Chaotic Modeling and Simulation (CMSIM) 1: 231–238, 2013

Inversive congruential generator with a variable shift

P. D. Varbanets[1] and S. P. Varbanets[2]

[1] I.I. Mechnikov Odessa National University, str. Dvoryanskaya 2, 65026 Odessa, Ukraine
(E-mail: varb@sana.od.ua)
[2] I.I. Mechnikov Odessa National University, str. Dvoryanskaya 2, 65026 Odessa, Ukraine
(E-mail: varb@sana.od.ua)

Abstract. We give the description for elements of the sequence of inversive congruential pseudorandom numbers y_n as polynomials on number n and initial value y_0. We also estimate some exponential sums over y_n.
Keywords: inversive congruential numbers, exponential sum, discrepancy.

1 Introduction

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

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

where $\overline{y}_n$ is a multiplicative inversive $mod\ p^m$ for y_n if $(y_n, p) = 1$. The parameters a, b, y_0 we call the multiplier, shift and initial value, respectively.

In the works of Eichenauer, Lehn, Topuzoğlu, Niederreiter, Flahive, Shparlinski, Grothe, Emmerih 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, [3],[4]). 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 the generalization for the generator (1). We consider the following recursive relation

$$y_{n+1} \equiv a\overline{y}_n + b + cF(n+1)y_0(mod\ p^m) \tag{2}$$

Received: 4 April 2012 / Accepted: 12 October 2012

ISSN 2241-0503

under conditions

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

The generator (2) we call the generator with a variable shift $b+cF(n+1)y_0$. The computational complexity of generator (2) is the same as for the generator (1), 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 $y_n, y_{n+1}, \dots, y_{n+N}$ will be revealed. Thus the generator (2) can be used in the cryptographical applications. Notice that the conditions $(a,p)=(y_0,p)=1$, $b\equiv c\equiv 0(mod\ p)$ guarantee that the recursion (2) produces the infinite sequence $\{y_n\}$.

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.

Notations: For p being a prime number

$$\begin{aligned}
&R_m := \{0,1,\dots,p^m-1\},\\
&R_m^* := \{a\in R_m \mid (a,p)=1\},\\
&e_m(u) := e^{2\pi i\frac{u}{p^m}}, u\in\mathbb{R},\\
&exp(x) := e^x \text{ for } x\in\mathbb{R},\\
&\nu_p(A)=\alpha\in\mathbb{N}\cup\{0\} \text{ if } p^\alpha \parallel A,\ p^{\alpha+1}\not| A.
\end{aligned}$$

For $u\in\mathbb{Z}$, $(u,p)=1$ we write $\overline{u}$ if $u\cdot\overline{u}\equiv 1(mod\ p^m)$.

2 Auxiliary results

We need the following simple statements.

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

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

Lemma 1. *The following estimate*

$$|S_N(f)|\le \max_{1\le n\le\tau}\left|\sum_{x=1}^{\tau} e^{2\pi i\left(f(x)+\frac{nx}{\tau}\right)}\right|\log\tau \tag{3}$$

holds.

Let $\mathfrak{I}(A,B;p)$ be a number of solutions of the congruence $A-Bu^2\equiv 0(mod\ p)$, $(u,p)=1$.

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

$$\begin{aligned}
f(x)&=A_1x+A_2x^2+p(A_3x^3+\cdots),\\
g(x)&=B_1x+p(B_2x^2+\cdots),
\end{aligned}$$

and, moreover, let $\nu_p(A_2)=\alpha>0$, $\nu_p(A_j)\geq\alpha$, $j=3,4,\ldots$. *Then we have the following estimates*

$$\left|\sum_{x\in R_m} e_m(f(x))\right|\leq\begin{cases}2p^{\frac{m+\alpha}{2}} & if\ \nu_p(A_1)\geq\alpha,\\ 0 & else;\end{cases} \tag{4}$$

$$\left|\sum_{x\in R_m^*} e_m(f(x)+g(\overline{x}))\right|\leq\begin{cases}(\mathfrak{I}(A_1,B_1;p)\cdot p)^{\frac{m}{2}} & if\ (B_1,p)=1,\\ 2p^{\frac{m+\alpha}{2}} & if\ \nu_p(A_1)\geq\alpha,\\ & \quad \nu_p(B_j)\geq\alpha,\\ & \quad j=1,2,\ldots,\\ 0 & if\ \nu_p(A_1)<\alpha\leq\nu_p(B_j),\\ & \quad j=1,2,3,\ldots.\end{cases} \tag{5}$$

3 Preparations

Consider the sequence $\{y_n\}$ produced by the recursion (2).
Let $n=2k$. We put

$$y_{2k}\equiv\frac{a_0^{(k)}+a_1^{(k)}y_0+\cdots}{b_0^{(k)}+b_1^{(k)}y_0+\cdots}:=\frac{A_k}{B_k}(mod\ p^m) \tag{6}$$

Twice using the recursion (2) we infer

$$\begin{aligned}y_{2(k+1)}=\frac{A_{k+1}}{B_{k+1}}&\equiv\frac{\left(aA^{(k)}+abB^{(k)}+b^2A^{(k)}\right)}{aB_k+bA_k+cA_kF(2k+1)y_0}+\\ &+\frac{\left(acB^{(k)}+bcA^{(k)}F(2k+2)+bcA^{(k)}F(2k+1)\right)y_0}{aB_k+bA_k+cA_kF(2k+1)y_0}\equiv\\ &\equiv\frac{(aA_k+abB_k+b^2A_k)}{aB_k+bA_k+cA_kF(2k+1)y_0}+\\ &+\frac{(acB_k+bcA_kF(2k+2)+bcA_kF(2k+1))\,y_0}{aB_k+bA_k+cA_kF(2k+1)y_0}+\\ &+\frac{c^2A_kF(2k+1)F(2k+2)y_0^2}{aB_k+bA_k+cA_kF(2k+1)y_0}\end{aligned} \tag{7}$$

Define the following matrices

$$\begin{aligned}&S_0=\begin{pmatrix}a+b^2 & ab\\ b & a\end{pmatrix},\ S_1=\begin{pmatrix}b & a\\ 0 & 0\end{pmatrix},\ S_2=\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix},\ S_3=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\\ &T_k=S_0+cy_0F(2k+2)S_1+bcy_0F(2k+1)S_2+\\ &\quad+c^2y_0^2F(2k+1)F(2k+2)S_3\end{aligned} \tag{8}$$

Now from (6)-(7) we obtain the matrix equality

$$\begin{pmatrix}A_{k+1}\\ B_{k+1}\end{pmatrix}=T_kT_{k-1}\cdots T_1\begin{pmatrix}A_0\\ B_0\end{pmatrix},\ \begin{pmatrix}A_0\\ B_0\end{pmatrix}=\begin{pmatrix}y_0\\ 1\end{pmatrix} \tag{9}$$

Denote

$$Y_i = cy_0F(2i+2)S_1 + cby_0F(2i+1)S_2 + c^2y_0^2F(2i+1)F(2i+2)S_3$$

Then we have

$$T_1T_2\cdots T_k = S_0^k + \sum_{\ell=1}^{k-1} S_0^{k-\ell} \sum_{j=0}^{k} {\sum_{i_1,\dots,i_\ell}}' Y_{i_1}\cdots Y_{i_\ell}, \tag{10}$$

where the sum ${\sum_{i_1,\dots,i_\ell}}'$ takes over all collections $i_1,\dots,i_\ell$ for which $0 \le i_1,\dots,i_\ell \le k$, $i_t \ne i_s$ for $t \ne s$, and $i_t \ne j$, $t = 1,\dots,\ell$, $s = 1,\dots,\ell$.

We will suppose that $\nu = \nu_p(b) < \nu_p(c) = \mu$. Therefore $Y_i \equiv 0 (mod\ p^\mu)$, and hence, all summands of sum ${\sum_{i_1,\dots,i_\ell}}'$ are equal to zero modulo p^m if $\ell > k_0 := \left[\frac{m+1}{\mu}\right]$.

First we study S_0^k in detail.

We have

$$S_0 = aI + bZ,$$

where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}.$$

Hence, putting $\ell_0 = \min\left(\left[\frac{k+1}{2\nu}\right], \left[\frac{m+1}{2\nu}\right]\right)$ we can write

$$S_0^k = \sum_{j=0}^{k} \binom{k}{j} a^{k-j}b^jZ^j = \sum_{\substack{j=0 \\ \text{j is even}}}^{\ell_0} + \sum_{\substack{j=0 \\ \text{j is odd}}}^{\ell_0} := \sum\nolimits_1 + \sum\nolimits_2, \tag{11}$$

where modulo p^m

$$\begin{aligned} \sum\nolimits_1 &= \sum_{j=0}^{\ell_0} \binom{k}{2j} a^{k-2j}b^{2j}Z^{2j}, \\ \sum\nolimits_2 &= \sum_{j=0}^{\ell_0} \binom{k}{2j+1} a^{k-2j-1}b^{2j+1}Z^{2j+1}. \end{aligned} \tag{12}$$

Notice that

$$Z^2 = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} a+b^2 & ab \\ b & a \end{pmatrix} = aI + bZ.$$

Consequently, raising to square in series the matrix Z we derive for $j \le \ell_0$

$$Z^{2j} = F_0(j)I + F_1(j)Z \tag{13}$$

where

$$\begin{cases} F_0(j) = f_{0,j} + b^2f_{2,j} + \cdots + b^{2j-2}f_{2j-2,j}, \\ F_1 = bf_{1,j} + b^3f_{3,j} + \cdots + b^{2j-1}f_{2j-1,j}, \\ f_{0,j} = a^j, \ \ f_{1,j} = a^{j-1}j. \end{cases} \tag{14}$$

Moreover, it is easy to see that

$$\begin{cases} f_{2,j} = a^{j-1}(2j-3),\ f_{3,j} = \overline{2}a^{j-1}(3j^2-9j+8), \\ f_{2j-4,j} = a^2(2j-3),\ f_{2j-2,j} = a, \\ f_{2j-3,j} = a(f_{2j-3,j-1}+2j-3),\ f_{2j-1,j} = 1, \\ f_{2\ell,j} = a^{j-\ell}(f_{2\ell,j-1}+f_{2\ell-1,j-1}), \\ f_{2\ell+1,j} = a^{j-\ell}(f_{2\ell,j-1}+f_{2\ell+1,j-1}+f_{2\ell-1,j-1}), \\ \ell = 2,3,\ldots,j-2. \end{cases} \tag{15}$$

So, for $k \geq m$ the coefficients $f_{\ell,j}$ does not depend on k.
From (13)-(14) we derive

$$\begin{aligned} Z^{2j+1} &= (ja^jb + f_{3,j}a^{j-1}b^3 + \cdots + ab^{2j-1})I + \\ &+ (a^j + a^{j-1}b^2(f_{2,j}+j) + \cdots + ab^{2j-2}(2j-1) + b^{2j})Z = \\ &= G_0(j)I + G_1(j)Z. \end{aligned} \tag{16}$$

Thereby the relations (13)-(16) give

$$\begin{aligned} S_0^k = &\sum_{j=0}^{\ell_0} a^{k-2j-1}b^{2j}\left(\binom{k}{2j}aF_0(j) + \binom{k}{2j+1}bG_0(j)\right)I + \\ &+ \sum_{j=0}^{\ell_0} a^{k-2j-1}b^{2j}\left(\binom{k}{2j}aF_1(j) + \binom{k}{2j+1}bG_1(j)\right)Z. \end{aligned} \tag{17}$$

Now after the simple calculations we obtain

$$S_0^k = H_0(k)I + H_1(k)Z, \tag{18}$$

where modulo p^m

$$\begin{cases} H_0(k) = a^k + ka^{k-1}b(1+b^2h_{01}) + k^2a^{k-2}b^2(\overline{2}+b^2h_{02}) + \\ \qquad + k^3a^{k-2}b^3H_{03}(k), \\ H_1(k) = a^{k-1}bk(1+b^2h_{11}) + k^3b^3H_{13}(k), \\ H_{03}(k), H_{13}(k) \in \mathbb{Z}[k],\ \ h_{01}, h_{02}, h_{11} \in \mathbb{Z}. \end{cases} \tag{19}$$

Repeating the argument used in the proof of relations (18),(19) we easy deduce that

$$\sum_{\ell=1}^{k_0} S_0^{k-\ell} \sum_{j=0}^{k} {\sum_{i_1,\ldots,i_\ell}}' Y_{i_1}\cdots Y_{i_\ell} = \overline{H}_0(k)I + \overline{H}_1(k)Z, \tag{20}$$

where

$$\begin{cases} \overline{H}_0(k) = kca^k\left[(\overline{f}_{0,0} + \overline{H}_{01}b) + kb^2\overline{H}_{02}(k)\right], \\ \overline{H}_1(k) = kbca^k\overline{H}_{1,0}(k), \end{cases} \tag{21}$$

$\overline{H}_{01}(k), \overline{H}_{02}(k), \overline{H}_{10}(k)$ are the integer polynomials with coefficients depending only on $\overline{a}, (\overline{a})^2, \ldots, (\overline{a})^m$, $b_0, b_0^2, \ldots, b_0^{\left[\frac{m+1}{\nu}\right]}$, $c_0, c_0^2, \ldots, c_0^{\left[\frac{m+1}{\mu}\right]}$, $b_0 = \frac{b}{p^\nu}$, $c_0 = \frac{c}{p^\mu}$.

After all this preliminaries it is straightforward to establish two representations for y_n:

Lemma 3. *Let p be a prime number, $p \geq 5$, and let $m \in \mathbb{N}$, $m \geq 3$; $a, b, c \in \mathbb{Z}$, $GCD(a, p) = 1$, $b \equiv c \equiv 0 (mod\ p)$, $\nu = \nu_p(b)$, $\mu = \nu_p(c)$, $\nu < \mu$, also, let $\{y_k\}$ is the sequence from (2). Then for any $y_0 \in R_m^*$ and $k = 0, 1, 2, \dots$ we have*

$$\begin{aligned} y_{2k} &= (kb - 2^{-1}k(k^2-1)a^{-1}b^3 + G_0(k)) + \\ &+ (1 + k(k+1)a^{-1}c + G_1(k))y_0 + \\ &+ (-ka^{-1}b - (k^3c + k^2(k+1)a^{-1})bc + \\ &+ (2^{-1}3k^3 - 2k^2 + 2^{-1}k)a^{-2}b^3 + G_2(k))y_0^2 + \\ &+ (k^2a^{-2}b^2 - k^2a^{-1}c + G_3(k))y_0^3 + G_4(k, y_0)y_0^4; \\ y_{2k+1} &= ((k+1)b - k^2a^{-1}c + k(k-1)a^{-1}b^3 + H_0(k)) + \\ &+ ((2k+)c + H_1(k))y_0 + (a - k^2c - 2k^2b^2 + H_{-1}(k))y_0^{-1} + \\ &+ (-kab + 2^{-1}3k^2(k+1)b^3 + 4^{-1}k^2(k^2-1)a^{-1}b^3 + \\ &+ H_{-2}(k))y_0^{-2} + y_0^{-3}H_3(k, y_0^{-1}), \end{aligned}$$

where

$G_i(k) \in \mathbb{Z}[k]$, $G_i(0) = 0$, $G_i(k) \equiv 0 (mod\ p^{\min(2\nu+\mu, 4\nu)})$, $i = 0, 1, 2, 3$;
$H_i(k) \in \mathbb{Z}[k]$, $H_i(0) = 0$, $H_i(k) \equiv 0 (mod\ p^{\min(2\nu+\mu, 4\nu)})$, $i = -2, \pm 1, 0$;
$G_4(k, u)$, $H_3(k, u)$, *are the polynomials on* k, u,

moreover,

$$G_4(0, u) = H_3(0, u) = 0,\ G_4(k, u) \equiv H_3(k, u) (mod\ p^{\min(2\nu+\mu, 4\nu)}).$$

Lemma 4. *For $k = 0, 1, 2, \dots$ we have*

$$\begin{aligned} y_{2k} &= y_0 + k(b(1 - a^{-1}y_0^2) + 2a^{-1}b^3(a + y_0^2) + a^{-1}cy_0 + C_1(y_0)) + \\ &+ k^2(-a^{-1}b^2y_0 + a^{-1}cy_0(1 - y_0^2) + C_2(y_0)) + k^3C_3(k, y_0) \\ y_{2k+1} &= (b + cy_0 + ay_0^{-1}) + k(b(1 - ay_0^{-2}) + 2cy_0 + D_1(y_0, y_0^{-1})) + \\ &+ k^2(c(a^{-1} - y_0^{-1}) + D_2(y_0, y_0^{-1})) + k^3D_3(k, y_0, y_0^{-1}) \end{aligned}$$

where $C_1(y_0) \equiv C_2(y_0) \equiv C_3(k, y_0) \equiv 0 (mod\ p^{\min(\nu+\mu, 3\nu)})$,
$D_1(y_0, y_0^{-1}) \equiv D_2(y_0, y_0^{-1}) \equiv D_3(k, y_0, y_0^{-1}) \equiv 0 (mod\ p^{\min(\nu+\mu, 3\nu)})$
for every $y_0, y_0^{-1} \in R_m^*$, $k \in \mathbb{Z}$.

Corollary 1. *Let τ be a period length of the sequence $\{y_n\}$ generated by recursion (2), y_0 be an initial value, and let $\nu_p(b) = \nu$, $\nu_p(c) = \mu > \nu$.*

(A) If $a \not\equiv y_0{}^2 (mod\ p)$, then $\tau = 2p^{m-\nu}$.
(B) If $\nu_p(a - y_0^2) = \delta < \min(3\nu, \mu)$, then $\tau = 2p^{m-\nu-\delta}$.
(C) Otherwise: $\tau \leq 2p^{m-\nu-\min(3\nu,\mu)}$.

4 Main results

Let the sequence $\{y_n\}$ is produced by recursion (2) and let the least length of period for $\{y_n\}$ is equal to τ.

For any N, $1 \leq N \leq \tau$, and $h \in \mathbb{Z}$ we define the sum

$$S_N(h, y_0) = \sum_{n=0}^{N-1} e_m(hy_n)$$

Theorem 1. *Let $\{y_n\}$ is the sequence generated by the recursion (2) with the parameters a, b, c and the function $F(n)$, $F(0) = 0$, and let $0 \le \nu_p(a - y_0^2) < \nu = \nu_p(b)$, $2\nu < \mu = \nu_p(c)$, $\nu_p(h) = s$. Then we have*

$$|S_N(h, y_0)| \le \begin{cases} 2p^{\frac{m+\nu+s}{2}} \left(\frac{N}{\tau} + \frac{\log \tau}{p}\right) & if \quad \nu + s < m \\ N & else. \end{cases}$$

Theorem 2. *In the notations of Theorem 1 we have*

$$\overline{S}_N(h) = \frac{1}{\varphi(p^m)} \sum_{y_0 \in R_m^*} |S_N(h, y_0)| \le 3Np^{-\frac{m-s-\nu}{4}}$$

The proofs of these theorems are an analogue of the proofs for Theorem 7 and 8[5] and by the representations of y_n which have been obtained in Lemmas 3 and 4, and using Lemmas 1 and 2.

Now applying the Turan-Koksma inequality(see,[3]) for the discrepancy D_N we obtain

Theorem 3. *Let $p > 2$ be a prime number, $y_0, a, b, c, m \in \mathbb{Z}$, $m \ge 3$ and let a, y_0 are co-primes to p and let $b \equiv c \equiv 0 (mod\ p)$, $0 < \nu_p(b) < \nu_p(c)$, $a \not\equiv y_0^2 (mod\ p)$. Then for the sequence $\{x_k\}$, $x_k = \frac{y_k}{p^m}$, $k = 0, 1, \ldots$, where y_k determine by (2) we have*

$$D_N(x_0, x_1, \ldots, x_{N-1}) \le \frac{1}{p^m} + 2N^{-1}p^{\frac{m-\nu}{2}} \left(\frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^2 + 1\right),$$

where $1 \le N \le \tau$, and τ is the least length of a period for $\{y_k\}$.

Next, we denote

$$X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1}),\ s = 2, 3, 4.$$

Theorem 4. *The discrepancy $D_N^{(s)}(X_0^{(s)}, X_1^{(s)}, \ldots, X_{N-1}^{(s)})$ produced by the recursion (2) with the period $\tau = 2p^{m-\nu}$ satisfies the inequality*

$$D_\tau^{(s)} \le \frac{\sqrt{p}}{\sqrt{p} - 1} p^{-\frac{m}{2}+\nu} \left(\frac{1}{\pi}\log p^{m-\nu} + \frac{3}{5}\right)^s + 2p^{-m+\nu}.$$

From the Theorems 3 and 4 it follows that the sequence $\{x_n\}$, $x - n = \frac{y_n}{p^m}$ passes the s-serial tests, $s = 2, 3, 4$ on equidistribution and statistical independence.

Thus, by the complexity of reconstruction for the parameters a, b, c, y_0, $F(u)$ under recursion (2) the sequence of PRN's $\{y_n\}$ can be used in cryptographical applications.

References

1. S.R. Blackburn, D. Gomez-Peres, I. Gutierrez and I. Shparlinski. Predicting nonlinear pseudorandom number generators. *Math. Comp.*, 74(251):1471–1494, 2004.

2. S.R. Blackburn, D. Gomez-Peres, I. Gutierrez and I. Shparlinski. Reconstructing noisy polynomial evaluation in residue rings. *J. of Algorithm*, 61(2):47–59, 2006.
3. H. Niederreiter. Random number generation and Quasi-Monte Carlo methods. *SIAM, Philadelphia*, 1992.
4. 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.
5. P. Varbanets, S. Varbanets. Exponential sums over the sequences of inversive congruential pseudorandom numbers with prime-power modulus. *VoronoÏ's impact on modern science*, Book 4(1):112–130, 2008.