MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 193
JANUARY 1991, PAGES 297–301

INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS AVOID THE PLANES

JÜRGEN EICHENAUER-HERRMANN

ABSTRACT. Nonlinear congruential pseudorandom number generators based on inversions have recently been introduced and analyzed. These generators do not show the lattice structure of the widely used linear congruential method. In the present paper it is proved that the points formed by d consecutive pseudorandom numbers of an inversive congruential generator with prime modulus possess an even stronger property: Any hyperplane in d-space contains at most d of these points, that is to say, the hyperplane spanned by d arbitrary points of an inversive congruential generator contains no further points. This feature makes the inversive congruential method particularly attractive for simulation problems where linear structures within the generated points should be avoided.

1. INTRODUCTION

The well-known lattice structure of linear congruential pseudorandom numbers makes them too regular for certain simulation purposes [2]. This defect of the linear congruential method was first pointed out by G. Marsaglia in his famous paper *Random numbers fall mainly in the planes* [4]. Therefore, nonlinear congruential pseudorandom number generators, which do not show the undesirable lattice structure, have been proposed and studied recently (cf. [1, 2, 3, 5, 6, 7]). In the present paper a nonlinear congruential generator based on inversions with respect to a prime modulus is considered.

Let $p \geq 3$ be a prime number, and denote by $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ and $\mathbb{Z}_{p,1} = \{1, 2, \ldots, p-1\}$ the set of nonnegative and the set of positive integers less than p, respectively. For an integer $x \in \mathbb{Z}_{p,1}$, let x^{-1} be the multiplicative inverse of x modulo p. For integers $a, b \in \mathbb{Z}_{p,1}$ an inversive congruential sequence $(x_n)_{n \geq 0}$ in $\mathbb{Z}_p$ is obtained by the recursion

$$x_{n+1} \equiv \begin{cases} ax_n^{-1} + b \pmod{p} & \text{for } x_n \neq 0, \\ b & \text{for } x_n = 0, \end{cases} \qquad n \geq 0.$$

In [2], conditions are derived for the generated sequence to have maximal period length p, which we assume to be true from now on. For example, the sequence has period length p if $x^2 - bx - a$ is a primitive polynomial over the finite field $\mathbb{Z}_p$.

Received November 30, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C10; Secondary 11K45.

Let d be an integer with $2 \leq d < p$, and denote by

$$V_d = \{(x_n, \ldots, x_{n+d-1}) \in \mathbb{Z}_p^d | x_n, \ldots, x_{n+d-2} \neq 0,\ 0 \leq n < p\}$$

the set of d-tuples of consecutive pseudorandom numbers generated by the inversive congruential method, where those d-tuples are omitted which contain a zero in one of the first $d-1$ coordinates. These $d-1$ "boundary" points are excluded for the sake of simplicity. For arbitrary integers $\alpha_0, \alpha_1, \ldots, \alpha_d \in \mathbb{Z}_p$ with $(\alpha_1, \ldots, \alpha_d) \neq (0, \ldots, 0)$ the set

$$H = \{(z_1, \ldots, z_d) \in \mathbb{Z}_p^d | \alpha_1 z_1 + \cdots + \alpha_d z_d \equiv \alpha_0 \pmod{p}\}$$

is a hyperplane in $\mathbb{Z}_p^d$. The main result of the present paper, which is proved in §3, is given in the following theorem.

Theorem. *Any hyperplane H in $\mathbb{Z}_p^d$ contains at most d points of the set V_d.*

This result demonstrates that, in contrast to the linear congruential method, inversive congruential pseudorandom numbers do not fall in the planes, they even "avoid" concentrating on any hyperplane. Therefore, the inversive congruential method seems to be particularly suitable for simulation problems where linear structures within the generated points may influence the simulation outcome, e.g., in simulating certain geometric probabilities.

2. Auxiliary results

First, some further notation is necessary. Put $\mathbb{Z}_{p,0} = \mathbb{Z}_p$. A function $f_1 : \mathbb{Z}_{p,1} \to \mathbb{Z}_p$ is given by

$$f_1(x) \equiv ax^{-1} + b \pmod{p},$$

and for k with $2 \leq k < p$, sets $\mathbb{Z}_{p,k}$ and functions $f_k : \mathbb{Z}_{p,k} \to \mathbb{Z}_p$ are defined recursively by

$$\mathbb{Z}_{p,k} = \{x \in \mathbb{Z}_{p,k-1} | f_{k-1}(x) \neq 0\}$$

and

$$f_k(x) = f_1(f_{k-1}(x)),$$

respectively. Let $\pi_0 : \mathbb{Z}_p \to \mathbb{Z}_p$ with $\pi_0(x) = x$ be the identity on $\mathbb{Z}_p$, and for k with $1 \leq k < p$, define functions $\pi_k : \mathbb{Z}_{p,k} \to \mathbb{Z}_p$ by

$$\pi_k(x) \equiv x \prod_{j=1}^{k} f_j(x) \pmod{p}.$$

A linear congruential sequence $(\tau_n)_{n \geq 0}$ in $\mathbb{Z}_p$ is given by $\tau_0 = 0$, $\tau_1 = 1$, and

$$\tau_n \equiv b\tau_{n-1} + a\tau_{n-2} \pmod{p}, \qquad n \geq 2,$$

and for k with $0 \leq k < p$, linear functions $l_k : \mathbb{Z}_p \to \mathbb{Z}_p$ are defined by

$$l_k(x) \equiv \tau_{k+1}x + \tau_k a \pmod{p}.$$

Lemma 1. *Let* $0 \le k < p$. *The function* π_k *is the restriction of the linear function* l_k *to the set* $\mathbb{Z}_{p,k}$, *i.e.,* $\pi_k(x) = l_k(x)$ *for* $x \in \mathbb{Z}_{p,k}$.

Proof. The lemma is proved by induction on k. For $k = 0$ the assertion follows from $\tau_0 = 0$ and $\tau_1 = 1$. If it is valid for some integer k with $0 \le k < p-1$, then

$$\begin{aligned}\pi_{k+1}(x) &\equiv x\pi_k(f_1(x)) \equiv xl_k(f_1(x)) \\ &\equiv x(\tau_{k+1}f_1(x) + \tau_k a) \\ &\equiv x(\tau_{k+1}(ax^{-1} + b) + \tau_k a) \\ &\equiv (b\tau_{k+1} + a\tau_k)x + \tau_{k+1}a \\ &\equiv \tau_{k+2}x + \tau_{k+1}a \equiv l_{k+1}(x) \pmod p\end{aligned}$$

for $x \in \mathbb{Z}_{p,k+1}$, which completes the proof. □

It follows from the results in [2] that $\tau_1, \ldots, \tau_p \neq 0$. Therefore, $\xi_k \in \mathbb{Z}_p$ with

$$\xi_k \equiv -\tau_{k+1}^{-1}\tau_k a \pmod p$$

is the unique zero of the linear function l_k for $0 \le k < p$.

Lemma 2. *The zeros* $\xi_0, \ldots, \xi_{p-1}$ *of the linear functions* $l_0, \ldots, l_{p-1}$ *are pairwise different, i.e.,* $\{\xi_0, \ldots, \xi_{p-1}\} = \mathbb{Z}_p$.

Proof. For $1 \le k \le p$, define integers $y_k \in \mathbb{Z}_p$ by $y_k \equiv \tau_{k+1}\tau_k^{-1} \pmod p$. Then

$$\begin{aligned}y_{k+1} &\equiv (b\tau_{k+1} + a\tau_k)\tau_{k+1}^{-1} \\ &\equiv ay_k^{-1} + b \pmod p, \qquad 1 \le k < p,\end{aligned}$$

i.e., $y_1, \ldots, y_p$ are the first p elements of an inversive congruential sequence with maximal period length p, which implies that $\{y_1, \ldots, y_p\} = \mathbb{Z}_p$. Because of

$$\xi_k \equiv b - y_{k+1} \pmod p, \qquad 0 \le k < p,$$

the integers $\xi_0, \ldots, \xi_{p-1}$ are pairwise different. □

For arbitrary integers $\alpha_0, \alpha_1, \ldots, \alpha_d \in \mathbb{Z}_p$ with $(\alpha_1, \ldots, \alpha_d) \neq (0, \ldots, 0)$, a polynomial $P_d: \mathbb{Z}_p \to \mathbb{Z}_p$ is defined by

$$P_d(x) \equiv (\alpha_1 x - \alpha_0)\prod_{j=0}^{d-2} l_j(x) + \sum_{k=2}^{d} \alpha_k l_{k-1}(x) \prod_{\substack{j=0 \\ j\neq k-2}}^{d-2} l_j(x) \pmod p.$$

Lemma 3. *The polynomial* P_d *has at most* d *zeros.*

Proof. First, we prove by contradiction that the polynomial P_d is not identically zero. Indeed, assume that $P_d(x) = 0$ for every $x \in \mathbb{Z}_p$. Since ξ_i is the zero of the linear function l_i, it follows that

$$P_d(\xi_i) \equiv \alpha_{i+2}l_{i+1}(\xi_i)\prod_{\substack{j=0 \\ j\neq i}}^{d-2} l_j(\xi_i) \pmod p$$

for $0 \le i \le d-2$. Hence, the assumption $P_d(\xi_i) = 0$ and Lemma 2 imply that $\alpha_{i+2} = 0$ for $0 \le i \le d-2$ which yields

$$P_d(x) \equiv (\alpha_1 x - \alpha_0) \prod_{j=0}^{d-2} l_j(x) \pmod{p}$$

for $x \in \mathbb{Z}_p$. Therefore, it follows from the assumption $P_d(\xi_{d-1}) = P_d(\xi_d) = 0$ and Lemma 2 that $\alpha_1 = 0$, which contradicts $(\alpha_1, \ldots, \alpha_d) \neq (0, \ldots, 0)$ and shows that the polynomial P_d is not identically zero. This proves the lemma, since P_d is at most of degree d. □

3. Proof of the theorem

The set V_d can be written in the form

$$V_d = \{(x, f_1(x), \ldots, f_{d-1}(x)) \in \mathbb{Z}_p^d | x \in \mathbb{Z}_{p,d-1}\},$$

since the inversive congruential sequence $(x_n)_{n \ge 0}$ has maximal period length p. Therefore,

$$\begin{aligned}
\#(H \cap V_d) &= \#\{x \in \mathbb{Z}_{p,d-1} | \alpha_1 x + \alpha_2 f_1(x) + \cdots + \alpha_d f_{d-1}(x) \equiv \alpha_0 \pmod{p}\} \\
&= \#\left\{ x \in \mathbb{Z}_{p,d-1} | (\alpha_1 x + \alpha_2 f_1(x) + \cdots + \alpha_d f_{d-1}(x)) \prod_{j=0}^{d-2} \pi_j(x) \right. \\
&\qquad \left. \equiv \alpha_0 \prod_{j=0}^{d-2} \pi_j(x) \pmod{p} \right\} \\
&= \#\left\{ x \in \mathbb{Z}_{p,d-1} | (\alpha_1 x - \alpha_0) \prod_{j=0}^{d-2} \pi_j(x) \right. \\
&\qquad \left. + \sum_{k=2}^{d} \alpha_k f_{k-1}(x) \pi_{k-2}(x) \prod_{\substack{j=0 \\ j \neq k-2}}^{d-2} \pi_j(x) \equiv 0 \pmod{p} \right\} \\
&= \#\left\{ x \in \mathbb{Z}_{p,d-1} | (\alpha_1 x - \alpha_0) \prod_{j=0}^{d-2} \pi_j(x) \right. \\
&\qquad \left. + \sum_{k=2}^{d} \alpha_k \pi_{k-1}(x) \prod_{\substack{j=0 \\ j \neq k-2}}^{d-2} \pi_j(x) \equiv 0 \pmod{p} \right\}
\end{aligned}$$

for any hyperplane H in $\mathbb{Z}_p^d$. Now, Lemmas 1 and 3 show that

$$\#(H \cap V_d) = \#\{x \in \mathbb{Z}_{p,d-1} | P_d(x) = 0\} \le d,$$

which completes the proof of the theorem.

BIBLIOGRAPHY

1. J. Eichenauer, H. Grothe, and J. Lehn, *Marsaglia's lattice test and non-linear congruential pseudo random number generators*, Metrika **35** (1988), 241–250.
2. J. Eichenauer and J. Lehn, *A non-linear congruential pseudo random number generator*, Statist. Papers **27** (1986), 315–326.
3. J. Eichenauer, J. Lehn, and A. Topuzoğlu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51** (1988), 757–759.
4. G. Marsaglia, *Random numbers fall mainly in the planes*, Proc. Nat. Acad. Sci. U.S.A. **61** (1968), 25–28.
5. H. Niederreiter, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287.
6. ____, *Remarks on nonlinear congruential pseudorandom numbers*, Metrika **35** (1988), 321–328.
7. ____, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144.

FACHBEREICH MATHEMATIK, TECHNISCHE HOCHSCHULE, SCHLOSSGARTENSTRASSE 7, D-6100 DARMSTADT, FEDERAL REPUBLIC OF GERMANY