y_0 y_1, p) = 1$, $\nu_p(b) = p^{\nu_0}$, $\nu_0 \geq 1$. Then for every $h \in Z$, $(h, p^m) = \mu \leq m$, we have*

$$\overline{S}_N(h) = \frac{1}{(\varphi(p^m))^2} \sum_{y_0, y_1 \in Z^*_{p^m}} |S_N(h, y_0, y_1)| \leq 12N^{\frac{1}{2}} + 12Np^{-\frac{m-\nu_0}{2}}.$$

Proof. Let $\nu_p(h) = 0$, i.e. $(h,p) = 1$. By the Cauchy-Schwarz inequality we get

$$\left|\overline{S}_N(h)\right|^2 = \frac{1}{(\varphi(p^m))^2} \left| \sum_{y_0, y_1 \in Z^*_{p^m}} \sum_{n=0}^{N-1} e_m(h y_n) \right|^2 =$$
$$= \frac{1}{(\varphi(p^m))^2} \sum_{y_0, y_1 \in Z^*_{p^m}} \sum_{k,\ell=0}^{N-1} e_m(h(y_k - y_\ell)) \leq$$
$$\leq \frac{1}{(\varphi(p^m))^2} \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h,-h)| = \frac{1}{(\varphi(p^m))^2} \sum_{r=0}^{\infty} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=r}}^{N-1} |\sigma_{k,\ell}(h,-h)| =$$
$$= \frac{1}{(\varphi(p^m))^2} \sum_{t=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=t}}^{N-1} |\sigma_{k,\ell}(h,-h)| + \frac{1}{(\varphi(p^m))^2} \sum_{k=0}^{N-1} |\sigma_{k,k}(h,-h)| =$$
$$= N + \frac{1}{(\varphi(p^m))^2} \sum_{t=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=t}}^{N-1} |\sigma_{k,\ell}(h,-h)|.$$

Using Theorem 1, we obtain

$$\left|\overline{S}_N(h)\right|^2 \leq N + \frac{1}{(\varphi(p^m))^2} \times$$

$$\times \sum_{r=0}^{m-1}\left(\sum_{\substack{k,\ell=0\\ k\not\equiv\ell \pmod 3\\ \nu_p(k-\ell)=r}}^{N-1}|\sigma_{k,\ell}(h,-h)|+\sum_{\substack{k,\ell=0\\ k\equiv\ell \pmod 3\\ \nu_p(k-\ell)=r}}^{N-1}|\sigma_{k,k}(h,-h)|\right)\le$$

$$\le N+\frac{1}{(\varphi(p^m))^2}\times$$

$$\times\left[4p^m\sum_{r=0}^{m-1}\frac{N^2}{p^r}+\left(\sum_{r<m-\nu_0}+\sum_{m-\nu_0\le r\le m-1}\right)\sum_{\substack{k,\ell=0\\ k\equiv\ell \pmod 3}}^{N-1}|\sigma_{k,\ell}(h,-h)|\right]\le$$

$$\le N+\frac{N}{(\varphi(p^{(m)}))^2}\times$$

$$\times\left(4Np^m+\sum_{r<m-\nu_0}\frac{N}{p^r}p^{m+\nu_0+r}+p^m\sum_{r\ge m-\nu_0}\frac{N}{p^r}\right)\le$$

$$\le N+N^2p^{-m}\cdot 11p^{\nu_0}(m-\nu_0).$$

Hence, for $(h,p)=1$ we obtain

$$\left|\overline{S}_N(h)\right|\le N^{\frac12}+12Np^{-\frac{m-\nu_0}{2}}.$$

□

Theorems 1-3 and Lemmas 4-5 permit to obtain the following bound for discrepancy pf the sequence of point $\{\frac{y_n}{p^m}\}\in[0,1)$ and points $X_n^{(s)}\in[0,1)^s$, $X_n^{(s)}=\left(\frac{y_n}{p^m},\frac{y_{n+1}}{p^m},\dots,\frac{y_{n+s-1}}{p^m}\right)$, where $\{y_n\}$ is generated by the recursion (5).

Theorem 4. *Let $p>2$ be a prime number, $y_0,y_1,a,b,m\in N$, $m\ge 3$, $(ay_0y_1,p)=1$, $\nu_p(b)=\nu_0\ge 1$. Then for the sequence $\{x_n\}$, $x_n=\frac{y_n}{p^m}$, $n=0,1,\dots$, with the period τ, generated by recursion (5), we have for any $1\le N\le\tau$,*

$$D_N(x_0,x_1,\dots,x_{N-1})\le\frac{1}{p^m}+3N^{-1}p^{\frac{m-\nu_0}{2}}\left(\frac1p\left(\frac{2}{\pi}\log p^m+\frac75\right)^2+1\right).$$

Theorem 5. *Let the sequence $\{X_n^{(s)}\}$ with the period $\tau=3p^{m-\nu_0}$ be produced by recursion (5). Then its discrepancy*

$$D_N^{(s)}(X_0^{(s)},\dots,X_{\tau-s}^{(s)})\le 2p^{-\frac{m}{2}+\nu_0}\left(\frac1\pi\log p^{m-\nu_0}+\frac35\right)^s+2p^{-m+\nu_0}$$

for every $s=1,2,3,4$.

The assertions of Theorems 4 and 5 are the simple conclusions of Theorems 2 and 3 and Lemmas 4 and 5.

From Theorems 4 and 5 we conclude that the sequence of PRN's $\{y_n\}$ produced by generater (5) passes the s-dimensional serial test on the equidistribution and statistical independency.

References

1. W.-S. Chou. The period lengths of inversive congruential recursions. *Acta Arith*, 73(4), 325-341, 1995.
2. J. Eichenauer and J. Lehn. A non-linear congruential pseudorandom number generator. *Statist. Hefte*, 27, 315-326, 1986.
3. J. Eichenauer, J. Lehn and A. Topuzoğlu. A nonlinear congruential pseudorandom number generator with power of two modulus. *Math. Comp.*, 51,757-759, 1988.
4. J. Eichenauer-Herrmann and A. Topuzoğlu. On the period of congruential pseudorandom number sequences generated by inversions. *J. Comput. Appl. Math.*, 31, 87-96, 1990.
5. J. Eichenauer-Herrmann, H. Grothe. A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus. *ACM Transactions of Modelling and Computer Simulation*, 2(1), 1-11, 1992.
6. T. Kato T., L.-M. Wu, N. Yanagihara. The serial test for a nonlinear PRN's generator. *Math. Comp.*, 63(214), 761-769, 1996.
7. T. Kato, L.-M. Wu, N. Yanagihara. On a nonlinear congruential pseudorandom number generator. *Math. of Comp.*, 65(213), 227-233, 1996.
8. H. Niederreiter. Some new exponential sums with applications to pseudorandom numbers. *Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. Janos. Bolyai, vol.13, North-Holland, Amsterdam*, 209-232, 1976.
9. H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods. SIAM*, Philadelphia, Pa., 1992.
10. H. Niederreiter, I. Shparlinski. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. *Acta Arith*, 90(1), 89-98, 2000.
11. H. Niederreiter, I. Shparlinski. On the Distribution of Inversive Congruential Pseudorandom Numbers in Parts of the Period. *Math. of Comput.*, 70, 1569-1574, 2000.
12. H. Niederreiter and I. Shparlinski. Recent advances in the theory of nonlinear pseudorandom number generators. *Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods, 2000, Springer-Verlag, Berlin*, 86-102, 2002.
13. P. Varbanets, S. Varbanets. Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus. *VoronoÏ's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine, September 22-28*, 112-130, 2008.
14. S. Varbanets. Generalizations of Inversive Congruential Generator. *Analytic and Probabilistic Methods in Number Theory, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania, 4-10 Septembre 2011*, 265-282, 2012.