ON GENERALIZED INVERSIve CONGRUENTIAL PSEUDORandom NUMBERS

JÜRGEN EICHENAUER-HERRMANN

Abstract. The inversive congruential method with prime modulus for generating uniform pseudorandom numbers has several very promising properties. Very recently, a generalization for composite moduli has been introduced. In the present paper it is shown that the generated sequences have very attractive statistical independence properties.

1. Introduction and main results

Several nonlinear congruential methods of generating uniform pseudorandom numbers in the interval \([0,1)\) have been studied during the last few years. A review of the developments in this area is given in the survey articles \([3, 13, 14, 16, 17]\) and in H. Niederreiter's excellent monograph \([15]\). A particularly attractive approach is the inversive congruential method with prime modulus, which has been analyzed in \([1, 2, 4-6, 11, 12, 17]\). Recently, a generalization for arbitrary composite moduli has been introduced in \([8]\). The present paper restricts itself to the case of a modulus \(m = p_1 \cdot p_2 \cdots p_r\) with arbitrary distinct primes \(p_1, p_2, \ldots, p_r \geq 5\). Let \(\mathbb{Z}_m = \{0, 1, \ldots, m-1\}\). For integers \(a, b \in \mathbb{Z}_m\) with \(\gcd(a, m) = 1\) a generalized inversive congruential sequence \((y_n)_{n \geq 0}\) of elements of \(\mathbb{Z}_m\) is defined by

\[
y_{n+1} = ay_n^{\varphi(m)-1} + b \pmod{m}, \quad n \geq 0,
\]

where \(\varphi(m) = (p_1 - 1) \cdots (p_r - 1)\) denotes the number of positive integers less than \(m\) which are relatively prime to \(m\). A sequence \((x_n)_{n \geq 0}\) of generalized inversive congruential pseudorandom numbers in the interval \([0,1)\) is obtained by \(x_n = y_n / m\) for \(n \geq 0\). The result below shows that these sequences are closely related to the following inversive congruential sequences with prime moduli. For \(1 \leq i \leq r\) let \(\mathbb{Z}_{p_i} = \{0, 1, \ldots, p_i - 1\}\), \(m_i = m / p_i\), and \(a_i, b_i \in \mathbb{Z}_{p_i}\) be integers with

\[
a \equiv m_i^2 a_i \pmod{p_i} \quad \text{and} \quad b \equiv m_i b_i \pmod{p_i}.
\]

Let \((y_n^{(i)})_{n \geq 0}\) be a sequence of elements of \(\mathbb{Z}_{p_i}\) given by

\[
y^{(i)}_{n+1} = a_i(y^{(i)}_n)^{p_i-2} + b_i \pmod{p_i}, \quad n \geq 0,
\]

Received by the editor May 24, 1993 and, in revised form, August 20, 1993. 
1991 Mathematics Subject Classification. Primary 65C10; Secondary 11K45.

Key words and phrases. Uniform pseudorandom numbers, inversive congruential method, composite modulus, statistical independence, discrepancy.

©1994 American Mathematical Society 0025-5718/94 $1.00 + $.25 per page 293
where \( y_0 \equiv m_i y_0^{(i)} \pmod{p_i} \) is assumed. Note that \( z^{p_i - 2} \equiv z^{-1} \pmod{p_i} \) for any integer \( z \in \mathbb{Z}_{p_i} \setminus \{0\} \) according to Fermat's Theorem; i.e., \( (y_n^{(i)})_{n \geq 0} \) is an (ordinary) inversive congruential sequence in the sense of [1]. As usual, a sequence \( (x_n^{(i)})_{n \geq 0} \) of (ordinary) inversive congruential pseudorandom numbers in the interval \([0, 1)\) is defined by \( x_n^{(i)} = y_n^{(i)}/p_i \) for \( n \geq 0 \).

**Theorem 1.** Let \( (y_n^{(i)})_{n \geq 0} \) and \( (x_n^{(i)})_{n \geq 0} \) for \( 1 \leq i \leq r \) be defined as above. Then

\[
y_n \equiv m_1 y_n^{(1)} + \cdots + m_r y_n^{(r)} \pmod{m}
\]

and

\[
x_n \equiv x_n^{(1)} + \cdots + x_n^{(r)} \pmod{1}
\]

for \( n \geq 0 \).

The proof of Theorem 1 is given in the third section. Theorem 1 shows that an implementation of generalized inversive congruential generators is possible, where exact integer computations have to be performed only in \( \mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r} \), but not in \( \mathbb{Z}_m \). From now on it is always assumed that the generalized inversive congruential sequence \( (y_n)_{n \geq 0} \) is purely periodic with maximal period length \( m \); i.e., \( \{y_0, y_1, \ldots, y_{m-1}\} = \mathbb{Z}_m \). Theorem 1 implies that \( (y_n^{(i)})_{n \geq 0} \) shares this property if and only if \( (y_n^{(i)})_{n \geq 0} \) is purely periodic with period length \( p_i \) for \( 1 \leq i \leq r \). A characterization of these (ordinary) inversive congruential generators is given in [6], whereas a handy sufficient condition demands for \( z^2 - b_i z - a_i \) (or equivalently, \( y^2 - by - a \)) to be a primitive polynomial modulo \( p_i \) for \( 1 \leq i \leq r \) (cf. [1, 11]).

Obviously, generalized inversive congruential pseudorandom numbers are well equidistributed in one dimension. A reliable theoretical approach for assessing their statistical independence properties is based on the discrepancy of \( s \)-tuples of pseudorandom numbers. For \( N \) arbitrary points \( t_0, t_1, \ldots, t_{N-1} \in [0, 1)^s \) the discrepancy is defined by

\[
D_N(t_0, t_1, \ldots, t_{N-1}) = \sup_J |F_N(J) - V(J)|,
\]

where the supremum is extended over all subintervals \( J \) of \([0, 1)^s\), \( F_N(J) \) is \( N^{-1} \) times the number of points among \( t_0, t_1, \ldots, t_{N-1} \) falling into \( J \), and \( V(J) \) denotes the \( s \)-dimensional volume of \( J \). For \( s \geq 2 \) consider the \( s \)-tuples

\[
x_n := (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0, 1)^s, \quad n \geq 0,
\]

of generalized inversive congruential pseudorandom numbers. In the following, the abbreviation \( D_m^{(s)} := D_m(x_0, x_1, \ldots, x_{m-1}) \) is used. In the results of the next theorems upper and lower bounds for the discrepancy \( D_m^{(s)} \) are established. Their proof is given in the third section.

**Theorem 2.** Let \( s \geq 2 \). Then the discrepancy \( D_m^{(s)} \) satisfies

\[
D_m^{(s)} < m^{-1/2} \left( \frac{2}{\pi} \log m \right)^s \prod_{i=1}^{r} (2s - 2 + sp_i^{-1/2}) + sm^{-1}
\]

for any generalized inversive congruential operator.
Theorem 3. There exist generalized inversive congruential generators with

\[ D_m^{(s)} \geq \frac{1}{2(\pi + 2)} m^{-1/2} \prod_{i=1}^{r} \left( \frac{p_i - 3}{p_i - 1} \right)^{1/2} \]

for all dimensions \( s \geq 2 \).

For a fixed number \( r \) of prime factors of \( m \), Theorem 2 shows that \( D_m^{(s)} = O(m^{-1/2}(\log m)^{s}) \) for any generalized inversive congruential sequence. In this case, Theorem 3 implies that there exist generalized inversive congruential generators having a discrepancy \( D_m^{(s)} \) which is at least of the order of magnitude \( m^{-1/2} \) for all dimensions \( s \geq 2 \). However, if \( m \) is composed only of small primes, then \( r \) can be of an order of magnitude \((\log m)/\log\log m\) and hence \( \prod_{i=1}^{r} (2s - 2 + sp_i^{-1/2}) = O(m^{\varepsilon}) \) for every \( \varepsilon > 0 \) (cf. [7]). Therefore, one obtains in the general case \( D_m^{(s)} = O(m^{-1/2+\varepsilon}) \) for every \( \varepsilon > 0 \). Since \( \prod_{i=1}^{r} ((p_i - 3)/(p_i - 1))^{1/2} \geq 2^{-r/2} \), similar arguments imply that in the general case the lower bound in Theorem 3 is at least of the order of magnitude \( m^{-1/2-\varepsilon} \) for every \( \varepsilon > 0 \). It is in this range of magnitudes where one also finds the discrepancy of \( m \) independent and uniformly distributed random points from \([0, 1]^s\), which almost always has the order of magnitude \( m^{-1/2}(\log\log m)^{1/2} \) according to the law of the iterated logarithm for discrepancies (cf. [9]). In this sense, generalized inversive congruential pseudorandom numbers model true random numbers very closely.

2. 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 \((h_1, \ldots, h_k) \in \mathbb{Z}^k\) with \(-q/2 < h_j < q/2\) for \( 1 \leq j \leq k \). Define

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

and

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

for \( h = (h_1, \ldots, h_k) \in C_k(q) \). For real \( t \) the abbreviation \( e(t) = e^{2\pi it} \) is used, and \( u \cdot v \) stands for the standard inner product of \( u, v \in \mathbb{R}^k \).

In the following, three known general results for estimating discrepancies are stated. The first lemma follows from [15, Theorem 3.10], the second one is a special version of [15, Corollary 3.17], and the third lemma is from [10, Lemma 2.3].

Lemma 1. Let \( N \geq 1 \) and \( q \geq 2 \) be integers, and let \( t_n = q^{-1}y_n \in [0, 1)^k \) with \( y_n \in \{0, 1, \ldots, q-1\}^k \) for \( 0 \leq n < N \). Then the discrepancy of the points \( t_0, t_1, \ldots, t_{N-1} \) satisfies

\[ D_N(t_0, t_1, \ldots, t_{N-1}) \leq \frac{k}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_k(q)} \frac{1}{r(\mathbf{h}, q)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right|. \]
Lemma 2. The discrepancy of $N$ arbitrary points $t_0, t_1, \ldots, t_{N-1} \in [0, 1)^k$ satisfies
\[
D_N(t_0, t_1, \ldots, t_{N-1}) \geq \frac{1}{2(\pi + 2)|h_1 h_2|N} \left| \sum_{n=0}^{N-1} e(h \cdot t_n) \right|
\]
for any lattice point $h = (h_1, h_2, 0, \ldots, 0) \in \mathbb{Z}^k$ with $h_1 h_2 \neq 0$.

Lemma 3. Let $q \geq 2$ be an integer. Then
\[
\sum_{h \in C_1(q)} \frac{1}{r(h, q)} < \frac{2}{\pi} \log q + \frac{2}{5}.
\]

Lemmata 1 and 2 indicate that a crucial role for the analysis of the discrepancy $D_m^{(q)}$ is played by the exponential sums
\[
S(h) := \sum_{n=0}^{m-1} e(h \cdot x_n)
\]
for $h \in \mathbb{Z}^s$. The next lemma shows that these sums are closely related to the exponential sums
\[
S_i(h) := \sum_{k \in \mathbb{Z}_{p_i}} e(h \cdot x_k^{(i)})
\]
for $h \in \mathbb{Z}^s$, where $x_k^{(i)} := (x_{ki}, x_{ki+1}, \ldots, x_{ki+s-1}) \in [0, 1)^s$ for $k \geq 0$ and $1 \leq i \leq r$.

Lemma 4. Let $h \in \mathbb{Z}^s$. Then
\[
S(h) = \prod_{i=1}^{r} S_i(h).
\]

Proof. First, it follows from
\[
x_n \equiv \sum_{i=1}^{r} x_n^{(i)} \pmod{1}, \quad n \geq 0,
\]
that
\[
S(h) = \sum_{n=0}^{m-1} e \left( \sum_{i=1}^{r} h \cdot x_n^{(i)} \right) = \prod_{n=0}^{m-1} \prod_{i=1}^{r} e(h \cdot x_n^{(i)}).
\]

Now, the Chinese Remainder Theorem implies that
\[
S(h) = \sum_{(k_1, \ldots, k_r) \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}} \prod_{i=1}^{r} e(h \cdot x_{k_i}^{(i)}).
\]

Since the sequence $(x_n^{(i)})_{n \geq 0}$ has period length $p_i$ for $1 \leq i \leq r$, one finally obtains
\[
S(h) = \sum_{(k_1, \ldots, k_r) \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}} \prod_{i=1}^{r} e(h \cdot x_{k_i}^{(i)})
\]
\[
= \prod_{i=1}^{r} \sum_{k \in \mathbb{Z}_{p_i}} e(h \cdot x_k^{(i)}) = \prod_{i=1}^{r} S_i(h). \quad \Box
Observe that $S_i(h) = p_i$ for all $h \in \mathbb{Z}^s$ with $h \equiv 0 \pmod{p_i}$. The upper bound for $|S_i(h)|$ with $h \not\equiv 0 \pmod{p_i}$ given in the next lemma follows from [11, proof of Theorem 1].

**Lemma 5.** Let $1 \leq i \leq r$ and $h \in \mathbb{Z}^s$ with $h \not\equiv 0 \pmod{p_i}$. Then

$$|S_i(h)| \leq (2s-2)p_i^{1/2} + s - 1.$$

### 3. Proof of the main results

**Proof of Theorem 1.** First, observe that $m_i \equiv 0 \pmod{p_i}$ for $i \neq j$, and hence $y_n \equiv m_1y_1^{(i)} + \cdots + m_r y_r^{(i)} \pmod{m}$ if and only if $y_n \equiv m_i y_i^{(i)} \pmod{p_i}$ for $1 \leq i \leq r$, which will be shown by induction on $n \geq 0$. Recall that $y_0 \equiv m_i y_i^{(i)} \pmod{p_i}$ is assumed for $1 \leq i \leq r$. Now, suppose that $1 \leq i \leq r$ and $y_n \equiv m_i y_i^{(i)} \pmod{p_i}$ for some integer $n \geq 0$. Then straightforward calculations and Fermat's Theorem yield

$$y_{n+1} \equiv ay_n^{p(i)-1} + b \equiv m_i(a_i m_i^{(i)} y_i^{(i)} y_n^{(i)})^{p(i)-1} + b_i)$$

$$\equiv m_i (a_i y_i^{(i)} + b_i) \equiv m_i y_{n+1} \pmod{p_i},$$

which implies the desired result. $\square$

**Proof of Theorem 2.** First, Lemma 1 is applied with $N = q = m$, $k = s$, and $t_n = x_n$ for $0 \leq n < m$. This yields

$$D_m^{(s)} \leq \frac{s}{m} + \frac{1}{m} \sum_{h \in C_z(m)} \frac{1}{r(h, m)}|S(h)|$$

$$= \frac{s}{m} + \frac{1}{m} \sum_{h \in C_z(m)} \frac{1}{r(h, m)} \prod_{i=1}^r |S_i(h)|$$

$$= \frac{s}{m} + \frac{1}{m} \sum_{I \subseteq \{1, \ldots, r\}} \sum_{|I| < r} \sum_{h \equiv 0 \pmod{p_i}, i \in I} \sum_{h \not\equiv 0 \pmod{p_i}, i \notin I} \frac{1}{r(h, m)} \prod_{i=1}^r |S_i(h)|,$$

where in the second step Lemma 4 has been used. Now, Lemma 5 can be applied to obtain

$$D_m^{(s)} \leq \frac{s}{m} + \frac{1}{m} \sum_{I \subseteq \{1, \ldots, r\}} \sum_{|I| < r} m! \prod_{i \in I} ((2s-2)p_i^{1/2} + s - 1) \sum_{h \in C_z(m)} \frac{1}{r(h, m)}$$

$$\leq \frac{s}{m} + \frac{1}{m} \sum_{I \subseteq \{1, \ldots, r\}} \sum_{|I| < r} m! \prod_{i \in I} ((2s-2)p_i^{1/2} + s - 1) \sum_{h \in C_z(m)} \frac{1}{r(h, m)},$$

where $m! := \prod_{i \in I} p_i$ for subsets $I$ of $\{1, \ldots, r\}$. Straightforward calculations
show that

\[
\sum_{h \in C_t(m) \atop h \equiv 0 \pmod{m'}} \frac{1}{r(h, m)} = \left( \sum_{h \in C_t(m) \atop h \equiv 0 \pmod{m'}} \frac{1}{r(h, m)} + 1 \right)^s - 1
\]

\[
= \left( \frac{1}{m'} \sum_{k \in C_t(m/m')} \frac{1}{r(k, m/m') + 1} \right)^s - 1,
\]

and hence Lemma 3 implies that

\[
\sum_{h \in C_t(m) \atop h \equiv 0 \pmod{m'}} \frac{1}{r(h, m)} \leq \left( \frac{1}{m'} \left( \frac{2 \pi \log(m/m') + \frac{2}{5}} + 1 \right)^s - 1
\]

\[
\leq \left( \frac{1}{m'} \left( \frac{2 \pi \log m + \frac{2}{5}} + 1 \right)^s - 1
\]

\[
\leq \frac{1}{m'} \left( \frac{2 \pi \log m + \frac{7}{5}} \right)^s.
\]

 Altogether, one obtains

\[
D_m^{(s)} < \frac{s}{m} + \frac{1}{m} \left( \frac{2 \pi \log m + \frac{7}{5}} \right)^s \sum_{l \in \{1, \ldots, r} \prod_{i \notin l} ((2s - 2)p_{i}^{1/2} + s - 1)
\]

\[
= \frac{s}{m} + \frac{1}{m} \left( \frac{2 \pi \log m + \frac{7}{5}} \right)^s \prod_{i=1}^{r} ((2s - 2)p_{i}^{1/2} + s),
\]

which yields the desired result. \( \square \)

**Proof of Theorem 3.** First, Lemma 2 is applied with \( N = m, \ k = s, \ t_n = x_n \) for \( 0 \leq n < m \), and \( h = (1, 1, 0, \ldots, 0) \in \mathbb{Z}^s \). This and Lemma 4 yield

\[
D_m^{(s)} \geq \frac{1}{2(\pi + 2)m} |S(h)| = \frac{1}{2(\pi + 2)m} \prod_{i=1}^{r} |S_i(h)|.
\]

Now, it follows from \([2, \text{Lemma 2}]\) that there exist inversive congruential generators with

\[
|S_i(h)| \geq \left( \frac{p_i - 3}{p_i - 1} \right)^{1/2} p_i^{1/2}
\]

for \( 1 \leq i \leq r \). Hence, according to the Chinese Remainder Theorem there exist generalized inversive congruential generators with

\[
D_m^{(s)} \geq \frac{1}{2(\pi + 2)m} \prod_{i=1}^{r} \left( \frac{p_i - 3}{p_i - 1} \right)^{1/2} p_i^{1/2}
\]

\[
= \frac{1}{2(\pi + 2)m^{-1/2}} \prod_{i=1}^{r} \left( \frac{p_i - 3}{p_i - 1} \right)^{1/2}. \quad \square
\]
ACKNOWLEDGMENTS

The author is very grateful to Professor H. Niederreiter for pointing out some errors in the interpretation of Theorems 2 and 3 which led to the present improved version. He would also like to thank Dr. K. Huber for valuable comments.

BIBLIOGRAPHY


Fachbereich Mathematik, Technische Hochschule Darmstadt, Schloßgartenstrasse 7, D-64289 Darmstadt, Germany