MATHEMATICS OF COMPUTATION
Volume 65, Number 213
January 1996, Pages 227–233

ON A NONLINEAR CONGRUENTIAL PSEUDORANDOM NUMBER GENERATOR

TAKASHI KATO, LI-MING WU, AND NIRO YANAGIHARA

ABSTRACT. A nonlinear congruential pseudorandom number generator with modulus $M = 2^w$ is proposed, which may be viewed to comprise both linear as well as inversive congruential generators. The condition for it to generate sequences of maximal period length is obtained. It is akin to the inversive one and bears a remarkable resemblance to the latter.

1. INTRODUCTION

A standard method of generating uniform pseudorandom numbers in the interval $I = [0, 1)$ (denoted as PRN) is the linear congruential one, which is given as follows: For a large modulus M, let

$$Z_M = \{0, 1, ..., M-1\} = Z/M.$$

A sequence $\{y_n\}$ of integers in Z_M is generated by the linear recursion

$$y_{n+1} \equiv cy_n + b \pmod{M}, \quad n = 0, 1, ..., \tag{1.1}$$

where $c, b \in Z_M$. The PRN are obtained by the normalization

$$x_n = y_n/M. \tag{1.2}$$

This linear method is widely used, and has been investigated by several authors [9]. However, there is some drawback owing to the linearity of the recursion, e.g., so-called coarse lattice structure. This state of affairs provided the motivation for several recent proposals of nonlinear congruential generators [1, 5, 9, 12].

Among them, one of the most interesting is the inversive congruential method [12], with prime modulus ($M = p$ for a prime p) or power of two modulus ($M = 2^w$ for a large integer w). The latter is described as follows: For $M = 2^w$, let

$$G_M = \{1, 3, ..., M-1\} = \{\text{positive odd integers less than } M\}.$$

For any $u \in G_M$, there is a unique $\overline{u} \in G_M$ such that $u\overline{u} \equiv 1 \pmod{M}$. Now a sequence $\{y_n\} \subset G_M$ is generated by the inversive recursion

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{M}, \quad n = 0, 1, ..., \tag{1.3}$$

Received by the editor October 7, 1994 and, in revised form, February 12, 1995.
1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 11K45.
Key words and phrases. Pseudorandom number, maximal period length, nonlinear congruential generator, power of two modulus.

in which $a, b \in Z_M$ are chosen so that $y_n \in G_M$ implies $y_{n+1} \in G_M$.

In the present note, we propose another nonlinear method similar to (1.3), i.e., for the modulus $M = 2^w$, we put with $y_0 \in G_M$,

$$y_{n+1} \equiv a\overline{y}_n + b + cy_n \pmod{M}, \quad n = 0, 1, ..., \tag{1.4}$$

in which of course $a, b, c \in Z_M$ should be chosen so that $y_n \in G_M$ implies $y_{n+1} \in G_M$. The PRN $\{x_n\}$ is defined by (1.2).

We will show that the *modified inversive method* (1.4) bears a close resemblance to (1.3). That is, we prove the following theorem.

Theorem. *Let $M = 2^w, w \geq 3$. Then the PRN $\{x_n\}$ derived from* (1.4) *is purely periodic with period $M/2$ if and only if*

$$a + c \equiv 1 \pmod 4 \quad \text{and} \quad b \equiv 2 \pmod 4.$$

Among the constants in the theorem, one of a or c may be zero, hence (1.4) can be viewed as to comprise both (1.1) and (1.3).

The discrepancy as well as lattice structure of the sequence $\{x_n\}$, generated by (1.4), will be studied in future papers.

Our proof of the theorem is very similar to the proofs in [5, Theorem] and [12, Theorem 8.9]. But we hope that the modified method (1.4) would be of some interest. By the way, we note that the difference equation

$$y(t+1) = y(t) + b + a/y(t)$$

has been studied from the viewpoint of complex analytic theory [7, 8, 13, 14, 15]. Its solutions exhibit distinctly fractal features.

2. Proof of Theorem

We divide the proof into three subsections (I),(II),(III).

(I) **Necessity.** Write the period of $\{x_n\}$ as $\mathrm{per}(x_n)$. Obviously, $\mathrm{per}(x_n) \leq M/2$.

Suppose that $\{x_n\}$ is purely periodic with $\mathrm{per}(x_n) = M/2$. Then $\{y_0, y_1, ..., y_{M/2-1}\} = G_M$, so we can assume that $y_0 = 1$. If we consider the sequence $\{y_n\}$ modulo 4, then it has period 2; hence $y_2 \equiv 1 \pmod 4$. If this sequence is taken modulo 8, then it has period 4; hence $y_2 \neq 1 \pmod 8$, and so $y_2 \equiv 5 \pmod 8$. Since $\bar{u} \equiv u \pmod 8$ for $u \in G_M$, it follows from (1.4) that

$$y_2 \equiv c(a+b+c) + b + a(a+b+c) = (a+c)^2 + (a+c+1)b \mod 8.$$

Suppose $a+c$ is even. Then b must be odd since $y_1 \equiv a+b+c \pmod 8 \in G_M$. Put $a+c = 2r,\ b = 1+2s$. Then $y_2 = 4r^2 + (1+2r)(1+2s) = 1 + 2(r+s) + 4rs + 4r^2$, which must be $\equiv 1 \pmod 4$. Hence, $r+s = 2t,\ t \in Z$. Then $y_1 = 1+4t \equiv 1 \pmod 4$, which contradicts that $\{y_n\}$ has period 2 (mod 4). Therefore, $a+c$ must be odd. Hence, $(a+c)^2 \equiv 1 \pmod 8$, and we have

$$y_2 \equiv 1 + (a+c+1)b \pmod 8,$$

so $(a+c+1)b \equiv 4 \pmod 8$. This implies $a+c \equiv 1 \pmod 4,\ b \equiv 2 \pmod 4$.

(II) **Sufficiency for the case where c is an even number.** Suppose $a+c \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$. Consider first the case $y_0 = 1$. For $M = 8$, it is checked by the above arguments that $\mathrm{per}(y_n) = 4$. Now let $M = 2^w$ with $w \geq 4$.

In this subsection we suppose that c is an even number.

Define a sequence $\{\alpha_n\} \subset G_M$, $n = 0, 1, 2, ...$, by

$$\alpha_{n+2} \equiv \overline{\alpha}_n(a{\alpha_n}^2 + b\alpha_n\alpha_{n+1} + c{\alpha_{n+1}}^2) \pmod M. \tag{2.1}$$

Put $\alpha_0 = \alpha_1 = 1$. By induction on n, we obtain

$$y_n \equiv \overline{\alpha}_n\alpha_{n+1} \pmod M,\ n = 0, 1, ... \tag{2.2}$$

Write (2.1) as

$$\alpha_{n+2} \equiv (a+c)\alpha_n + b\alpha_{n+1} + c\beta_n \pmod M, \tag{2.3}$$

$$\beta_n = \overline{\alpha}_n({\alpha_{n+1}}^2 - {\alpha_n}^2). \tag{2.3'}$$

With the integer matrix

$$A = \begin{pmatrix} 0 & 1 \\ a+c & b \end{pmatrix}$$

we see, from (2.3), that

$$\begin{pmatrix} \alpha_{n+1} \\ \alpha_{n+2} \end{pmatrix} \equiv A \begin{pmatrix} \alpha_n \\ \alpha_{n+1} \end{pmatrix} + c \begin{pmatrix} 0 \\ \beta_n \end{pmatrix},$$

and so

$$\begin{pmatrix} \alpha_n \\ \alpha_{n+1} \end{pmatrix} \equiv A^n \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} + R_n \pmod M, \tag{2.4}$$

where

$$R_n = c \begin{pmatrix} 0 \\ \beta_{n-1} \end{pmatrix} + cA \begin{pmatrix} 0 \\ \beta_{n-2} \end{pmatrix} + \cdots + cA^{n-1} \begin{pmatrix} 0 \\ \beta_0 \end{pmatrix}.$$

By induction on $h \geq 2$, using $a + c \equiv 1 \pmod 4$, $b \equiv 2 \pmod 4$, it is shown, as in [12, p.188], that for $m = 2^h$

$$A^m \equiv \begin{pmatrix} 2mp + m + 1 & 2mq + 3m \\ 2mq + 3m & 2mp + 3m + 1 \end{pmatrix} \mod 4m = 2^{h+2}, \tag{2.5}$$

for all $h \geq 2$, with some integers p, q.

We will show that, for $m = 2^h$ $(2 \leq h \leq w-1)$,

$$R_m = 4mS_m \tag{2.6}$$

for an integer vector S_m . Equation (2.6) holds for $h = 2$, since c *is assumed to be even*. Now suppose it holds for $m = 2^h$. Then

$$\alpha_m = 1 + 2m(p+q) + 4m + 4mT_0 + 4m{S_m}^{(0)} + s_mM,$$

$$\alpha_{m+1} = 1 + 2m(p+q) + 6m + 4mT_1 + 4m{S_m}^{(1)} + s_{m+1}M$$

with integers T_0, T_1, s_m, s_{m+1}, where we write $S_m = {}^t({S_m}^{(0)}, {S_m}^{(1)})$. Hence, we have

$$\alpha_m = \alpha_0 + 2mU_0, \quad \alpha_{m+1} = \alpha_1 + 2mU_1$$

with integers U_0, U_1. Then

$$\beta_m = \overline{\alpha}_m\big\{(1+2mU_0)^2 - (1+2mU_1)^2\big\} = 4mW_0 = \beta_0 + 4mW_0$$

for an integer W_0. Thus,

$$\alpha_{m+2} = (a+c)(\alpha_0 + 2mU_0) + b(\alpha_1 + 2mU_1) + c\beta_m = \alpha_2 + 2mU_2,$$

with an integer U_2. It is easy to see that

$$\overline{\alpha}_{m+1} = \overline{\alpha}_1 + 2mV_1, \quad \overline{\alpha}_{m+2} = \overline{\alpha}_2 + 2mV_2.$$

Then

$$\begin{aligned}\beta_{m+1} &= \overline{\alpha}_{m+1}\big\{(\alpha_2 + 2mU_2)^2 - (\alpha_1 + 2mU_1)^2\big\} \\ &= 4m\overline{\alpha}_{m+1}(\alpha_2 U_2 - \alpha_1 U_1 + m{U_2}^2 - m{U_1}^2) \\ &\qquad + (\overline{\alpha}_{m+1} - \overline{\alpha}_1)({\alpha_2}^2 - {\alpha_1}^2) + \overline{\alpha}_1({\alpha_2}^2 - {\alpha_1}^2) \\ &= \beta_1 + 4mW_1\end{aligned}$$

with an integer W_1, since ${\alpha_{k+1}}^2 - {\alpha_k}^2$ is divided by 8 for any k.

Repeating this procedure, we get

$$\alpha_{m+k} = \alpha_k + 2mU_k \quad \text{with some integer } U_k, \quad k = 0, ..., m-1, \tag{2.7}$$

$$\overline{\alpha}_{m+k} = \overline{\alpha}_k + 2mV_k \quad \text{with some integer } V_k, \quad k = 0, ..., m-1, \tag{2.8}$$

$$\beta_{m+k} = \beta_k + 4mW_k \quad \text{with some integer } W_k, \quad k = 0, ..., m-1. \tag{2.9}$$

Now

$$\begin{pmatrix} \alpha_{2m} \\ \alpha_{2m+1} \end{pmatrix} = A^{2m} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} + R_{2m},$$

in which we obtain by (2.9)

$$\begin{aligned} R_{2m} &= c\begin{pmatrix} 0 \\ \beta_{2m-1} \end{pmatrix} + cA\begin{pmatrix} 0 \\ \beta_{2m-2} \end{pmatrix} + \cdots + cA^{m-1}\begin{pmatrix} 0 \\ \beta_m \end{pmatrix} \\ &\quad + cA^m\begin{pmatrix} 0 \\ \beta_{m-1} \end{pmatrix} + cA^{m+1}\begin{pmatrix} 0 \\ \beta_{m-2} \end{pmatrix} + \cdots + cA^{2m-1}\begin{pmatrix} 0 \\ \beta_0 \end{pmatrix} \\ &= c\begin{pmatrix} 0 \\ \beta_{m-1} \end{pmatrix} + cA\begin{pmatrix} 0 \\ \beta_{m-2} \end{pmatrix} + \cdots + cA^{m-1}\begin{pmatrix} 0 \\ \beta_0 \end{pmatrix} \\ &\quad + A^m\left\{c\begin{pmatrix} 0 \\ \beta_{m-1} \end{pmatrix} + cA\begin{pmatrix} 0 \\ \beta_{m-2} \end{pmatrix} + \cdots + cA^{m-1}\begin{pmatrix} 0 \\ \beta_0 \end{pmatrix}\right\} \\ &\quad + 4mc\left\{\begin{pmatrix} 0 \\ W_{m-1} \end{pmatrix} + A\begin{pmatrix} 0 \\ W_{m-2} \end{pmatrix} + \cdots + A^{m-1}\begin{pmatrix} 0 \\ W_0 \end{pmatrix}\right\} \\ &= (I + A^m)R_m + 4mcW, \end{aligned}$$

thus by (2.5) and (2.6) we have, with an integer vector W,

$$R_{2m} = 8m\{(I + A^m)/2\} S_m + 8m(c/2)W = 4(2m)S_{2m},$$

since c is even by our assumption. Hence (2.6) holds for $2m = 2^{h+1}$. Thus, we obtain (2.6) for any $m = 2^h$ $(2 \le h \le w-1)$, from which we see by the above arguments that (2.7) holds for any $m = 2^h$ $(2 \le h \le w-1)$.

By (2.7) with $m = M/2$ $(h = w-1)$, we obtain $\alpha_{n+M/2} = \alpha_n$ for any n, which implies $y_{n+M/2} = y_n$. Therefore, $\mathrm{per}(y_n)$ divides $M/2$. Since we already know that $\mathrm{per}(y_n) \le M/2$, to prove that $\mathrm{per}(y_n) = M/2$, it suffices to show that $\mathrm{per}(y_n) > M/4$.

If we had $\mathrm{per}(y_n) \le M/4$, then $y_{M/4} = y_0 = 1$, and so $\alpha_{M/4+1} \equiv \alpha_{M/4} \pmod M$ by (2.2). However, by (2.4) with $n = M/4$, and by (2.5), (2.6) with $h = w-2$, we obtain a contradiction $\alpha_{M/4+1} \equiv \alpha_{M/4} + M/2 \pmod M$. So $\mathrm{per}(y_n) = M/2$ is proved if $y_0 = 1$. In particular, $\{y_0, y_1, ..., y_{M/2-1}\} = G_M$. If we have an arbitrary initial value $y_0 \in G_M$, then the sequence $y_0, y_1, ...$ is a shifted version of the sequence with initial value 1, and so again $\mathrm{per}(x_n) = \mathrm{per}(y_n) = M/2$.

(III) **Sufficiency for the case where c is an odd number.** Now we turn to the case when c is odd. Then a must be even.

The equation (1.4) can be written as

$$y_{n+1} \equiv (a+c)y_n + b + a\overline{y}_n(1 - {y_n}^2) \mod M, \tag{2.10}$$

i.e.,

$$\begin{pmatrix} y_{n+1} \\ 1 \end{pmatrix} \equiv \begin{pmatrix} a+c & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_n \\ 1 \end{pmatrix} + a \begin{pmatrix} z_n \\ 0 \end{pmatrix} \mod M,$$

in which $z_n = \overline{y}_n(1 - {y_n}^2)$. Put

$$A = \begin{pmatrix} a+c & b \\ 0 & 1 \end{pmatrix}.$$

We obtain that

$$\begin{pmatrix} y_n \\ 1 \end{pmatrix} \equiv A^n \begin{pmatrix} y_0 \\ 1 \end{pmatrix} + R_n,$$

where

$$R_n = a \begin{pmatrix} z_{n-1} \\ 0 \end{pmatrix} + aA \begin{pmatrix} z_{n-2} \\ 0 \end{pmatrix} + \cdots + aA^{n-1} \begin{pmatrix} z_0 \\ 0 \end{pmatrix}. \tag{2.11}$$

Since $a + c \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$, we see by induction that, for $m = 2^h, h \ge 1$,

$$A^m = \begin{pmatrix} 1 + 4mP_m & 2m + 4mQ_m \\ 0 & 1 \end{pmatrix} \tag{2.12}$$

with integers P_m and Q_m . We will show that, for $m = 2^h, 1 \le h \le w-1$,

$$R_m = 4mS_m, \tag{2.13}$$

with integer vector $S_m = {}^t(s_m, 0)$. Equation (2.13) is easily seen to hold for $m = 2$ ($h = 1$). Suppose it holds for $m = 2^h$. Then

$$y_m = y_0 + 4mP_m y_0 + 2m + 4mQ_m + 4ms_m = y_0 + 2mU_0$$

with an integer U_0. Further, it is easy to see that

$$\overline{y}_m = \overline{y}_0 + 2mV_0$$

with an integer V_0. Then

$$z_m = (\overline{y}_0 + 2mV_0)\{1 - (y_0 + 2mU_0)^2\} = z_0 + 4mW_0$$

with an integer W_0, since $z_0 = 0$. Then

$$\begin{aligned} y_{m+1} &\equiv (a + c)(y_0 + 2mU_0) + b + a(z_0 + 4mW_0) \\ &= (a + c)y_0 + b + az_0 + 2mU_1 = y_1 + 2mU_1. \end{aligned}$$

Repeating this procedure, we get, for $k = 0, 1, ..., m - 1$,

$$y_{m+k} = y_k + 2mU_k, \tag{2.14}$$

$$\overline{y}_{m+k} = \overline{y}_k + 2mV_k, \tag{2.15}$$

$$z_{m+k} = z_k + 4mW_k. \tag{2.16}$$

Thus, with some integer vector T_m,

$$\begin{aligned} R_{2m} &= a\begin{pmatrix} z_{2m-1} \\ 0 \end{pmatrix} + aA\begin{pmatrix} z_{2m-2} \\ 0 \end{pmatrix} + ... + aA_{m-1}\begin{pmatrix} z_m \\ 0 \end{pmatrix} \\ &\quad + aA^m\begin{pmatrix} z_{m-1} \\ 0 \end{pmatrix} + aA^{m+1}\begin{pmatrix} z_{m-2} \\ 0 \end{pmatrix} + ... + aA^{2m-1}\begin{pmatrix} z_0 \\ 0 \end{pmatrix} \\ &= a\begin{pmatrix} z_{m-1} \\ 0 \end{pmatrix} + aA\begin{pmatrix} z_{m-2} \\ 0 \end{pmatrix} + ... + aA^{m-1}\begin{pmatrix} z_0 \\ 0 \end{pmatrix} \\ &\quad + A^m\left\{a\begin{pmatrix} z_{m-1} \\ 0 \end{pmatrix} + aA\begin{pmatrix} z_{m-2} \\ 0 \end{pmatrix} + ... + aA^{m-1}\begin{pmatrix} z_0 \\ 0 \end{pmatrix}\right\} \\ &\quad + 4ma\left\{\begin{pmatrix} W_{m-1} \\ 0 \end{pmatrix} + A\begin{pmatrix} W_{m-2} \\ 0 \end{pmatrix} + ... + A^{m-1}\begin{pmatrix} W_0 \\ 0 \end{pmatrix}\right\} \\ &= R_m + A^m R_m + 4maT_m \\ &= 4 \times (2m)[(I + A^m)/2]S_m + 4 \times (2m)(a/2)T_m \\ &= 4 \times (2m)S_{2m}, \end{aligned}$$

since a is even, which shows that (2.13) holds for $2m = 2^{h+1}$. Therefore, (2.13) holds for any $m = 2^h, 1 \le h \le w - 1$.

Hence, (2.14) holds for $m = M/2 = 2^{w-1}$, i.e., we obtain $y_{M/2} = y_0$. Thus, $\mathrm{per}(y_n)$ divides $M/2$. Suppose $\mathrm{per}(y_n) \le M/4$. Then $y_{M/4} = y_0$. But by (2.12) and (2.13), we obtain $y_{M/4} \equiv y_0 + M/2 \pmod{M}$, which is absurd. As in (II), we conclude that $\mathrm{per}(y_n) = M/2$.

References

1. J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers avoid the planes*, Math. Comp. **56** (1991), 297–301. MR **91k:**65021
2. ———, *Statistical independence of a new class of inversive congruential pseudorandom numbers*, Math. Comp. **60** (1993), 375–384. MR **93d:**65011
3. ———, *On generalized inversive congruential pseudorandom numbers*, Math. Comp. **63** (1994), 293–299. MR **94k:**11088
4. J. Eichenauer-Herrmann, H. Grothe, H. Niederreiter, and A. Topuzoglu, *On the lattice structure of a nonlinear generator with modulus* 2^α, J. Comput. Appl. Math. **31** (1990), 81–85. MR **91j:**65012
5. J. Eichenauer, J. Lehn, and A. Topuzoglu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51** (1988), 757–759. MR **89i:**65007
6. J. Eichenauer-Herrmann and H. Niederreiter, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus*, Math. Comp. **58** (1992), 775–779. MR **92i:**65018
7. T. Kimura, *On the iteration of analytic functions*, Funkcial. Ekvac. **14** (1971), 197–238. MR **46:**2019
8. ———, *On meromorphic solutions of the difference equation* $y(x+1) = y(x) + 1 + \lambda/y(x)$, Symposium on Ordinary Differential Equations, Lecture Notes in Math., vol. 312, Springer-Verlag, Berlin and New York, 1973, pp. 74–86. MR **53:**3527
9. D. E. Knuth, *The art of computer programming, Vol. 2, Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, MA, 1981. MR **83i:**68003
10. H. Niederreiter, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144. MR **90e:**65008
11. ———, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345. MR **92h:**65010
12. ———, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992. MR **93h:**65008
13. K. Takano, *On the hypertranscendency of solutions of a difference equation of Kimura*, Funkcial. Ekvac. **16** (1973), 241–254. MR **50:**5074
14. N. Yanagihara, *Meromorphic solutions of the difference equation* $y(x+1) = y(x)+1+\lambda/y(x)$. I, Funkcial. Ekvac. **21** (1978), 97–104. MR **80a:**30021
15. ———, *Meromorphic solutions of the difference equation* $y(x+1) = y(x) + 1 + \lambda/y(x)$. II, Funkcial. Ekvac. **21** (1978), 223–240. MR **81h:**30028

Department of Mathematics, Faculty of Science, Chiba University, 1-33 Yayoi-cho, Inage-ku, Chiba City, 263 JAPAN

E-mail address: yanaba@math.s.chiba-u.ac.jp