MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 207
JULY 1994, PAGES 293–299

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 $p_1, p_2, \dots, p_r \geq 5$. Let $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$. 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

$$y_{n+1} \equiv a y_n^{\varphi(m)-1} + b \pmod{m}, \qquad n \geq 0,$$

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 $\mathbb{Z}_{p_i} = \{0, 1, \dots, p_i - 1\}$, $m_i = m/p_i$, 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

$$y_{n+1}^{(i)} \equiv a_i (y_n^{(i)})^{p_i-2} + b_i \pmod{p_i}, \qquad n \geq 0,$$

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.

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 $z \in \mathbb{Z}_{p_i}\backslash\{0\}$ 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 $(y_n)_{n\geq 0}$ 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 $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^s$ 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 $[0, 1)^s$, $F_N(J)$ is N^{-1} times the number of points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the s-dimensional volume of J. For $s \geq 2$ consider the s-tuples

$$\mathbf{x}_n := (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0, 1)^s, \qquad n \geq 0,$$

of generalized inversive congruential pseudorandom numbers. In the following, the abbreviation $D_m^{(s)} := D_m(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{m-1})$ 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*

$$D_m^{(s)} < m^{-1/2}\left(\frac{2}{\pi}\log m + \frac{7}{5}\right)^s \prod_{i=1}^{r}(2s - 2 + s p_i^{-1/2}) + s m^{-1}$$

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

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

and

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

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

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* $\mathbf{t}_n = q^{-1}\mathbf{y}_n \in [0, 1)^k$ *with* $\mathbf{y}_n \in \{0, 1, \dots, q-1\}^k$ *for* $0 \leq n < N$. *Then the discrepancy of the points* $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ *satisfies*

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

Lemma 2. *The discrepancy of N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1} \in [0, 1)^k$ satisfies*

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

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

Lemma 3. *Let $q \geq 2$ be an integer. Then*

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

Lemmas 1 and 2 indicate that a crucial role for the analysis of the discrepancy $D_m^{(s)}$ is played by the exponential sums

$$S(\mathbf{h}) := \sum_{n=0}^{m-1} e(\mathbf{h} \cdot \mathbf{x}_n)$$

for $\mathbf{h} \in \mathbb{Z}^s$. The next lemma shows that these sums are closely related to the exponential sums

$$S_i(\mathbf{h}) := \sum_{k \in \mathbb{Z}_{p_i}} e(\mathbf{h} \cdot \mathbf{x}_k^{(i)})$$

for $\mathbf{h} \in \mathbb{Z}^s$, where $\mathbf{x}_k^{(i)} := (x_k^{(i)}, x_{k+1}^{(i)}, \dots, x_{k+s-1}^{(i)}) \in [0, 1)^s$ for $k \geq 0$ and $1 \leq i \leq r$.

Lemma 4. *Let $\mathbf{h} \in \mathbb{Z}^s$. Then*

$$S(\mathbf{h}) = \prod_{i=1}^{r} S_i(\mathbf{h}).$$

Proof. First, it follows from

$$\mathbf{x}_n \equiv \sum_{i=1}^{r} \mathbf{x}_n^{(i)} \pmod 1, \qquad n \geq 0,$$

that

$$S(\mathbf{h}) = \sum_{n=0}^{m-1} e\left(\sum_{i=1}^{r} \mathbf{h} \cdot \mathbf{x}_n^{(i)} \right) = \sum_{n=0}^{m-1} \prod_{i=1}^{r} e(\mathbf{h} \cdot \mathbf{x}_n^{(i)}).$$

Now, the Chinese Remainder Theorem implies that

$$S(\mathbf{h}) = \sum_{\substack{(k_1, \dots, k_r) \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r} \\ n \equiv k_i \pmod{p_i},\, 1 \leq i \leq r}} \prod_{i=1}^{r} e(\mathbf{h} \cdot \mathbf{x}_n^{(i)}).$$

Since the sequence $(\mathbf{x}_n^{(i)})_{n \geq 0}$ has period length p_i for $1 \leq i \leq r$, one finally obtains

$$\begin{aligned} S(\mathbf{h}) &= \sum_{(k_1, \dots, k_r) \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}} \prod_{i=1}^{r} e(\mathbf{h} \cdot \mathbf{x}_{k_i}^{(i)}) \\ &= \prod_{i=1}^{r} \sum_{k \in \mathbb{Z}_{p_i}} e(\mathbf{h} \cdot \mathbf{x}_k^{(i)}) = \prod_{i=1}^{r} S_i(\mathbf{h}). \quad \square \end{aligned}$$

Observe that $S_i(\mathbf{h}) = p_i$ for all $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \equiv \mathbf{0} \pmod{p_i}$. The upper bound for $|S_i(\mathbf{h})|$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ given in the next lemma follows from [11, proof of Theorem 1].

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

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

3. Proof of the main results

Proof of Theorem 1. First, observe that $m_i \equiv 0 \pmod{p_j}$ for $i \ne j$, and hence $y_n \equiv m_1 y_n^{(1)} + \cdots + m_r y_n^{(r)} \pmod{m}$ if and only if $y_n \equiv m_i y_n^{(i)} \pmod{p_i}$ for $1 \le i \le r$, which will be shown by induction on $n \ge 0$. Recall that $y_0 \equiv m_i y_0^{(i)} \pmod{p_i}$ is assumed for $1 \le i \le r$. Now, suppose that $1 \le i \le r$ and $y_n \equiv m_i y_n^{(i)} \pmod{p_i}$ for some integer $n \ge 0$. Then straightforward calculations and Fermat's Theorem yield

$$\begin{aligned} y_{n+1} &\equiv a y_n^{\varphi(m)-1} + b \equiv m_i(a_i m_i^{\varphi(m)} (y_n^{(i)})^{\varphi(m)-1} + b_i) \\ &\equiv m_i(a_i (y_n^{(i)})^{p_i-2} + b_i) \equiv m_i y_{n+1}^{(i)} \pmod{p_i}, \end{aligned}$$

which implies the desired result. □

Proof of Theorem 2. First, Lemma 1 is applied with $N = q = m$, $k = s$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \le n < m$. This yields

$$\begin{aligned} D_m^{(s)} &\le \frac{s}{m} + \frac{1}{m} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} |S(\mathbf{h})| \\ &= \frac{s}{m} + \frac{1}{m} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \prod_{i=1}^{r} |S_i(\mathbf{h})| \\ &= \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1, \dots, r\} \\ |I| < r}} \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i},\ i \in I \\ \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i},\ i \notin I}} \frac{1}{r(\mathbf{h}, m)} \prod_{i=1}^{r} |S_i(\mathbf{h})|, \end{aligned}$$

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

$$\begin{aligned} D_m^{(s)} &\le \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1, \dots, r\} \\ |I| < r}} m^I \prod_{i \notin I} ((2s-2)p_i^{1/2} + s - 1) \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i},\ i \in I \\ \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i},\ i \notin I}} \frac{1}{r(\mathbf{h}, m)} \\ &\le \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1, \dots, r\} \\ |I| < r}} m^I \prod_{i \notin I} ((2s-2)p_i^{1/2} + s - 1) \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{m^I}}} \frac{1}{r(\mathbf{h}, m)}, \end{aligned}$$

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

$$\sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}\ (\mathrm{mod}\, m^I)}} \frac{1}{r(\mathbf{h}, m)} = \left(\sum_{\substack{h\in C_1(m)\\ h\equiv 0\ (\mathrm{mod}\, m^I)}} \frac{1}{r(h, m)} + 1 \right)^s - 1$$
$$= \left(\frac{1}{m^I} \sum_{k\in C_1(m/m^I)} \frac{1}{r(k, m/m^I)} + 1 \right)^s - 1,$$

and hence Lemma 3 implies that

$$\sum_{\substack{\mathbf{h}\in C_s(m)\\ \mathbf{h}\equiv\mathbf{0}\ (\mathrm{mod}\, m^I)}} \frac{1}{r(\mathbf{h}, m)} < \left(\frac{1}{m^I} \left(\frac{2}{\pi} \log(m/m^I) + \frac{2}{5} \right) + 1 \right)^s - 1$$
$$\leq \left(\frac{1}{m^I} \left(\frac{2}{\pi} \log m + \frac{2}{5} \right) + 1 \right)^s - 1$$
$$\leq \frac{1}{m^I} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s .$$

Altogether, one obtains

$$D_m^{(s)} < \frac{s}{m} + \frac{1}{m} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s \sum_{I\subset\{1,\dots,r\}} \prod_{i\notin I} ((2s-2)p_i^{1/2} + s - 1)$$
$$= \frac{s}{m} + \frac{1}{m} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s \prod_{i=1}^{r} ((2s-2)p_i^{1/2} + s),$$

which yields the desired result. □

Proof of Theorem 3. First, Lemma 2 is applied with $N = m$, $k = s$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < m$, and $\mathbf{h} = (1, 1, 0, \dots, 0) \in \mathbb{Z}^s$. This and Lemma 4 yield

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

Now, it follows from [2, Lemma 2] that there exist inversive congruential generators with

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

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

1. J. Eichenauer and J. Lehn, *A non-linear congruential pseudo random number generator*, Statist. Papers **27** (1986), 315–326.
2. J. Eichenauer-Herrmann, *Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **62** (1994), 783–786.
3. ——, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
4. ——, *Inversive congruential pseudorandom numbers avoid the planes*, Math. Comp. **56** (1991), 297–301.
5. ——, *Statistical independence of a new class of inversive congruential pseudorandom numbers*, Math. Comp. **60** (1993), 375–384.
6. M. Flahive and H. Niederreiter, *On inversive congruential generators for pseudorandom numbers*, Finite Fields, Coding Theory, and Advances in Communications and Computing (G. L. Mullen and P. J.-S. Shiue, eds.), Dekker, New York, 1992, pp. 75–80.
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Clarendon Press, Oxford, 1979.
8. K. Huber, *On the period length of generalized inversive pseudorandom number generators*, Appl. Algebra in Eng. Comm. and Comput. (to appear).
9. 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.
10. H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Adv. in Math. **26** (1977), 99–181.
11. ——, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144.
12. ——, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287.
13. ——, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345.
14. ——, *Nonlinear methods for pseudorandom number and vector generation*, Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems, vol. 374, Springer, Berlin, 1992, pp. 145–153.
15. ——, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992.
16. ——, *Finite fields, pseudorandom numbers, and quasirandom points*, Finite Fields, Coding Theory, and Advances in Communications and Computing (G. L. Mullen and P. J.-S. Shiue, eds.), Dekker, New York, 1992, pp. 375–394.
17. ——, *New methods for pseudorandom number and pseudorandom vector generation*, Proc. 1992 Winter Simulation Conf. (Arlington, VA, 1992), IEEE Press, Piscataway, NJ, 1992, pp. 264–269.

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