INVERSIVE GENERATOR OF THE SECOND ORDER
WITH A VARIABLE SHIFT
FOR THE SEQUENCE OF PRN’S

Pavel Varbanets and Sergey Varbanets
(Odessa, Ukraine)

Dedicated to the memory of Professor Antal Iványi

Communicated by Imre Kátai
(Received February 5, 2017; accepted March 30, 2017)

Abstract. The inversive congruential generator of second order modulo a prime power is investigated. This generator generalizes the inversive congruential generator of the first order studied in the works of Eichenauer, Lehn, Topuzoglu, Niederreiter, Shparlinski etc. Also we prove that the produced sequences of pseudo random numbers pass the \( s \)-dimensional test on the uniform distribution for \( s = 1, 2, 3 \).

1. Introduction

Uniform pseudorandom numbers (abbreviate., PRN’s) in the interval \([0, 1]\) are basic ingredients of any stochastic simulation. Their 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

Key words and phrases: Inversive congruential generator, sequences of pseudorandom numbers, exponential sum, discrepancy.

2010 Mathematics Subject Classification: 11K45, 11T23, 11T71.
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], [4], [10], [11], [14]. These generators have several attractive properties such as uniformity, unpredictability (statistical independence), pretty large period and simple calculative complexity. The most common types of the inversive generators are defined by the following congruential recursions.

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

$$\mathcal{F} = \begin{cases} 0, & \text{if } y = 0, \\ \text{multiplicative inverse to } y \text{ in } F_q^* & \text{if } y \neq 0. \end{cases}$$

Then the recursion

$$(1) \quad y_{n+1} = ay_n + b, \quad n = 0, 1, 2, \ldots.$$ 

produces the inversive congruential generator over $F_q$.

The generator (1) was introduced in [2]. In the works [7], [10] the equation (1) was replaced with the congruence $y_{n+1} \equiv ay_n^{-1} \pmod{p^m}$, $m \geq 2$, where $y_n^{-1}$ defines by the congruence $y_n y_n^{-1} \equiv 1 \pmod{p^m}$ if $(y_n, p) = 1$.

Other inversive generators consider over the ring $\mathbb{Z}_{p^m}$.

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

$$(2) \quad y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m}, (a, b \in \mathbb{Z}), \quad n = 0, 1, 2, \ldots.$$ 

where $y_n^{-1}$ is a multiplicative inverse modulo $p^m$ for $y_n$ if $(y_n, p) = 1$. The parameters $a$, $b$, $y_0$ are called the multiplier, shift and initial value, respectively.

In the works of Eichenauer, Lehn, Topuzoglu [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]). 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).
The sequences of PRN’s produced by inversive generators with constant shift can not be used for the cryptographic applications since \( a \) and \( b \) can be calculated from only three consecutive elements provided that \( p^m \) is known.

The generator (2) is called the inversive generator with constant shift. In [15] we have given two generalizations for the generator (2). The first generalization is associated with the recurrence relation

\[
y_{n+1} \equiv ay_n^{-1} + b + cF(n+1)y_0 \pmod{p^m}
\]

under conditions

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

The generator (3) is called 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 hard 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, since the reconstruction of polynomial by its values in the \( k \)-points is impossible if its degree is larger than \( k \)). Thus the generator (3) can be used in the cryptographical applications. Notice that the conditions \( (a, p) = (y_0, p) = 1, \quad b \equiv c \equiv 0 \pmod{p} \) guarantee that the recursion (3) produces the infinite sequence \( \{y_n\} \).

The second congruential recursion has the form

\[
y_{n+1} \equiv ay_n^{-1} + cy_n \pmod{p^m}
\]

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

The generator (4) is the linear-inversive congruential generator.

We must notice that the conditions \( a \equiv b \equiv 0 \pmod{p}, \quad (y_0, p) = (c, p) = 1 \) also make possible to generate the sequence of PRN’s with appropriate properties for PRN’s \( \{x_n\} \). However, the conditions \( a \equiv c \equiv 0 \pmod{p}, \quad (y_0, p) > (b, p) = 1 \) do not 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 \( a + c = 1 \) (mod 4) and \( b \equiv 3 \) (mod 4).

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

\[
y_{n+1} \equiv ay_{n-1}^{-1}y_0^{-1} + b + cF(n)y_1 \pmod{p^m},
\]

where \( (a, p) = 1, \quad b \equiv c \equiv 0 \pmod{p}, \quad (y_0, p) = (y_1, p) = 1, \quad F(n) \) is an integral valued function.
Notice that our 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 \(m \in \mathbb{N}\) the notation \(\mathbb{Z}_{p^m}\) (respectively, \(\mathbb{Z}_{p^m}^*\)) denotes the complete (respectively, reduced) system of residues modulo \(p^m\). For \(z \in \mathbb{Z}, (z, p) = 1\) let \(z^{-1}\) be the multiplicative inverse of \(z\) modulo \(p^m\); we let \(a \cdot b^{-1}\) (mod \(p^m\)) stand for \(a \cdot b^{-1}\). We write \(\nu_p(A) = \alpha\) if \(p^\alpha | A\) and \(p^{\alpha+1} \not| A\) for \(A \in \mathbb{Z}\). For integer \(t\), the abbreviation \(e_{2\pi i}(t) = e^{2\pi it}\) is used.

We need the following simple statements. Let \(f(x)\) be a periodic function with a period \(\tau\). For any \(N \in \mathbb{N}, 1 \leq N \leq \tau\), we denote

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

Lemma 1. The following estimate

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

holds.

This statement can be derived by inequalities for complete exponential sums on a usual way.

Lemma 2. Let \(h_1, h_2, k, \ell\) 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 \(j = 2, 3, \ldots\) we have

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

Moreover, for every polynomial \(G(u) = A_1u + A_2u^2 + p^l G_1(u) \in \mathbb{Z}[u]\) we have

\[
h_1 G(k) + h_2 G(\ell) = A_1(h_1k + h_2\ell) + A_2(h_1k^2 + h_2\ell^2) + p^{l+s} G_2(k, \ell),
\]

where \(s \geq \min(\nu_p(h_1 + h_2), \nu_p(h_1k + h_2\ell)), h_1, h_2, k, \ell \in \mathbb{Z}, G_2(u, v) \in \mathbb{Z}[u, v]\).
Proof. By the equality

\[ h_1 k^j + h_2 \ell^j = (h_1 k^{j-1} + h_2 \ell^{j-1})(k + \ell) - k\ell(h_1 k^{j-2} + h_2 \ell^{j-2}) \],

applying the method of mathematical induction, we obtain at once \( \nu_p(h_1 k^j + h_2 \ell^j) \geq \delta, \ j = 2, 3, \ldots \). ■

Lemma 3. Let \( p > 2 \) be a prime number, \( m \geq 2 \) be a positive integer, \( m_0 = \left\lceil \frac{m}{2} \right\rceil \), \( f(x), g(x), h(x) \) be polynomials over \( \mathbb{Z} \):

\[ f(x) = A_1 x + A_2 x^2 + \cdots, \]
\[ g(x) = B_1 x + B_2 x^2 + \cdots, \]
\[ h(x) = C_\ell x + C_{\ell+1} x^{\ell+1} + \cdots, \ \ell \geq 1, \]
\[ \nu_p(A_j) = \lambda_j, \ \nu_p(B_j) = \mu_j, \ \nu_p(C_j) = \nu_j, \]

and, moreover,

\[ k = \lambda_2 < \lambda_3 \leq \cdots, \ \ 0 = \mu_1 < \mu_2 < \mu_3 \leq \cdots, \]
\[ \nu_p(C_\ell) = 0, \ \nu_p(C_j) > 0, \ j \geq \ell + 1. \]

Then the following bounds occur

\[ \left| \sum_{x \in \mathbb{Z}_{p^m}} e_m(f(x)) \right| \leq \begin{cases} 2p^{m+k} & \text{if } \nu_p(A_1) \geq k, \\ 0 & \text{if } \nu_p(A_1) < k; \end{cases} \]
\[ \left| \sum_{x \in \mathbb{Z}_{p^m}} e_m(f(x) + g(x^{-1})) \right| \leq I(p^{m-m_0})p^{\frac{m}{2}} \]
\[ \left| \sum_{x \in \mathbb{Z}_{p^m}} e_m(h(x)) \right| \leq \begin{cases} 1 & \text{if } \ell = 1, \\ 0 & \text{if } \ell > 1, \end{cases} \]

where \( I(p^{m-m_0}) \) is a number of solutions of the congruence

\[ y \cdot f'(y) \equiv g'(y^{-1}) \cdot y^{-1} \pmod{p^{m-m_0}}, \ y \in \mathbb{Z}_{p^m}^\ast. \]

Proof. Consider the sum \( \sum_1 := \sum_{x \in \mathbb{Z}_{p^m}} e \left( \frac{f(x)}{p^m} \right) \). At first, let \( \nu_p(A_1) = k_1 < k \). Then

\[ \sum_1 = p^{k_1} \sum_{x \in \mathbb{Z}_{p^m-k_1}} e \left( \frac{A_1' x + A_2' x^2 + \cdots}{p^{m-k_1}} \right), \]

where \( A_j' = p^{-k_1} A_j, \ (A_1', p) = 1, \ A_j' \equiv 0 \pmod{p}, \ j = 2, 3, \ldots. \)
Putting \( x = y + p^{m-k_1-1}z \), \( y \in \mathbb{Z}_{p^{m-k_1-1}}, \ z \in \mathbb{Z}_p \), we derive

\[
\left| \sum_1 \right| = p^{k_1} \left| \sum_{y \in \mathbb{Z}_{p^{m-k_1}}} e\left( \frac{A_1' y + A_2' y^2 + \cdots}{p^{m-k_1-1}} \right) \sum_{z \in \mathbb{Z}_p} e\left( \frac{A_1' z}{p} \right) \right| = 0.
\]

For \( k_1 \geq k \) is suffices to consider the case \( k = 0 \). Then, putting

\[ x = y + p^{m-m_0}z, \ y \in \mathbb{Z}_{p^{m-m_0}}, \ z \in \mathbb{Z}_{p^m}, \]

we come to the sum which is analogous to the Gauss sum, and hence,

\[
\left| \sum_1 \right| = p^m.
\]

Next, for \( m = 1 \) we have from the Segal’s estimate (see, [13])

\[
\left| \sum_3 \right| = \left| \sum_{x \in \mathbb{Z}_p^*} e\left( \frac{C_2 x^t}{p} \right) \right| = 1 + \sum_{x \in \mathbb{Z}_p} e\left( \frac{C_2 x^t}{p} \right) \leq 1 + (\ell, p-1) p^{\frac{1}{2}}.
\]

If \( m > 1 \) we put \( x = y(1 + p^{m-m_0}z), \ y \in \mathbb{Z}_{p^{m-m_0}}, \ z \in \mathbb{Z}_{p^m} \). Then

\[
\left| \sum_3 \right| = \left| \sum_{y \in \mathbb{Z}_{p^{m-m_0}}} e\left( \frac{h(y)}{p^m} \right) \cdot \sum_{z \in \mathbb{Z}_{p^{m_0}}} e\left( \frac{yh'(y)}{p^{m_0}} z \right) \right|
\]

\[
= p^{m_0} \left| \sum_{y \in \mathbb{Z}_{p^{m-m_0}} \atop yh'(y) \equiv 0 \pmod{p^{m_0}}} e\left( \frac{h(y)}{p^m} \right) \right|.
\]

The congruence \( yh'(y) \equiv 0 \pmod{p^{m_0}} \) over \( \mathbb{Z}_{p^{m-m_0}} \) has not solutions. Hence for \( m > 1 \) we have \( \sum_3 = 0 \).

At last, we consider the sum \( \sum_2 \).

Same as previous we can write \( x = y(1 + p^{m-m_0}z) \).

And hence modulo \( p^m \) we have

\[ x^k = y^k + kp^{m-m_0}(y^{-1})^k z, \ k \in \mathbb{Z}, \]

\[
f(x) + g(x^{-1}) = f(y) + g(y) + p^{m-m_0}(yf'(y) - y^{-1}g'(y^{-1})).
\]

So, we obtain for \( m = 2m_0 \)

\[
\left| \sum_2 \right| = p^{m_0} \left| \sum_{y \in \mathbb{Z}_{p^{m-m_0}}} e\left( \frac{f(y) + g(y^{-1})}{p^m} \right) \right| \leq
\]

\[
\leq p^{m_0} I(p^{m_0}) = p^{\frac{m_0}{2}} I(p^{m-m_0}).
\]
Inversive generator for the sequence of PRN’s

For \( m = 2m_0 + 1 \), we put in the last sum \( y = u + py_j \), where \( y_j \) runs \( I(p^{m_0}) \) of solutions of the congruence

\[
yf'(y) \equiv y^{-1}g'(y^{-1}) \pmod{p^{m_0}}.
\]

So,

\[
\left| \sum_{y_j} \right| = p^{m_0} \left| \sum_{u_j \in \mathbb{Z}_p^*} e \left( \frac{A_1 u + B_1 u^{-1}}{p} \right) \right| \leq 2I(p^{m-m_0})p^{m_0} + \frac{1}{2} = 2p^{\frac{m}{2}}I(p^{m-m_0}).
\]

Departures from uniformity or independence can be detected by theoretical tests that use the numerical quantity \( D_s^N \), \( s = 1, 2, \ldots \), it is called the discrepancy of the points \( X_0, X_1, \ldots, X_{N-1}, X_j \in [0,1)^s \), \( j = 0, 1, \ldots, N-1 \) and which is defined by

\[
D(t_0, t_1, \ldots, t_{N-1}) = \sup_I \left| \frac{A_N(I)}{N} - |I| \right|
\]

where the supremum is extended over all subintervals \( I \) of \([0,1]^d\), \( A_N(I) \) is the number of points among \( t_0, t_1, \ldots, t_{N-1} \) falling into \( I \), and \( |I| \) denotes the d-dimensional volume \( I \).

The \( s \)-dimensional points \( X_n^{(s)} \) produced from our sequence \( x_0, x_1, \ldots, x_{N-1} \) of PRN’s in \([0,1)\) in the following manner

\[
X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1}), n = 0, 1, \ldots, N - s.
\]

We say that the sequence of points \( x_0, x_1, \ldots, x_{N-1} \) passes \( s \)-dimensional serial test on uniformity and independence (unpredictability) if \( D^{(1)}_N, D^{(2)}_N, \ldots, D^{(s)}_N \) tends to zero as \( N \to \infty \).

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

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

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

and

\[
r(h, q) = \prod_{j=1}^{d} r(h_j, q) \text{ for } h = (h_1, \ldots, h_d) \in C_d(q).
\]
Lemma 4 (Niederreiter, [9]). Let $N \geq 1$ and $q \geq 2$ be integers. For $N$ arbitrary points $t_0, t_1, \ldots, t_{N-1} \in [0,1]^d$, the discrepancy $D_N(t_0, t_1, \ldots, t_{N-1})$ satisfies

$$D_N(t_0, t_1, \ldots, t_{N-1}) \leq \frac{d}{q} + \frac{1}{N} \sum_{b \in C_{\mu}(q)} \frac{1}{\tau(h,q)} \left| \sum_{n=0}^{N-1} e(\tau b \cdot t) \right|. $$

Corollary 1. Let $\{\eta_k\}$, $\eta_k \in \{0,1,\ldots,q-1\}^d$, be a purely periodic sequence with a period $\tau$. Then for the discrepancy of the sequence of points $t_k = \frac{\eta_k}{q} \in [0,1]^d$, $k = 0, 1, \ldots, N-1$; $N \leq \tau$, the following estimate

$$D_N(t_0, t_1, \ldots, t_{N-1}) \leq \frac{d}{q} + \frac{1}{N} \sum_{b \in C_{\mu}(q)} \sum_{h_0 \in \{0,1\}^d} r^{-1}(h,q)r^{-1}(h_0,\tau) \cdot |\mathcal{S}| \cdot \log \tau $$

holds, where $\mathcal{S} := \sum_{k=0}^{\tau-1} e(\tau b_k + \frac{k\tau}{q})$.

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

3. Preparations

We will obtain the representation of $y_n$ in the form of rational function on $y_0, y_1$.

Let $\nu_p(b) = \nu_0$, $\nu_p(c) = \mu_0$, $1 \leq 2\nu_0 < \mu_0 \leq m$. A straightforward computation by recursion [5] shows that modulo $p^{3\nu_0}$ we have

$$y_6 = \frac{2a^2b + a^2y_0 + a^2cF(2) + F(5)y_1 + 2ab^2y_0y_1}{a^2 + ab^2y_0 + aby_0y_1 + acF(1)y_1 + acF(4)y_0y_1}, $$

$$y_7 = \frac{3a^2b^2 + 2a^2by_0 + a^2(1 + cF(3) + cF(6))y_0y_1}{2a^2b + a^2y_0 + a^2cF(2) + F(5)y_1 + 2ab^2y_0y_1}, $$

$$y_8 = \frac{a^3 + 3a^2b^2y_0 + a^2cF(1)y_1 + a^2by_0y_1 + a^2cF(4) + F(7)y_0y_1^2}{3a^2b^2 + 2a^2by_0 + a^2(1 + cF(3) + cF(6))y_0y_1}. $$

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

$$(6) \quad y_n = \frac{A^{(n)}_0 + A^{(n)}_1 y_0 + A^{(n)}_2 y_1 + A^{(n)}_3 y_0y_1}{B^{(n)}_0 + B^{(n)}_1 y_0 + B^{(n)}_2 y_1 + B^{(n)}_3 y_0y_1}. $$
Inversive generator for the sequence of PRN’s

From the above, for \( y_n \) we involve

\[
y_{n+2} = \frac{C}{D},
\]

where

\[
C = (aB_0^{(n)} + bA_0^{(n+1)}) + (aB_1^{(n)} + bA_1^{(n+1)})y_0 +
+ (aB_2^{(n+1)} + bA_2^{(n+1)} + cF(n + 1)A_0^{(n+1)})y_1 +
+ (aB_3^{(n)} + bA_3^{(n+1)} + cF(n + 1)A_1^{(n+1)})y_0y_1,
\]

\[
D = A_0^{(n+1)} + A_1^{(n+1)}y_0 + A_2^{(n+1)}y_1 + A_3^{(n+1)}y_0y_1.
\]

Without restricting the generality we will suppose that \( cF(n) \equiv cn + +p^\mu F_0(n) \pmod{p^m} \), where \( \mu = \min(\nu_0 + \mu_0, 3\nu_0) \).

Now, a straightforward computation suggest that modulo \( p^{3\nu_0} \) we have for \( k \geq 3 \)

\[
\begin{cases}
A_0^{(3k)} \equiv ka^k b, & A_1^{(3k)} \equiv a^k; \quad A_2^{(3k)} \equiv \frac{k(3k + 1)}{2}a^k c; \\
A_3^{(3k)} \equiv \frac{k^2 - k + 2}{2}a^{k-1}b^2; \\
B_0^{(3k)} \equiv a^k, & B_1^{(3k)} \equiv \frac{k(k + 1)}{2}a^{k-1}b^2, & B_2^{(3k)} = 0; \\
B_3^{(3k)} = (k - 1)a^{k-1}b;
\end{cases}
\]

\[
\begin{cases}
A_0^{(3k+1)} = \frac{k(k + 1)}{2}a^k b^2, & A_1^{(3k+1)} = ka^k b; \\
A_2^{(3k+1)} = 0, & A_3^{(3k+1)} = a^k \left( 1 + \frac{3k(k - 1)}{2}c \right); \\
B_0^{(3k+1)} = ka^k b, & B_1^{(3k+1)} = a^k, \quad B_2^{(3k+1)} = \frac{k(3k + 1)}{2}a^k c; \\
B_3^{(3k+1)} = \frac{k^2 - k + 2}{2}a^{k-1}b^2;
\end{cases}
\]

\[
\begin{cases}
A_0^{(3k+2)} \equiv a^{k+1}, & A_1^{(3k+2)} \equiv \frac{k(k + 1)}{2}a^k b^2, \\
A_2^{(3k+2)} \equiv 0, & A_3^{(3k+2)} = ka^k b, \quad A_4^{(3k+2)} = \frac{(k + 1)(3k + 2)}{2}a^k c; \\
B_0^{(3k+2)} = \frac{k(k + 1)}{2}a^k b^2, & B_1^{(3k+2)} = ka^k b; \\
B_2^{(3k+2)} = 0, & B_3^{(3k+2)} = a^k \left( 1 + \frac{3k(k + 1)}{2} \right), \quad B_4^{(3k+2)} \equiv 0.
\end{cases}
\]
The validity of the formulas (10), (8) is not difficult establishes by the method of mathematical induction. The formula (9) follows by recursion (5). Other summands of $A_j^{(n)}$, $j = 0, 1, 2$; $n = \{3k \text{ or } 3k + 1 \text{ or } 3k + 2\}$, which modulo $p^3y_0$ are equal to 0, be represented the polynomials from $\mathbb{Z}[n]$ (it comes from formula (7)). So, we may write

$$A_0^{(3k)} = ka^k b + p^3y_0 F_0(k), \ldots, B_3^{(3k)} = (k - 1)a^{k-1} b + p^3y_0 G_3(k).$$

A stabilization of form of the coefficients of the polynomials $F_0(k), \ldots, G_3(k)$ in the formulas described above occurs for $k \geq 4m$, because beginning with $k^\ell$, $\ell \geq m$ for corresponding coefficients is equal to zero modulo $p^m$.

The number of summands in any $F_j(k)$ or $G_j(k)$, $j = 0, 1, 2$ be less than $4m_0$, where $m_0 = \left\lceil \frac{m+1}{\nu_0} \right\rceil$ 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 $a^k$, $k - m_0 \leq \ell \leq k$.

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 mod $p^m$ to the respective summand of denominator and applying the expanding $(1 + pu)^{-1} = 1 - pu + p^2a^2 - \cdots + (-1)^{m-1}(pu)^{m-1} \pmod{p^m}$, we obtain the representation of $y_k$ power expansion of $k$ with coefficients which depend only on $y_0$, $y_1$ and $(a^{-1})^j$, $0 \leq j \leq m$, where $a \cdot a^{-1} \equiv 1 \pmod{p^m}$.

So, after simple calculations we deduce modulo $p^m$

$$y_{3k} = \left(k b + y_0 + \frac{k^2 - k + 2}{2} a^{-1} b^2 y_0 y_1 \right) \left(1 - \frac{k(k + 1)}{2} a^{-1} b^2 y_0 - \right)$$

$$- (k - 1)a^{-1} by_0 y_1 + (k - 1) b^2 y_0^2 y_1^2).$$

From here we have

$$y_{3k} = (y_0 + a^{-1} b y_0^2 y_1 + b^2 y_0 y_1^2 + a^{-1} b^2 y_0 y_1) +$$

$$k \left(b + a^{-1} b^2 y_0 y_1 - \frac{1}{2} a^{-1} b^2 y_0^2 - \right)$$

$$-a^{-1} b y_0^2 y_1 - 2b^2 y_0 y_1^2 - \frac{1}{2} a^{-1} b^2 y_0 y_1) +$$

$$+ k^2 \left(-a^{-1} b^2 y_0 y_1 - \frac{1}{2} a^{-1} b^2 y_0^2 + b^2 y_0 y_1^2 + \frac{1}{2} a^{-1} b^2 y_0 y_1 \right).$$

(11)
Next, by analogy, we infer

\[ y_{3k+1} = (y_1 - a^{-1}b^2y_1^2) + kb \left( \frac{1}{2} (y_0^{-1} - a^{-1}y_1^2) + 1 - y_0^{-1}y_1 \right) + k^2b^2 \frac{1}{2} (-y_0^{-1} + a^{-1}b^2y_1^2), \]

(12)

\[ y_{3k+2} = ay_0^{-1}y_1^{-1} + kb \left( (-ay_0^{-2}y_1^{-1} + 1) - \frac{1}{2}by_1^{-1} (ay_0^{-2}y_1^{-1} - 1) \right) + k^2b^2 \frac{1}{2} y_0^{-1} (-1 + a^{-1}y_0y_1^2). \]

(13)

So, from \[11\]-\[13\], collecting the summands with the same degree of \( k \), we infer the following statement.

**Proposition 1.** Let the sequence \{\( y_n \)\} be produced by the recursion \[5\] with \((a, p) = (y_0, p) = (y_1, p) = 1, \nu_p(b) = \nu_0 > 0, \nu_p(c) = \mu_0 > 2\nu_0\). There exist the polynomials \( F_0(x), F_1(x), F_2(x) \in \mathbb{Z}[x] \) with the coefficient depending on \( y_0, y_1 \), such that

\[ y_{3k} = A_0 + A_1k + A_2k^2 + p^\mu G_0(k, y_0, y_0^{-1}, y_1, y_1^{-1}), \]

(14)

\[ y_{3k+1} = B_0 + B_1k + B_2k^2 + p^\mu G_1(k, y_0, y_0^{-1}, y_1, y_1^{-1}), \]

(15)

\[ y_{3k+2} = C_0 + C_1k + C_2k^2 + C_3k^3 + C_4k^4 + p^\mu G_2(k, y_0, y_0^{-1}, y_1, y_1^{-1}), \]

(16)

where

\[ A_1 = b + a^{-1}b^2y_0y_1 - \frac{1}{2} a^{-1}b^2y_0^2 - a^{-1}by_0y_1 - 2b^2y_0y_1^2 - \frac{1}{2} a^{-1}b^2y_0y_1, \]

\[ A_2 = -a^{-1}b^2y_0y_1 - \frac{1}{2} a^{-1}b^2y_0^2 + b^2y_0y_1 + \frac{1}{2} a^{-1}b^2y_0y_1, \]

\[ B_1 = b \left( \frac{1}{2} b (y_0^{-1} - a^{-1}y_1^2) + 1 - y_0^{-1}y_1 \right), \]

\[ B_2 = b^2 \frac{1}{2} (-y_0^{-1} + a^{-1}b^2y_1^2), \]

\[ C_1 = b \left( (-ay_0^{-2}y_1^{-1} + 1) - \frac{1}{2}by_1^{-1} (ay_0^{-2}y_1^{-1} - 1) \right), \]

\[ C_2 = b^2 \frac{1}{2} y_0^{-1} (-1 + a^{-1}y_0y_1^2), \]

\[ \mu = \min (\nu_0 + \mu_0, 3\nu_0). \]
In process of proof the Proposition 1 we obtain also the following corollaries.

**Corollary 2.** Let \( \nu_p(y_0 - ay_1^{-2}) = \alpha \leq \nu_0 \) and let \( \tau \) be a period length of the sequence \( \{y_n\} \) generated by recursion (5) with initial values \( y_0, y_1 \). Then we have

\[
\tau = 3p^{\nu_0 - \alpha},
\]

and \( \tau \leq 3p^{\nu_0 - \alpha} \) on all occasions.

**Corollary 3.** For \( k = 3, 4, \ldots \), we have modulo \( p^\mu \), \( \mu = \min(2\nu_0, \mu_0) \)

\[
y_{3k} = \left(1 + a^{-1}b^2y_1 + ka^{-1}b^2y_1 - a^{-1}k^2b^2y_1 - \frac{1}{2}a^{-1}b^2y_1\right)y_0 + \\
+ \left(a^{-1}by_1 - \frac{1}{2}a^{-1}b^2 - a^{-1}bky_1 - \frac{1}{2}a^{-1}b^2k^2\right)y_0 + \\
+ (a^{-2}b^2y_1^2 - 2a^{-1}bky_1^2 + a^{-2}b^2k^2y_1^2)y_0 + kb,
\]

\[
y_{3k+1} = \left(\frac{1}{2}b^2k^2y_0^{-2} - \frac{1}{2}b^2k^2y_0^{-1} - \frac{1}{2}k^2b^2a^{-1}\right)y_1 + \\
+ \left(-a^{-1}b^2 - \frac{1}{2}a^{-1}b^2k^{-1}y_0^{-1}\right)y_1,
\]

\[
y_{3k+2} = kb + (a^{-1}y_0^{-1} + \frac{1}{2}kb - b^2k)^y_1^{-1} + \\
+ \left(-abky_0^{-1} + \frac{1}{2}b^2k^{-1}y_0^{-1}\right)y_1^{-2} + \frac{1}{2}a^2b^2k^2y_0^{-1}y_1^{-3}.
\]

4. **Bound of discrepancy of the sequences generated by recursion (5)**

In this section we prove the theorems 1-3 on the estimates of exponential sums over the sequence of pseudorandom numbers \( \{y_n\} \) generated by recursion (5), and obtain the bound of discrepancy.

Note, that the shift \( b + cF(n) \) in (5) is given by

\[
b_0p^{\nu_0} + c_0p^{\nu_0}(n + p^{\mu_1}F_0(n))
\]

where \((b_0, p) = (c_0, p) = 1, \mu_1 > 0\).

As we can see below, the summand \( c_0p^{\nu_0}F(n) \) has no influences on the character of equidistribution of the sequence \( \{\frac{y_n}{p^{\nu_0}}\} \) at the interval \([0, 1)\). Its
Inversive generator for the sequence of PRN’s

use is only if to avoid for intruder the reconstruction of the polynomial $F(n)$ by the certain values of $y_n$, $n = n_0, n_0 + 1, \ldots, n_0 + r$ (it is true if $F(n)$ is a polynomial with large power).

Denote

$$\sigma_{k, \ell}(h_1, h_2; p^m) := \sum_{y_0, y_1 \in \mathbb{Z}_{p^m}^*} e\left(\frac{h_1 y_k + h_2 y_\ell}{p^m}\right), \ (h_1, h_2 \in \mathbb{Z}).$$

Here we consider $y_k, y_\ell$ as functions of initial values $y_0, y_1$ generated by (5).

From Proposition 1 and Lemmas 2 and 3 we can see that the summation over $y_0, y_1$ gives the following theorem

**Theorem 1.** Let $\nu_p(\gcd(h_1, h_2, p^m)) = s$, $\nu_p(\gcd(h_1 + h_2, h_1 k + h_2 \ell, p^m)) = t$. Then we have

$$\sigma_{k, \ell}(h_1, h_2) \ll \begin{cases} p^{m+s} & \text{if } k \equiv \ell \pmod{3}, \\ p^{m+t} & \text{if } k \not\equiv \ell \pmod{3}. \end{cases}$$

In order to prove this theorem it is enough to put $y_0 = x_0(1 + p^{m_0 + \varepsilon}z_0)$, $y_1 = x_1(1 + p^{m_0 + \varepsilon}z_1)$, $x_0, y_0 \in \mathbb{Z}_{p^m_0}^*$, $z_0, z_1 \in \mathbb{Z}_{p^m_0}$ and apply Lemmas 2 and 3.

For $1 \leq N \leq \tau := 3p^{m-\nu_0}$ denote

$$S_N(h, y_0, y_1) = \sum_{k=0}^{N-1} e_{p^m}(hy_k).$$

**Theorem 2.** Let the sequence $\{y_n\}$ is generated by recursion (5), $(h, p^m) = p^s$ and the condition $y_0 y_1^2 \not\equiv a \pmod{p}$ is fulfilled. Then the following bound

$$|S_\tau(h, y_0, y_1)| \leq \begin{cases} O(m) & \text{if } \nu_0 + s < m, \\ \tau & \text{if } \nu_0 + s \geq m \end{cases}$$

holds.

**Proof.** This statement is the corollary of Proposition 1 if we take into account that the summand $O(m)$ in (17) appears in virtue of the fact that the representation $y_n$ as a polynomial on $k$ from Proposition 1 holds only for $k \geq 2m_0 + 1$.

Further we will study only special case of initial values $y_0 = y_1$.

**Corollary 4.** For $1 \leq N \leq \tau$ we have

$$S_N(h; y_0, y_0) := S_N(h, y_0) \ll \begin{cases} p^{m_0 + \varepsilon} \frac{N}{2} & \text{if } \nu_0 + s < m, \\ N & \text{if } \nu_0 + s \geq m. \end{cases}$$
Indeed, from Lemma 1 we have

\[
|S_N(h, y_0)| \leq \max_{1 \leq n \leq \tau} \left| \sum_{k=1}^\tau e^{2\pi i \left( \frac{hy_k + nk}{p^m} \right)} \right|
\]

\[
= \max_{1 \leq n \leq \tau} \left| \sum_{k=1}^{p^m-\nu_0} \sum_{j \in \{0,\pm 1\}} e^{2\pi i \left( \frac{hy_k + j}{p^m} + \frac{n(3k+j)}{p^\nu_0} \right)} \right| \leq
\]

\[
\leq p^{\nu_0} \left( \sum_1 + \sum_2 + \sum_3 \right) + O(m),
\]

where

\[
\sum_1 = \max_{1 \leq n \leq \tau} \left| \sum_{k=1}^{p^m-\nu_0} e^{2\pi i \left( \frac{hF_0(k) + nk + \nu p^{-\nu_0} H_0(k)}{p^m} \right)} \right|
\]

\[
\sum_2 = \max_{1 \leq n \leq \tau} \left| \sum_{k=1}^{p^m-\nu_0} e^{2\pi i \left( \frac{hF_1(k) + nk + \nu p^{-\nu_0} H_1(k)}{p^m} \right)} \right|
\]

\[
\sum_3 = \max_{1 \leq n \leq \tau} \left| \sum_{k=1}^{p^m-\nu_0} e^{2\pi i \left( \frac{hF_2(k) + nk + \nu p^{-\nu_0} H_2(k)}{p^m} \right)} \right|
\]

for \( F_j(k), H_j(k), j = 0, 1, 2 \) defined by the relations \( (14) - (15) \).

Now we take into consideration that for \( 1 - a^{-1}y_0^3 \not\equiv 0 \mod p \). Therefore the coefficients for \( k^2 \) in the polynomials \( F_j(k) \) exactly be divisible on \( p^{2\nu_0} \).

Hence, by Lemma 3 (the case (i)) we obtain

\[
\sum_j \ll \begin{cases} 
\frac{p^{m+\nu_0+3}}{N} & \text{if } \nu_0 + s < m, \\
p^{m} & \text{if } \nu_0 + s \geq m.
\end{cases}
\]

Let

\[
\bar{\sigma}_{k,\ell}(h) = \sum_{y_0 \in \mathbb{Z}_{p^m}} e^{2\pi i \left( \frac{h(y_k - y_0)}{p^m} \right)}.
\]

**Theorem 3.** Let the sequence \( \{y_n\} \) be generated by recursion \( (5) \) with \( (a, p) = (1, \nu_p(b) = \nu_0, \nu_p(c) = \mu_0, \mu_0 > 2\nu_0, F(n) \) is a polynomial with integer coefficients of the form \( F(u) \equiv u \pmod{p^{\nu_0+1}} \). Moreover, let \( y_0 = y_1, (y_0, p) = 1 \). Then, for \( k \equiv \ell \pmod{3} \) the following estimate

\[
\bar{\sigma}_{k,\ell}(h) \ll \begin{cases} 
p^{m+\nu_0+\nu_p(h)} & \text{if } \nu_0 + \nu_p(h) < m, \\
p^{m} / 2 & \text{if } \nu_0 + \nu_p(h) \geq m.
\end{cases}
\]

holds.
Inversive generator for the sequence of PRN's

Proof. We consider only the case \( k \equiv \ell \equiv 0 \pmod{3} \) because the other cases are similar.

We have

\[
h(y_3k - y_3\ell) = h(k - \ell) - a^{-1}bh(k - \ell)y_0^3 + h(1 - a^{-2})(k^2 - \ell^2)b^2y_0^5 + p^\mu hH_0(y_0),
\]

where \( \mu = (\mu_0, 3\nu_0) \), \( H(y_0) \) is the polynomial with the coefficients \( h_j \equiv 0 \pmod{p^t} \) by Lemma 2. Then for \( \nu_\mu(h) + \nu_\mu(k - \ell) + \nu_0 < m - 1 \) the statement of lemma follows from the relation

\[
\sum_{y \in \mathbb{Z}_{p^t}^*} e^{2\pi i \frac{Ax^3 + px^y + y^5}{p^t} f(u)} = \sum_{y \in \mathbb{Z}_{p^t}} e^{2\pi i \frac{Ax^3 + px^y + y^5}{p^t} f(u)} - \sum_{y \in \mathbb{Z}_{p^t-1}} e^{2\pi i \frac{Ax^3 + px^y + y^5}{p^t} f(u)} = \sum_1 + \sum_2, \quad (\ell \geq 1), \quad (A, p) = 1
\]

say.

Now, putting \( y = u + p^\alpha v \), where \( \alpha = \left\lfloor \frac{t-1}{2} \right\rfloor \) or \( \left\lfloor \frac{t-2}{2} \right\rfloor \) (respectively, for \( \sum_1 \) or \( \sum_2 \)) by Lemma 3 we obtain the statement of theorem.

\[\blacksquare\]

Remark 1. In case of \( k \not\equiv \ell \pmod{3} \) from Lemma 3 we easy obtain

\[
\tilde{\sigma}_{k,\ell}(h) \ll \begin{cases} 
0 & \text{if } s \leq m - 2, \\
 p^{2(m-1)} & \text{if } s = m - 1 \\
p^{2m} & \text{if } s = m.
\end{cases}
\]

In the case under consideration \( y_0 = y_1 \) we additionally will assume that \( a \) is not a cubic residue modulo \( p \) such that \( y_0^3 \not\equiv a \pmod{p} \) for every \( y_0 \), \( (y_0, p) = 1 \).

The following theorem gives a mean value of \( S_N(h, y_0) \).

Theorem 4. Let the sequence \( \{y_n\} \) be produced by \([5]\) with parameters \( a, b \), \( y_0, (a, p) = (y_0, p) = 1, \nu_\mu(b) = p^{\nu_0}, 1 \leq \nu_0 \leq \frac{m}{2} \). Then for every \( h \in \mathbb{Z}, (h, p^m) = \mu_1 \leq s \), we have

\[
\overline{S}_N(h) = \frac{1}{\varphi(p^m)} \sum_{y_0 \in \mathbb{Z}_{p^m}^*} |S_N(h, y_0)| \leq 36p^{\mu_1}N^\frac{1}{2} \sqrt{\log p^m}.
\]
Proof. Without loss of generality we will assume that \( \nu_p(h) = 0 \), i.e. \((h, p) = 1\). By the Cauchy-Schwarz inequality we get

\[
\|S_N(h)\|^2 \leq \frac{1}{\varphi(p^m)} \sum_{y_0 \in \mathbb{Z}_{p^m}} \left| \sum_{n=0}^{N-1} e_m(h y_n) \right|^2.
\]

\[
= \frac{1}{\varphi(p^m)} \sum_{y_0 \in \mathbb{Z}_{p^m}} \sum_{k,\ell=0}^{N-1} e_m(h(y_k - y_\ell)) \leq \leq \frac{1}{\varphi(p^m)} \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h, -h)| = \frac{1}{\varphi(p^m)} \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h, -h)| = \frac{1}{\varphi(p^m)} \sum_{t=0}^{m-1} \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h, -h)| + \frac{1}{\varphi(p^m)} \sum_{k=0}^{N-1} |\sigma_{k,k}(h, -h)| = N + \frac{1}{\varphi(p^m)} \sum_{t=0}^{m-1} \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h, -h)|.
\]

Using Theorem 3, we obtain

\[
|S_N(h)|^2 \leq N + \frac{1}{\varphi(p^m)} \times \left( \sum_{r=0}^{m-1} \left( \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h, -h)| \right) + \sum_{k,\ell=0}^{N-1} |\sigma_{k,k}(h, -h)| \right) \leq \leq \frac{1}{\varphi(p^m)} \times \left[ 4p^m \sum_{r=0}^{m-1} \frac{N^2}{p^r} + \left( \sum_{r<m-v_0} + \sum_{m-v_0 \leq r \leq m-1} \right) \sum_{k=0}^{N-1} |\sigma_{k,k}(h, -h)| \right] \leq \leq \frac{N}{\varphi(p^m)} \times \left( 4N + \sum_{r<m-v_0} \frac{N}{p^r} + \sum_{r \geq m-v_0} \frac{N}{p^r} \right) \log p^m \leq \leq N + \left( N^2 p^{-m} + 11N^2 p^{-\frac{3m}{2} + v_0} \right) \log p^m.
\]
Hence, for \((h, p) = 1\) we obtain

\[
|S_N(h)| \leq \left(12N^{1/2} + 12Np^{-\nu_0} + 12Np^{-\frac{3}{2}+\nu_0}\right)\sqrt{\log p^m} \leq 36N^{1/2}\sqrt{\log p^m}.
\]

\[\textbf{Theorem 5.}\] Let the sequence \(\{y_n\}\) be produced by recursion (5) with parameters \(a, b, y_0, \ (a, p) = \ (y_0, p) = 1, \ \nu_p(b) = p^\nu_0, \ 1 \leq \nu_0 \leq \frac{mp}{2}\). Then for all but at most \(p^{(1+o(1))m}\) values \(y_0 \in \mathbb{Z}_{p^m}\) we have

\[
S_N(h) = O\left(N^{\frac{1}{2}+o(1)}\right).
\]

From the Corollary 5 and Lemma 4 we easily infer

\[\textbf{Theorem 6.}\] Let \(D_N(x_0, \ldots, x_{N-1}) \leq N^{-\frac{1}{2}+\varepsilon(N)}(\log p^m)^2\).

(here \(x_n = \frac{y_n}{p^m}\), \(n = 0, 1, 2, \ldots, \varepsilon(N) \to +0\) for \(N \to \infty\)).

Let \(a\) be a cubic nonresidue modulo \(p\). Then the least length of period for \(\{y_n\}\) is equal to \(\tau = 3p^{m-\nu_0}\).

\[\textbf{Theorem 7.}\] Let \(p > 2\) be a prime number, \(y_0, a, b, m \in \mathbb{N}, \ m \geq 3, \ (a, y_0, p) = \ (a, p) = 1, \ \nu_p(b) = \nu_0 \geq 1, \ \nu_p(c) = \mu_0, \ \mu_0 > 2\nu_0\). Then for the sequence \(\{x_n\}\), \(x_n = \frac{y_n}{p^m}\), \(n = 0, 1, \ldots, \) with the period \(\tau = 3p^{m-\nu_0}\), generated by recursion (5) with \(cF(n) = cn + p^nF_0(n), \ F_0(n)\) is an integral-valued function, \(\mu = \min(\nu_0 + \mu_0, 3\nu_0)\), we have for any \(1 \leq N \leq \tau\),

\[
D_N(x_0, x_1, \ldots, x_{N-1}) \leq \frac{1}{p^m} + 3N^{-1}p^{m-\nu_0}\left(\frac{1}{p} \left(\frac{2}{\pi} \log p^m + \frac{7}{5}\right)^2 + 1\right). 
\]
The assertions of Theorems 5 and 6 are the simple conclusions of Theorems 3 and 4 and Lemma 4 (see [14]).

From Theorems 5 and 6 we conclude that the sequence of PRN’s \( \{y_n\} \) produced by generator (5) passes the \( s \)-dimensional serial test on the equidistribution and statistical independency.

**Remark 2.** We investigated the inversive congruential generator (5) under condition \( 0 < 2 \nu_p(b) < \nu_p(c) \). This restriction may be weaken with requirements \( 0 < \nu_p(b) < \nu_p(c) \) through the additional technical difficulties.

**Remark 3.** The description of \( y_n \) produced by recursion (5) allow to consider other cases of selection an initial value \( y_1 \) as function at \( y_0 \).

### References


Inversive generator for the sequence of PRN’s


**P. Varbanets and S. Varbanets**
Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
Odessa, 65026 Ukraine
varb@sana.od.ua
varb@sana.od.ua