MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 201
JANUARY 1993, PAGES 375–384

STATISTICAL INDEPENDENCE OF A NEW CLASS OF INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS

JÜRGEN EICHENAUER-HERRMANN

ABSTRACT. Linear congruential pseudorandom numbers show several undesirable regularities which can render them useless for certain stochastic simulations. This was the motivation for important recent developments in nonlinear congruential methods for generating uniform pseudorandom numbers. It is particularly promising to achieve nonlinearity by employing the operation of multiplicative inversion with respect to a prime modulus. In the present paper a new class of such inversive congruential generators is introduced and analyzed. It is shown that they have excellent statistical independence properties and model true random numbers very closely. The methods of proof rely heavily on Weil-Stepanov bounds for rational exponential sums.

1. INTRODUCTION

The outcome of a stochastic simulation strongly depends on the quality of the pseudorandom numbers. General background material on pseudorandom number generation can be found in the book of Knuth [23] and the survey article of Niederreiter [28]. The classical standard method of generating uniform pseudorandom numbers in the interval $[0, 1)$ is the linear congruential method. Theoretical results on the structural and statistical properties of the generated sequences indicate that a reasonable behavior can be obtained if a judicious choice of parameters is made which depends on the dimension of the simulation problem (cf. [27–29]). Hence, a considerable computational effort has to be expended to guarantee acceptable properties, at least for a very modest range of dimensions (cf. [1, 19, 20]). However, linear congruential sequences show an unfavorable coarse lattice structure which stems from the simple nature of the underlying linear recursion and cannot be overcome even by the most judicious choice of parameters (cf. [25, 26, 37]).

This state of affairs provided the motivation for recent work on nonlinear congruential methods in order to overcome the deficiencies of the linear congruential method (cf. [2–9, 11–18, 30–33]). A review of the development of this area is given in [10] and in Niederreiter's excellent survey articles [34, 35]. The key idea behind these methods is the use of different nonlinear recursions in modular arithmetic instead of the simple linear recursion. Understandably, all these techniques are somewhat slower than the linear congruential method.

Received by the editor October 17, 1991.
1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 11K45.

0025-5718/93 $1.00 + $.25 per page

However, nowadays the computer time taken for pseudorandom number generation in a typical stochastic simulation can almost always be neglected (cf. [21, 36]).

The most promising results have been obtained for prime moduli. For a (large) prime p put $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ and $\mathbf{Z}_p^* = \mathbf{Z}_p \backslash \{0\}$. The following general class of nonlinear congruential generators was introduced in [2]: A *nonlinear congruential sequence* $(y_n)_{n \geq 0}$ of elements of $\mathbf{Z}_p$ is generated by

$$y_{n+1} = f(y_n), \qquad n \geq 0,$$

where $f: \mathbf{Z}_p \to \mathbf{Z}_p$ is a function such that $(y_n)_{n \geq 0}$ is purely periodic with maximal period length p. Niederreiter [30] pointed out that there exists a uniquely determined permutation polynomial g of degree s with $1 \leq s \leq p-2$ over the finite field $\mathbf{Z}_p$ such that

$$y_n = g(n), \qquad n \geq 0.$$

In Niederreiter [31] it is shown that any nonlinear congruential generator has excellent statistical independence properties for all dimensions $d \leq s$ provided the degree s of g is small relative to $p^{1/2}$.

In contrast, the present paper deals with certain polynomials g of maximal degree $s = p - 2$ and establishes favorable statistical independence properties for all dimensions $d < p$. In the following the abbreviation $\overline{z} \equiv z^{p-2} \pmod{p}$, $\overline{z} \in \mathbf{Z}_p$, is used for integers z. Note that $\overline{z}$ is the multiplicative inverse of z modulo p if $z \not\equiv 0 \pmod{p}$. A method for its efficient calculation is based on the Euclidean algorithm with the integers z and p (cf. [10]). The standard inversive congruential method, which was introduced in [4], generates a sequence $(y_n)_{n \geq 0}$ of elements of $\mathbf{Z}_p$ by the recursion $y_{n+1} \equiv a\overline{y}_n + b \pmod{p}$ for $n \geq 0$. In the present paper the following new class of inversive congruential generators is considered which has even better structural and statistical independence properties than the standard type. For integers $a, b \in \mathbf{Z}_p$ with $a \neq 0$ an *inversive congruential sequence* $(y_n)_{n \geq 0}$ of elements of $\mathbf{Z}_p$ is defined by

$$y_n = \overline{an + b}, \qquad n \geq 0.$$

A sequence $(x_n)_{n \geq 0}$ of *inversive congruential pseudorandom numbers* in the interval $[0, 1)$ is obtained by the normalization $x_n = y_n/p$ for $n \geq 0$. Obviously, any inversive congruential sequence is purely periodic with maximal period length p, i.e., $\{y_0, y_1, \ldots, y_{p-1}\} = \mathbf{Z}_p$, which guarantees that the one-dimensional distribution of the corresponding pseudorandom numbers is as good as possible. Hence, any inversive congruential generator passes the *uniformity test* for equidistribution in $[0, 1)$.

Statistical independence properties of pseudorandom numbers are at least as important for stochastic simulations as uniformity properties. A reliable theoretical test for statistical independence is the *serial test*, which employs the discrepancy of tuples of pseudorandom numbers. For a given dimension $k \geq 2$ and for N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^k$ the *discrepancy* is defined by

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^k$, $F_N(J)$ is N^{-1} times the number of terms among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$

denotes the volume of J. In the present paper, for a sequence of inversive congruential pseudorandom numbers $(x_n)_{n\geq 0}$, the points

$$\mathbf{x}_n = (x_{n+n_1}, x_{n+n_2}, \ldots, x_{n+n_k}) \in [0, 1)^k, \qquad 0 \leq n < p,$$

are considered, where $n_1, n_2, \ldots, n_k$ are arbitrary integers with $0 = n_1 < n_2 < \cdots < n_k < p$, and the abbreviation

$$D_p^{(k)} = D_p(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1})$$

is used for their discrepancy. An inversive congruential generator passes the k-dimensional serial test if $D_p^{(k)}$ is reasonably small. Since an exact calculation of the discrepancy $D_p^{(k)}$ is impossible, one is interested in bounds for $D_p^{(k)}$. In the present paper upper and lower bounds for $D_p^{(k)}$ are established, which are essentially best possible. In §2 the main results are stated precisely and the behavior of inversive congruential generators under the serial test is discussed. Section 3 contains several auxiliary results. The proof of the main results is given in §4. The methods of proof rely heavily on Weil-Stepanov bounds for rational exponential sums. Extensive background material on exponential sums can be found in [24].

2. Main results

Theorem 1. *Let $2 \leq k < p$. Then the discrepancy $D_p^{(k)}$ for any inversive congruential generator satisfies*

$$D_p^{(k)} < 2p^{-1/2}\left((k-1)\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^k + 1\right) + kp^{-1}.$$

Theorem 2. *Let $0 < t \leq 1$. Then there exist more than $A_p(t)(p-1)$ values of $a \in \mathbf{Z}_p^*$ such that the discrepancy $D_p^{(k)}$ for any corresponding inversive congruential generator satisfies*

$$D_p^{(k)} \geq \frac{t}{2(\pi+2)}p^{-1/2}$$

for all dimensions $k \geq 2$, where

$$A_p(t) = \frac{(1-t^2)p}{(4-t^2)p + 12p^{1/2} + 9}.$$

Theorem 1 shows that $D_p^{(k)} = O(p^{-1/2}(\log p)^k)$ for any inversive congruential generator, where the implied constant is absolute. It should be observed that this bound is independent not only of the specific choice of the parameters a, b in the inversive congruential method, but also of the parameters $n_2, \ldots, n_k$. This is a remarkable contrast to the linear congruential method, where the behavior under the serial test strongly depends on these quantities (and on the dimension k).

Theorem 2 implies that a positive proportion of the inversive congruential generators has a discrepancy $D_p^{(k)}$ which is at least of the order of magnitude $p^{-1/2}$ for all dimensions $k \geq 2$. Therefore the upper bound in Theorem 1 is in general best possible up to the logarithmic factor.

Theorems 1 and 2 show that in the inversive congruential method the discrepancy $D_p^{(k)}$ has on the average an order of magnitude between $p^{-1/2}$ and

$p^{-1/2}(\log p)^k$. It is in this range of magnitudes where one also finds the discrepancy of p independent and uniformly distributed random points from $[0, 1)^k$, which should be roughly $p^{-1/2}(\log\log p)^{1/2}$ according to the law of the iterated logarithm for discrepancies (cf. [22]). In this sense, inversive congruential pseudorandom numbers model true random numbers very closely.

3. Auxiliary results

First, some further notation is necessary. For integers $k \geq 1$ and $q \geq 2$ let $C_k(q)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbf{Z}^k$ with $-q/2 < h_j \leq q/2$ for $1 \leq j \leq k$. Put

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

and define

$$r(\mathbf{h}, q) = \prod_{j=1}^{k} r(h_j, q)$$

for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(q)$. For $t \in \mathbb{R}$ the abbreviation $e(t) = e^{2\pi i t}$ is used, for integers z we put $\chi(z) = e(z/p)$, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$.

Below, four known results are stated. The first two lemmas follow from Lemmas 2.2 and 2.3 in [27], the third lemma is a special case of a classical result of Weil [39] (cf. [32, 38]), and the last lemma is a special version of Lemma 1 in [33].

Lemma 1. *Let $N \geq 1$ and $q \geq 2$ be integers. Suppose that $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1} \in \mathbf{Z}_q^k$. Then the discrepancy of the points $\mathbf{t}_n = q^{-1}\mathbf{y}_n \in [0, 1)^k$ for $0 \leq n < N$ satisfies*

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

Lemma 2. *Let $q \geq 2$ be an integer. Then*

$$\sum_{h \in C_1(q)} \frac{1}{r(h, q)} < \frac{2}{\pi} \log q + \frac{2}{5}.$$

Lemma 3. *Let P, Q be polynomials over the finite field $\mathbf{Z}_p$ with $1 \leq \deg(Q) < \deg(P) < p$. Let r denote the number of distinct poles of $P\overline{Q}$ in the algebraic closure of $\mathbf{Z}_p$ (including the point at infinity) and let $m_1, \ldots, m_r$ be the multiplicities of the poles. Then*

$$\left| \sum_{\substack{z \in \mathbf{Z}_p \\ Q(z) \not\equiv 0 \pmod p}} \chi(P(z)\overline{Q(z)}) \right| \leq \left(r - 2 + \sum_{i=1}^{r} m_i \right) p^{1/2}.$$

Lemma 4. *The discrepancy of N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^k$ satisfies*

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) \geq \frac{1}{2(\pi+2)|h_1 h_2|N} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right|$$

for any lattice point $\mathbf{h} = (h_1, h_2, 0, \ldots, 0) \in \mathbf{Z}^k$ *with* $h_1 h_2 \neq 0$.

Lemmas 1 and 4 show that the exponential sums $S(\mathbf{h}) = \sum_{n \in \mathbf{Z}_p} e(\mathbf{h} \cdot \mathbf{x}_n)$ for $\mathbf{h} \in C_k(p)$ are the crucial quantities for the analysis of the discrepancy $D_p^{(k)}$. Put $J(\mathbf{h}) = \{1 \leq j \leq k | h_j \neq 0\}$ for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(p)$. The following technical result is used for the proof of Theorems 1 and 2.

Lemma 5. *Let* $\mathbf{h} \in C_k(p)$. *Then* $|S(\mathbf{h})| \leq m(2p^{1/2}+1) - (2p^{1/2}-1)$, *where* m *denotes the number of nonzero coordinates of* $\mathbf{h}$.

Proof. The definition of an inversive congruential sequence implies that

$$S(\mathbf{h}) = \sum_{n \in \mathbf{Z}_p} \chi \left(\sum_{j \in J(\mathbf{h})} h_j \overline{(a(n+n_j)+b)} \right)$$

for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(p)$. If $m = 1$, then

$$S(\mathbf{h}) = \sum_{z \in \mathbf{Z}_p} \chi(z) = 0,$$

which proves the desired inequality. From now on, $m \geq 2$ is assumed. Put

$$N(\mathbf{h}) = \{n \in \mathbf{Z}_p | a(n+n_j)+b \equiv 0 \pmod{p} \text{ for some } j \in J(\mathbf{h})\}.$$

Then one obtains

$$|S(\mathbf{h})| \leq m + \left| \sum_{\substack{n \in \mathbf{Z}_p \\ n \notin N(\mathbf{h})}} \chi \left(\sum_{j \in J(\mathbf{h})} h_j \overline{(a(n+n_j)+b)} \right) \right|$$

$$= m + \left| \sum_{\substack{n \in \mathbf{Z}_p \\ n \notin N(\mathbf{h})}} \chi \left(\left(\sum_{j \in J(\mathbf{h})} h_j \prod_{\substack{l \in J(\mathbf{h}) \\ l \neq j}} (a(n+n_l)+b) \right) \cdot \overline{\left(\prod_{j \in J(\mathbf{h})} (a(n+n_j)+b) \right)} \right) \right|.$$

Now, let $j_0 \in J(\mathbf{h})$ be fixed and put

$$Z(\mathbf{h}) = \{\overline{a(n_{j_0} - n_j)} \in \mathbf{Z}_p | j \in J(\mathbf{h})\}.$$

Then the transformation $z = \overline{a(n + n_{j_0}) + b}$ yields

$$|S(\mathbf{h})| \le m + \left| \sum_{\substack{z \in \mathbf{Z}_p \\ z \notin Z(\mathbf{h})}} \chi\left(\left(\sum_{j \in J(\mathbf{h})} h_j \prod_{\substack{l \in J(\mathbf{h}) \\ l \ne j}} (\overline{z} + a(n_l - n_{j_0})) \right) \cdot \overline{\left(\prod_{j \in J(\mathbf{h})} (\overline{z} + a(n_j - n_{j_0})) \right)} \right) \right|$$

$$= m + \left| \sum_{\substack{z \in \mathbf{Z}_p \\ z \notin Z(\mathbf{h})}} \chi\left(z \left(\sum_{j \in J(\mathbf{h})} h_j \prod_{\substack{l \in J(\mathbf{h}) \\ l \notin \{j, j_0\}}} (a(n_l - n_{j_0})z + 1) \right) \cdot \overline{\left(\prod_{\substack{j \in J(\mathbf{h}) \\ j \ne j_0}} (a(n_j - n_{j_0})z + 1) \right)} \right) \right|$$

$$\le m + 1 + \left| \sum_{\substack{z \in \mathbf{Z}_p \\ z \notin Z(\mathbf{h}) \setminus \{0\}}} \chi(P(z)\overline{Q(z)}) \right|$$

with the polynomials

$$P(z) = z \left(\sum_{j \in J(\mathbf{h})} h_j \prod_{\substack{l \in J(\mathbf{h}) \\ l \notin \{j, j_0\}}} (a(n_l - n_{j_0})z + 1) \right)$$

and

$$Q(z) = \prod_{\substack{j \in J(\mathbf{h}) \\ j \ne j_0}} (a(n_j - n_{j_0})z + 1)$$

for $z \in \mathbf{Z}_p$. Since $\deg(P) = m$ and $\deg(Q) = m - 1 \ge 1$, Lemma 3 can be applied with $r = \deg(Q) + 1 = m$ and $m_1 = \cdots = m_r = 1$, which implies that $|S(\mathbf{h})| \le m + 1 + (2m - 2)p^{1/2}$, i.e., the desired result. □

Finally, some further prerequisites are necessary in order to prove Theorem 2. First, a short calculation and the transformation $z \equiv n + \overline{a}b \pmod{p}$ show that $S(\mathbf{h}) = K_{n_2}(\overline{a})$ for $\mathbf{h} = (1, -1, 0, \ldots, 0) \in \mathbf{Z}^k$, where

$$K_\gamma(c) = \sum_{z \in \mathbf{Z}_p} \chi(c(\overline{z} - \overline{(z + \gamma)}))$$

for $c \in \mathbf{Z}_p^*$ and $\gamma \in \mathbf{Z}_p^*$. Hence, Lemma 5 implies that $|K_\gamma(c)| \le 2p^{1/2} + 3$ for $c \in \mathbf{Z}_p^*$ and $\gamma \in \mathbf{Z}_p^*$.

Lemma 6. *Let* $\gamma \in \mathbf{Z}_p^*$. *Then*

$$\sum_{c \in \mathbf{Z}_p^*} |K_\gamma(c)|^2 \ge p(p - 1).$$

Proof. Easy calculations show that

$$\begin{aligned}\sum_{c\in\mathbf{Z}_p^*}|K_\gamma(c)|^2 &= \sum_{c\in\mathbf{Z}_p^*}\sum_{y,z\in\mathbf{Z}_p}\chi(c(\bar{y}-\overline{(y+\gamma)}-\bar{z}+\overline{(z+\gamma)}))\\ &= \sum_{y,z\in\mathbf{Z}_p}\sum_{c\in\mathbf{Z}_p}\chi(c(\bar{y}-\overline{(y+\gamma)}-\bar{z}+\overline{(z+\gamma)}))-p^2\\ &= p|\{(y,z)\in\mathbf{Z}_p^2\mid \bar{y}-\overline{(y+\gamma)}\equiv\bar{z}-\overline{(z+\gamma)}\pmod p\}|-p^2\\ &\geq p|\{(y,z)\in\mathbf{Z}_p^2\mid y=z \text{ or } y\equiv -(z+\gamma)\pmod p\}|-p^2\\ &\geq p(2p-1)-p^2=p(p-1).\quad\square\end{aligned}$$

4. Proof of the main results

Proof of Theorem 1. First, Lemma 1 is applied with $N=q=p$ and $\mathbf{t}_n=\mathbf{x}_n$ for $0\leq n<p$. This yields

$$\begin{aligned}D_p^{(k)} &\leq \frac{k}{p}+\frac{1}{p}\sum_{\mathbf{h}\in C_k(p)}\frac{1}{r(\mathbf{h},p)}|S(\mathbf{h})|\\ &= \frac{k}{p}+\frac{1}{p}\sum_{m=1}^{k}\sum_{\substack{J\subset\{1,\dots,k\}\\|J|=m}}\sum_{\substack{\mathbf{h}\in C_k(p)\\J(\mathbf{h})=J}}\frac{1}{r(\mathbf{h},p)}|S(\mathbf{h})|.\end{aligned}$$

Now, Lemma 5 can be used in order to obtain

$$D_p^{(k)}\leq\frac{k}{p}+\frac{1}{p}\sum_{m=1}^{k}(m(2p^{1/2}+1)-(2p^{1/2}-1))\binom{k}{m}\left(\sum_{h\in C_1(p)}\frac{1}{r(h,p)}\right)^m.$$

Therefore, Lemma 2 implies that

$$\begin{aligned}D_p^{(k)} &< \frac{k}{p}+\frac{1}{p}\sum_{m=1}^{k}(m(2p^{1/2}+1)-(2p^{1/2}-1))\binom{k}{m}\left(\frac{2}{\pi}\log p+\frac{2}{5}\right)^m\\ &= \frac{k}{p}+\frac{1}{p}\left((2p^{1/2}+1)k\left(\frac{2}{\pi}\log p+\frac{2}{5}\right)\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\right.\\ &\qquad\left.-(2p^{1/2}-1)\left(\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^k-1\right)\right)\\ &= 2p^{-1/2}\left((k-1)\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^k+1\right)+(k-1)p^{-1}\\ &\quad -p^{-1}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(2kp^{1/2}-k\left(\frac{2}{\pi}\log p+\frac{2}{5}\right)-\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)\right)\\ &< 2p^{-1/2}\left((k-1)\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^k+1\right)+kp^{-1}\\ &\quad -2kp^{-1}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(p^{1/2}-\frac{2}{\pi}\log p-\frac{9}{10}\right),\end{aligned}$$

which yields the desired result, since $p^{1/2}-\frac{2}{\pi}\log p-\frac{9}{10}>0$. $\square$

Proof of Theorem 2. First, Lemma 4 is applied with $N = p$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \le n < p$, and $\mathbf{h} = (1, -1, 0, \ldots, 0) \in \mathbf{Z}^k$. This yields

$$D_p^{(k)} \ge \frac{1}{2(\pi + 2)p} |K_{n_2}(\bar{a})| .$$

Now, it is proved by contradiction that for every fixed $\gamma \in \mathbf{Z}_p^*$ and $0 < t \le 1$ there exist more than $A_p(t)(p-1)$ values of $c \in \mathbf{Z}_p^*$ such that $|K_\gamma(c)| \ge tp^{1/2}$, which completes the proof. Suppose that $|K_\gamma(c)| \ge tp^{1/2}$ for at most $A_p(t)(p-1)$ values of $c \in \mathbf{Z}_p^*$. Then $|K_\gamma(c)| < tp^{1/2}$ for at least $(1 - A_p(t))(p-1)$ values of $c \in \mathbf{Z}_p^*$. Since $|K_\gamma(c)| \le 2p^{1/2} + 3$ for all $c \in \mathbf{Z}_p^*$, it follows that

$$\sum_{c \in \mathbf{Z}_p^*} |K_\gamma(c)|^2 < (1 - A_p(t))(p-1)t^2 p + A_p(t)(p-1)(2p^{1/2} + 3)^2 = p(p-1) ,$$

which is a contradiction to Lemma 6. □

Acknowledgment

The author would like to thank the referee for valuable suggestions.

Bibliography

1. I. Borosh and H. Niederreiter, *Optimal multipliers for pseudo-random number generation by the linear congruential method*, BIT **23** (1983), 65–74.
2. J. Eichenauer, H. Grothe, and J. Lehn, *Marsaglia's lattice test and non-linear congruential pseudo random number generators*, Metrika **35** (1988), 241–250.
3. J. Eichenauer, H. Grothe, J. Lehn, and A. Topuzoğlu, *A multiple recursive non-linear congruential pseudo random number generator*, Manuscripta Math. **59** (1987), 331–346.
4. J. Eichenauer and J. Lehn, *A non-linear congruential pseudorandom number generator*, Statist. Papers **27** (1986), 315–326.
5. ____, *On the structure of quadratic congruential sequences*, Manuscripta Math. **58** (1987), 129–140.
6. J. Eichenauer, J. Lehn, and A. Topuzoğlu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51** (1988), 757–759.
7. J. Eichenauer and H. Niederreiter, *On Marsaglia's lattice test for pseudorandom numbers*, Manuscripta Math. **62** (1988), 245–248.
8. J. Eichenauer-Herrmann, *A remark on the discrepancy of quadratic congruential pseudorandom numbers*, J. Comput. Appl. Math. (to appear)
9. ____, *Construction of inversive congruential pseudorandom number generators with maximal period length*, J. Comput. Appl. Math. **40** (1992), 345–349.
10. ____, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
11. ____, *Inversive congruential pseudorandom numbers avoid the planes*, Math. Comp. **56** (1991), 297–301.
12. ____, *On the autocorrelation structure of inversive congruential pseudorandom number sequences*, Statist. Papers (to appear)

13. ____, *On the discrepancy of inversive congruential pseudorandom numbers with prime power modulus*, Manuscripta Math. **71** (1991), 153–161.

14. J. Eichenauer-Herrmann and H. Grothe, *A new inversive congruential pseudorandom number generator with power of two modulus*, ACM Trans. Modeling Computer Simulation (to appear)

15. J. Eichenauer-Herrmann, H. Grothe, H. Niederreiter, and A. Topuzoğlu, *On the lattice structure of a nonlinear generator with modulus* 2^{α}, J. Comput. Appl. Math. **31** (1990), 81–85.

16. 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.

17. ____, *On the discrepancy of quadratic congruential pseudorandom numbers*, J. Comput. Appl. Math. **34** (1991), 243–249.

18. J. Eichenauer-Herrmann and A. Topuzoğlu, *On the period length of congruential pseudorandom number sequences generated by inversions*, J. Comput. Appl. Math. **31** (1990), 87–96.

19. G. S. Fishman, *Multiplicative congruential random number generators with modulus* 2^{β} : *An exhaustive analysis for* $\beta = 32$ *and a partial analysis for* $\beta = 48$, Math. Comp. **54** (1990), 331–344.

20. G. S. Fishman and L. R. Moore, *An exhaustive analysis of multiplicative congruential random number generators with modulus* $2^{31} - 1$, SIAM J. Sci. Statist. Comput. **7** (1986), 24–45; Erratum, *ibid.*, p. 1058.

21. F. James, *A review of pseudorandom number generators*, Comput. Phys. Comm. **60** (1990), 329–344.

22. J. Kiefer, *On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm*, Pacific J. Math. **11** (1961), 649–660.

23. D. E. Knuth, *The art of computer programming*, vol. 2, 2nd ed., Addison-Wesley, Reading, MA, 1981.

24. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.

25. G. Marsaglia, *Random numbers fall mainly in the planes*, Proc. Nat. Acad. Sci. U.S.A. **61** (1968), 25–28.

26. ____, *Regularities in congruential random number generators*, Numer. Math. **16** (1970), 8–10.

27. H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Adv. in Math. **26** (1977), 99–181.

28. ____, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.

29. ____, *The serial test for pseudo-random numbers generated by the linear congruential method*, Numer. Math. **46** (1985), 51–68.

30. ____, *Remarks on nonlinear congruential pseudorandom numbers*, Metrika **35** (1988), 321–328.

31. ____, *Statistical independence of nonlinear congruential pseudorandom numbers*, Monatsh. Math. **106** (1988), 149–159.

32. ____, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144.

33. ____, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287.

34. ____, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–346.

35. ____, *Nonlinear methods for pseudorandom number and vector generation*, Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Economics and Math. Systems, vol. 374, Springer, Berlin, 1992, pp. 145–153.

36. B. D. Ripley, *Computer generation of random variables: a tutorial*, Internat. Statist. Rev. **51** (1983), 301–319.

37. ____, *The lattice structure of pseudo-random number generators*, Proc. Roy. Soc. London Ser. A **389** (1983), 197–204.

38. S. A. Stepanov, *On estimating rational trigonometric sums with prime denominator*, Trudy Mat. Inst. Steklov. **112** (1971), 346–371. (Russian)

39. A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.

FACHBEREICH MATHEMATIK, TECHNISCHE HOCHSCHULE DARMSTADT, SCHLOSSGARTENSTRASSE 7, D–6100 DARMSTADT, GERMANY