MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 206
APRIL 1994, PAGES 787–797

EXPLICIT INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS WITH POWER OF TWO MODULUS

JÜRGEN EICHENAUER-HERRMANN AND KATJA ICKSTADT

ABSTRACT. An explicit version of the inversive congruential method with power of two modulus for generating uniform pseudorandom numbers is introduced. Statistical independence properties of the generated sequences are studied by means of the serial test. The method of proof relies on a detailed analysis of certain exponential sums.

1. INTRODUCTION

Several nonlinear congruential methods of generating uniform pseudorandom numbers in the interval $[0, 1)$ have been introduced and analyzed in the last few years. A review of the development of this important area is given in the survey articles [3, 4, 16–18, 20–22] and in H. Niederreiter's excellent monograph [19]. The most promising approach is the inversive congruential method, which is typically considered with respect to a prime modulus (cf. [1, 5, 7, 11, 14, 15]) or a power of two modulus (cf. [2, 6, 8, 9, 14]). The latter case is studied in the present paper.

Let $m = 2^\omega$ for an integer $\omega \geq 5$. An inversive congruential sequence $(y_n)_{n\geq 0}$ is usually defined by the recursion $y_{n+1} \equiv ay_n^{-1} + b \pmod m$, where a and b are integers with $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$ and y_n^{-1} denotes the multiplicative inverse of y_n modulo m. In the present paper an explicit version of this inversive congruential method is introduced and studied. This approach is motivated by very attractive results for an explicit version of the inversive congruential method with prime modulus (cf. [7, 21, 22]). In the following let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for integers $n \geq 2$, and write $\mathbb{Z}_n^*$ for the set of all odd integers in $\mathbb{Z}_n$. For integers $a \in \mathbb{Z}_m$ with $a \equiv 2 \pmod 4$ and $b \in \mathbb{Z}_m^*$ an *explicit inversive congruential sequence* $(y_n)_{n\geq 0}$ of elements of $\mathbb{Z}_m^*$ is defined by

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

A sequence $(x_n)_{n\geq 0}$ of *explicit inversive congruential pseudorandom numbers* in the interval $[0, 1)$ is obtained by $x_n = y_n/m$ for $n \geq 0$. It follows at once from the condition $a \equiv 2 \pmod 4$ that any explicit inversive congruential sequence is purely periodic with maximal period length $m/2$, i.e.,

Received by the editor October 20, 1992 and, in revised form, March 9, 1993.
1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 11K45.
Key words and phrases. Pseudorandom numbers, inversive congruential method, power of two modulus, discrepancy.

0025-5718/94 $1.00 + $.25 per page

$\{y_0, y_1, \ldots, y_{m/2-1}\} = \mathbb{Z}_m^*$, which guarantees that the corresponding pseudorandom numbers are equidistributed in one dimension.

Statistical independence properties of pseudorandom numbers are very important for their application in a stochastic simulation. A reliable theoretical test for statistical independence is the *serial test*, which employs the discrepancy of k-tuples of successive pseudorandom numbers. 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 points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the k-dimensional volume of J. For a sequence $(x_n)_{n\geq 0}$ of explicit inversive congruential pseudorandom numbers the abbreviations

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

and

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

are used. An explicit inversive congruential generator passes the k-dimensional serial test if $D_{m/2}^{(k)}$ is reasonably small. According to the law of the iterated logarithm for discrepancies (cf. [12]), $D_{m/2}^{(k)}$ should be of an order of magnitude $m^{-1/2}$, since the discrepancy of N independent and uniformly distributed random points from $[0, 1)^k$ is roughly $N^{-1/2}(\log\log N)^{1/2}$.

In the present paper, upper and lower bounds for the discrepancy $D_{m/2}^{(k)}$ are established. The second section contains several auxiliary results. The main results are given in the third section. Their proof is based on a thorough evaluation of certain exponential sums. The reader is referred to [13] for background material on this topic. In the fourth section the behavior of explicit inversive congruential generators under the serial test is discussed.

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 $-q/2 < h_j \leq q/2$ 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 $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(q)$. For $t \in \mathbf{R}$ and integers $\alpha \geq 1$ and z, the abbreviations $e(t) = e^{2\pi i t}$ and $\chi_\alpha(z) = e(z/2^\alpha)$ are used, respectively. Let $\mathbf{u}\cdot\mathbf{v}$ stand for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbf{R}^k$.

Below, three known general results for estimating discrepancies are stated. The first two lemmas follow from [19, Theorem 3.10 and Corollary 3.17] and the third lemma can be deduced from [14, Lemma 4].

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* $\mathbf{y}_n \in \mathbf{Z}_q^k$ *for* $0 \leq n < N$. *Then the discrepancy of the points* $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ *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. *The discrepancy* $D_N = D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1})$ *of* N *arbitrary points* $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^k$ *satisfies*

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right| \leq \frac{2}{\pi} \left(\left(\frac{\pi + 1}{2} \right)^l - \frac{1}{2^l} \right) N D_N \prod_{j=1}^{k} \max(1, 2|h_j|)$$

for any nonzero lattice point $\mathbf{h} = (h_1, \ldots, h_k) \in \mathbb{Z}^k$, *where* l *denotes the number of nonzero coordinates of* $\mathbf{h}$.

Lemma 3. *Let* $q = 2^\alpha$ *for some integer* $\alpha \geq 1$. *Then*

$$\sum_{\substack{h \in C_1(q) \\ h \equiv 1 \pmod 2}} \frac{1}{r(h, q)} < \frac{1}{\pi} \log q + \frac{3}{5}.$$

In the following, for a fixed integer $a \in \mathbb{Z}_m$ with $a \equiv 2 \pmod 4$, the mapping $\phi = (\phi_1, \phi_2)\colon \mathbb{Z}^2 \to \mathbb{Z}^2$ is defined by

$$\phi(y, z) = ((ay + 1)(az + 1), y - z).$$

For integers $\alpha \geq 3$ let

$$N_\alpha = \{(s, t) \in \mathbb{Z}_{2^\alpha}^2 \mid t \equiv 0 \pmod 2, s \equiv 2t + 1 \pmod 8\}.$$

Observe that $\phi(y, z) \pmod{2^\alpha} \in N_\alpha$ for odd integers y and z. The following technical result is used later on in the proof of Lemma 5.

Lemma 4. *Let* $(s, t) \in N_\alpha$ *for some integer* $\alpha \geq 3$. *Then there exists exactly one* $(y, z) \in \mathbb{Z}_{2^{\alpha-2}}^* \times \mathbb{Z}_{2^\alpha}^*$ *with*

$$\phi(y, z) \equiv (s, t) \pmod{2^\alpha}.$$

Proof. For integers $\alpha \geq 3$ and $(s, t) \in N_\alpha$, let

$$M_\alpha(s, t) = \{(y, z) \in \mathbb{Z}_{2^\alpha}^* \times \mathbb{Z}_{2^\alpha}^* \mid \phi(y, z) \equiv (s, t) \pmod{2^\alpha}\}.$$

Below, it is proved by induction on $\alpha \geq 3$ that for $(s, t) \in N_\alpha$ the set $M_\alpha(s, t)$ contains exactly four elements, and that any two elements $(y, z), (y', z') \in M_\alpha(s, t)$ satisfy $(y, z) \equiv (y', z') + 2^{\alpha-2}(\lambda, \lambda) \pmod{2^\alpha}$ for some $\lambda \in \mathbb{Z}_4$. This statement is equivalent to the assertion of Lemma 4, since

$$\phi(y + 2^{\alpha-2}, z + 2^{\alpha-2}) \equiv \phi(y, z) \pmod{2^\alpha}$$

for integers y and z.

For $\alpha = 3$ the above statement can be shown by inspection. Now, assume that it is valid for some integer $\alpha \geq 3$. Let $(s, t) \in N_{\alpha+1}$ be fixed. Then $(s, t) \pmod{2^\alpha} \in N_\alpha$ and the assumption implies that there exists an element $(y_\alpha, z_\alpha) \in \mathbb{Z}_{2^\alpha}^* \times \mathbb{Z}_{2^\alpha}^*$ with $\phi(y_\alpha, z_\alpha) \equiv (s, t) \pmod{2^\alpha}$. Hence,

$$\phi(y_\alpha, z_\alpha) \equiv (s, t) + 2^\alpha(\tilde{s}, \tilde{t}) \pmod{2^{\alpha+1}}$$

with suitable $\tilde{s}, \tilde{t} \in \mathbb{Z}_2$. In the following, let $(y, z) \in \mathbb{Z}_{2^{\alpha+1}}^* \times \mathbb{Z}_{2^{\alpha+1}}^*$ be an arbitrary element. It suffices to consider the case $(y, z) \pmod{2^\alpha} \in M_\alpha(s, t)$, since otherwise (y, z) cannot belong to the set $M_{\alpha+1}(s, t)$. Therefore, by the assumption, $(y, z) \equiv (y_\alpha, z_\alpha) + 2^{\alpha-2}(\lambda, \lambda) \pmod{2^\alpha}$ with a suitable $\lambda \in \mathbb{Z}_4$. Hence, one obtains

$$(y, z) \equiv (y_\alpha, z_\alpha) + 2^{\alpha-2}(\lambda, \lambda) + 2^\alpha(\tilde{y}, \tilde{z}) \pmod{2^{\alpha+1}}$$

with suitable $\tilde{y}, \tilde{z} \in \mathbb{Z}_2$. A short calculation shows that

$$\begin{aligned}\phi(y, z) &\equiv \phi(y_\alpha + 2^{\alpha-2}\lambda + 2^\alpha\tilde{y}, z_\alpha + 2^{\alpha-2}\lambda + 2^\alpha\tilde{z}) \\ &\equiv \phi(y_\alpha, z_\alpha) + 2^\alpha(\lambda, \tilde{y} - \tilde{z}) \\ &\equiv (s, t) + 2^\alpha(\lambda + \tilde{s}, \tilde{y} - \tilde{z} + \tilde{t}) \pmod{2^{\alpha+1}}.\end{aligned}$$

Therefore, an element $(y, z) \in \mathbb{Z}_{2^{\alpha+1}}^* \times \mathbb{Z}_{2^{\alpha+1}}^*$ belongs to $M_{\alpha+1}(s, t)$ if and only if $\lambda + \tilde{s} \equiv \tilde{y} - \tilde{z} + \tilde{t} \equiv 0 \pmod 2$, which is equivalent to $\tilde{z} \equiv \tilde{y} + \tilde{t} \pmod 2$ and $\lambda = \tilde{s} + 2\tilde{\lambda}$ with a suitable $\tilde{\lambda} \in \mathbb{Z}_2$. Hence,

$$(y, z) \equiv (y_\alpha + 2^{\alpha-2}\tilde{s}, z_\alpha + 2^{\alpha-2}\tilde{s} + 2^\alpha\tilde{t}) + 2^{\alpha-1}(\lambda', \lambda') \pmod{2^{\alpha+1}},$$

where $\lambda' = \tilde{\lambda} + 2\tilde{y} \in \mathbb{Z}_4$. Consequently, the set $M_{\alpha+1}(s, t)$ contains exactly four elements, and any two elements $(y, z), (y', z') \in M_{\alpha+1}(s, t)$ satisfy $(y, z) \equiv (y', z') + 2^{\alpha-1}(\lambda, \lambda) \pmod{2^{\alpha+1}}$ for some $\lambda \in \mathbb{Z}_4$, which yields the desired result. □

A crucial role in the present paper is played by certain exponential sums, which are defined by

$$S(u, v; 2^\alpha) = \sum_{z \in \mathbb{Z}_{2^\alpha}^*} \chi_\alpha(uz^{-1} + v(z + a)^{-1})$$

for integers u, v, and $\alpha \geq 1$, where $a \in \mathbb{Z}_m$ with $a \equiv 2 \pmod 4$ is fixed. Some relevant properties of these exponential sums are collected in Lemma 5.

Lemma 5. *Let u, v, and $\alpha \geq 2$ be integers.*

(a) *If $u + v \equiv 1 \pmod 2$, then $S(u, v; 2^\alpha) = 0$.*

(b) *If $u \equiv v \equiv 0 \pmod 2$, then $S(u, v; 2^\alpha) = 2S(\frac{u}{2}, \frac{v}{2}; 2^{\alpha-1})$.*

(c) *If $u \equiv v \equiv 1 \pmod 2$ and $\alpha \geq 5$, then*

$$|S(u, v; 2^\alpha)| = \begin{cases} 2^{(\alpha+2)/2} & \text{for } u + v \equiv 0 \pmod 8, \\ 0 & \text{for } u + v \not\equiv 0 \pmod 8. \end{cases}$$

Proof. (a) A short calculation shows that

$$\begin{aligned} S(u, v; 2^\alpha) &= \sum_{z \in \mathbb{Z}_{2^{\alpha-1}}^*} (\chi_\alpha(uz^{-1} + v(z+a)^{-1}) \\ &\qquad + \chi_\alpha(u(z+2^{\alpha-1})^{-1} + v(z+a+2^{\alpha-1})^{-1})) \\ &= \sum_{z \in \mathbb{Z}_{2^{\alpha-1}}^*} \chi_\alpha(uz^{-1} + v(z+a)^{-1})(1 + \chi_1(u+v)). \end{aligned}$$

Therefore, the desired result follows from $\chi_1(u+v) = -1$ for $u+v \equiv 1 \pmod 2$.

(b) Since $\chi_1(u+v) = 1$ for $u+v \equiv 0 \pmod 2$, it follows from part (a) of the proof that

$$S(u, v; 2^\alpha) = 2 \sum_{z \in \mathbb{Z}_{2^{\alpha-1}}^*} \chi_{\alpha-1}\left(\frac{u}{2} z^{-1} + \frac{v}{2}(z+a)^{-1}\right) = 2S\left(\frac{u}{2}, \frac{v}{2}; 2^{\alpha-1}\right).$$

(c) First, the transformation $y \equiv z^{-1} \pmod{2^\alpha}$ for $z \in \mathbb{Z}_{2^\alpha}^*$ yields

$$S(u, v; 2^\alpha) = \sum_{y \in \mathbb{Z}_{2^\alpha}^*} \chi_\alpha(uy + vy(ay+1)^{-1}).$$

Hence, one obtains

$$\begin{aligned} |S(u, v; 2^\alpha)|^2 &= S(u, v; 2^\alpha) \cdot \overline{S(u, v; 2^\alpha)} \\ &= \sum_{y, z \in \mathbb{Z}_{2^\alpha}^*} \chi_\alpha(u(y-z) + v(y(ay+1)^{-1} - z(az+1)^{-1})) \\ &= \sum_{y, z \in \mathbb{Z}_{2^\alpha}^*} \chi_\alpha(\phi_2(y, z)(u + v(\phi_1(y, z))^{-1})), \end{aligned}$$

where the mapping $\phi = (\phi_1, \phi_2)$ is defined as above. Since

$$\phi(y + 2^{\alpha-2}, z + 2^{\alpha-2}) \equiv \phi(y, z) \pmod{2^\alpha}$$

for integers y and z, it follows, together with Lemma 4, that

$$\begin{aligned} |S(u, v; 2^\alpha)|^2 &= 4 \sum_{(y, z) \in \mathbb{Z}_{2^{\alpha-2}}^* \times \mathbb{Z}_{2^\alpha}^*} \chi_\alpha(\phi_2(y, z)(u + v(\phi_1(y, z))^{-1})) \\ &= 4 \sum_{(s, t) \in N_\alpha} \chi_\alpha(t(u + vs^{-1})) = 4(\Sigma_1 + \Sigma_2), \end{aligned}$$

where the abbreviations

$$\Sigma_1 = \sum_{\substack{s \in \mathbb{Z}_{2^\alpha} \\ s \equiv 1 \pmod 8}} \sum_{\substack{t \in \mathbb{Z}_{2^\alpha} \\ t \equiv 0 \pmod 4}} \chi_\alpha(t(u + vs^{-1}))$$

and

$$\Sigma_2 = \sum_{\substack{s \in \mathbb{Z}_{2^\alpha} \\ s \equiv 5 \pmod 8}} \sum_{\substack{t \in \mathbb{Z}_{2^\alpha} \\ t \equiv 2 \pmod 4}} \chi_\alpha(t(u + vs^{-1}))$$

are used. Straightforward calculations show that

$$\Sigma_1 = 4 \sum_{\substack{s \in \mathbb{Z}_{2^{\alpha-2}} \\ s \equiv 1 \pmod 8 \\ u + vs^{-1} \equiv 0 \pmod{2^{\alpha-2}}}} 2^{\alpha-2} = \begin{cases} 2^\alpha & \text{for } u + v \equiv 0 \pmod 8, \\ 0 & \text{for } u + v \not\equiv 0 \pmod 8 \end{cases}$$

and

$$\Sigma_2 = 2 \sum_{\substack{s \in \mathbb{Z}_{2^{\alpha-2}} \\ s \equiv 5 \pmod 8}} \sum_{\tau \in \mathbb{Z}_{2^{\alpha-1}}^*} (\chi_{\alpha-1}(\tau(u + vs^{-1})) + \chi_{\alpha-1}(\tau(u + v(s + 2^{\alpha-2})^{-1})))$$

$$= 2 \sum_{\substack{s \in \mathbb{Z}_{2^{\alpha-2}} \\ s \equiv 5 \pmod 8}} \sum_{\tau \in \mathbb{Z}_{2^{\alpha-1}}^*} \chi_{\alpha-1}(\tau(u + vs^{-1}))(1 + \chi_1(1)) = 0,$$

which completes the proof. □

Finally, another exponential sum is defined by

$$G(u, v; 2^\alpha) = \sum_{y \in \mathbb{Z}_{2^\alpha}} \chi_\alpha(uy^2 + vy)$$

for integers u, v, and $\alpha \geq 1$. The following result can be deduced from [10, Lemma 6].

Lemma 6. *If u, v, and $\alpha \geq 1$ are integers with $\gcd(u, 2^\alpha) > \gcd(v, 2^\alpha)$, then $G(u, v; 2^\alpha) = 0$.*

3. Bounds for the discrepancy

Theorem 1. *The discrepancy $D_{m/2}^{(2)}$ of any explicit inversive congruential generator with power of two modulus m satisfies*

$$D_{m/2}^{(2)} < \frac{8}{7}(4 + \sqrt{2}) m^{-1/2} \left(\frac{1}{\pi} \log m + \frac{3}{5} \right)^2 + 4m^{-1}.$$

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

$$D_{m/2}^{(2)} \leq \frac{2}{m} + \frac{2}{m} \sum_{\mathbf{h} \in C_2(m)} \frac{1}{r(\mathbf{h}, m)} \left| \sum_{n=0}^{m/2-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right|$$

$$= \frac{2}{m} + \frac{2}{m} \sum_{\mathbf{h} \in C_2(m)} \frac{1}{r(\mathbf{h}, m)} \left| \sum_{n=0}^{m/2-1} \chi_\omega(h_1(an + b)^{-1} + h_2(an + b + a)^{-1}) \right|$$

$$= \frac{2}{m} + \frac{2}{m} \sum_{\mathbf{h} \in C_2(m)} \frac{1}{r(\mathbf{h}, m)} |S(h_1, h_2; m)|$$

$$= \frac{2}{m} + \frac{2}{m} \sum_{\substack{\mathbf{h} \in C_2(m) \\ \mathbf{h} \equiv 0 \pmod{2^{\omega-1}}}} \frac{1}{r(\mathbf{h}, m)} |S(h_1, h_2; m)|$$

$$+ \frac{2}{m} \sum_{\alpha=0}^{\omega-2} \sum_{\substack{\mathbf{h} \in C_2(m) \\ \gcd(h_1, h_2, m) = 2^\alpha}} \frac{1}{r(\mathbf{h}, m)} |S(h_1, h_2; m)|$$

$$= \frac{4}{m} + \frac{1}{m^2} + \frac{2}{m} \sum_{\alpha=0}^{\omega-2} \sum_{\substack{\mathbf{g} \in C_2(2^{\omega-\alpha}) \\ \gcd(g_1, g_2, 2) = 1}} \frac{1}{r(2^\alpha \mathbf{g}, m)} |S(2^\alpha g_1, 2^\alpha g_2; m)|.$$

Now, Lemma 5 can be used in order to obtain

$$D_{m/2}^{(2)} \le \frac{4}{m} + \frac{1}{m^2} + \frac{2}{m}\sum_{\alpha=0}^{\omega-2} 2^{\alpha} \sum_{\substack{\mathbf{g}\in C_2(2^{\omega-\alpha}) \\ \gcd(g_1, g_2, 2)=1}} \frac{1}{r(2^{\alpha}\mathbf{g}, m)} |S(g_1, g_2; 2^{\omega-\alpha})|$$

$$= \frac{4}{m} + \frac{1}{m^2} + \frac{2}{m}\sum_{\alpha=0}^{\omega-2} 2^{\alpha} \sum_{\substack{\mathbf{g}\in C_2(2^{\omega-\alpha}) \\ g_1\equiv g_2\equiv 1 \pmod 2}} \frac{1}{r(2^{\alpha}\mathbf{g}, m)} |S(g_1, g_2; 2^{\omega-\alpha})|$$

$$= \frac{4}{m} + \frac{1}{m^2} + \frac{2}{m}\sum_{\alpha=0}^{\omega-2} 2^{-\alpha} \sum_{\substack{\mathbf{g}\in C_2(2^{\omega-\alpha}) \\ g_1\equiv g_2\equiv 1 \pmod 2}} \frac{1}{r(\mathbf{g}, 2^{\omega-\alpha})} |S(g_1, g_2; 2^{\omega-\alpha})|$$

$$< \frac{4}{m} + \frac{1}{m^2} + \frac{2}{m}\sum_{\alpha=0}^{\omega-2} 2^{-\alpha+(\omega-\alpha+2)/2} \sum_{\substack{\mathbf{g}\in C_2(2^{\omega-\alpha}) \\ g_1\equiv g_2\equiv 1 \pmod 2}} \frac{1}{r(\mathbf{g}, 2^{\omega-\alpha})}$$

$$= \frac{4}{m} + \frac{1}{m^2} + \frac{4}{m^{1/2}}\sum_{\alpha=0}^{\omega-2} 2^{-3\alpha/2} \left(\sum_{\substack{g\in C_1(2^{\omega-\alpha}) \\ g\equiv 1 \pmod 2}} \frac{1}{r(g, 2^{\omega-\alpha})} \right)^2.$$

Finally, it follows from Lemma 3 that

$$D_{m/2}^{(2)} < \frac{4}{m} + \frac{1}{m^2} + \frac{4}{m^{1/2}}\sum_{\alpha=0}^{\omega-2} 2^{-3\alpha/2} \left(\frac{1}{\pi}\log 2^{\omega-\alpha} + \frac{3}{5} \right)^2$$

$$< \frac{4}{m} + \frac{4}{m^{1/2}}\sum_{\alpha=0}^{\omega-1} 2^{-3\alpha/2} \left(\frac{1}{\pi}\log 2^{\omega-\alpha} + \frac{3}{5} \right)^2$$

$$< \frac{4}{m} + \frac{4}{m^{1/2}} \left(\frac{1}{\pi}\log m + \frac{3}{5} \right)^2 \sum_{\alpha=0}^{\infty} 2^{-3\alpha/2}$$

$$= \frac{4}{m} + \frac{8(4+\sqrt{2})}{7m^{1/2}} \left(\frac{1}{\pi}\log m + \frac{3}{5} \right)^2. \quad \square$$

Theorem 2. *The discrepancy $D_{m/2}^{(2)}$ of any explicit inversive congruential generator with power of two modulus m satisfies*

$$D_{m/2}^{(2)} \ge \frac{2}{\pi+2} m^{-1/2}.$$

Proof. First, Lemma 2 is applied with $k = 2$, $N = m/2$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \le n < m/2$, $\mathbf{h} = (1, -1)$, and hence $l = 2$. This yields

$$\left| \sum_{n=0}^{m/2-1} e(\mathbf{h}\cdot\mathbf{x}_n) \right| \le (\pi+2) m D_{m/2}^{(2)}.$$

Now, it follows as in the proof of Theorem 1 that

$$\left| \sum_{n=0}^{m/2-1} e(\mathbf{h}\cdot\mathbf{x}_n) \right| = |S(1, -1; m)|.$$

Finally, an application of Lemma 5(c) shows that $|S(1, -1; m)| = 2m^{1/2}$, which yields the desired result. □

In the following, let $\omega = 3\nu + 2 + \mu$ with suitable integers $\nu \geq 1$ and $\mu \in \{0, 1, 2\}$, and put

$$\lambda = \begin{cases} 1 & \text{for } \mu \in \{0, 1\}, \\ 2 & \text{for } \mu = 2. \end{cases}$$

Theorem 3. *The discrepancy $D_{m/2}^{(k)}$ of any explicit inversive congruential generator with power of two modulus m satisfies*

$$D_{m/2}^{(k)} \geq \frac{2^{(\mu-1)/3}}{27\lambda^3(\pi^2 + 3\pi + 3)} m^{-1/3}$$

for all dimensions $k \geq 3$.

Proof. First, Lemma 2 is applied with $N = m/2$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < m/2$, $\mathbf{h} = \lambda(1, 2, -27, 0, \ldots, 0) \in \mathbb{Z}^k$, and hence $l = 3$. This yields

$$\left| \sum_{n=0}^{m/2-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \leq 54\lambda^3(\pi^2 + 3\pi + 3) m D_{m/2}^{(k)}.$$

A short calculation shows that

$$\begin{aligned} \sum_{n=0}^{m/2-1} e(\mathbf{h} \cdot \mathbf{x}_n) &= \sum_{n=0}^{m/2-1} \chi_\omega(\lambda((an+b)^{-1} + 2(an+b+a)^{-1} - 27(an+b+2a)^{-1})) \\ &= \sum_{y \in \mathbb{Z}_m^*} \chi_\omega(\lambda(y^{-1} + 2(y+a)^{-1} - 27(y+2a)^{-1})) \\ &= \sum_{z \in \mathbb{Z}_m^*} \chi_\omega(\lambda R(z)), \end{aligned}$$

where the function $R: \mathbb{Z}_m^* \to \mathbb{Z}_m$ is defined by

$$R(z) \equiv z + 2z(az+1)^{-1} - 27z(2az+1)^{-1} \pmod{m}.$$

Next, observe that

$$R'(z) \equiv 1 + 2(az+1)^{-2} - 27(2az+1)^{-2} \pmod{m}$$

and

$$R''(z) \equiv 4a(27(2az+1)^{-3} - (az+1)^{-3}) \pmod{m}.$$

Since $\lambda 2^{3\nu+3} \equiv 0 \pmod{m}$, it follows after straightforward, but tedious, calculations that

$$\begin{aligned} \sum_{z \in \mathbb{Z}_m^*} \chi_\omega(\lambda R(z)) &= \sum_{x \in \mathbb{Z}_{2^\nu}^*} \sum_{y \in \mathbb{Z}_{2^{\omega-\nu}}} \chi_\omega(\lambda R(x + 2^\nu y)) \\ &= \sum_{x \in \mathbb{Z}_{2^\nu}^*} \sum_{y \in \mathbb{Z}_{2^{\omega-\nu}}} \chi_\omega(\lambda(R(x) + 2^\nu R'(x)y + 2^{2\nu-1}R''(x)y^2)) \\ &= \sum_{x \in \mathbb{Z}_{2^\nu}^*} \chi_\omega(\lambda R(x)) G(2^{\nu-1}\lambda R''(x), \lambda R'(x); 2^{\omega-\nu}). \end{aligned}$$

Now, a short calculation shows that

$$R'(x) \equiv 2(ax+2)^2(2a^2x^2 - 2ax - 3)(ax+1)^{-2}(2ax+1)^{-2} \pmod{m}$$

and

$$R''(x) \equiv 4a(ax+2)(19a^2x^2+31ax+13)(ax+1)^{-3}(2ax+1)^{-3} \pmod{m}$$

for $x \in \mathbb{Z}_m^*$. In the following, let $x \in \mathbb{Z}_{2^\nu}^*$ be fixed and define an integer $\xi \in \{2, 3, \ldots, \nu+1\}$ by $\gcd(ax+2, 2^{\nu+1}) = 2^\xi$. Since $2a^2x^2 - 2ax - 3 \equiv 1 \pmod 2$ and $19a^2x^2 + 31ax + 13 \equiv 1 \pmod 2$, it follows that

$$\gcd(\lambda R'(x), 2^{\omega-\nu}) = 2^{\min(2\xi+\lambda, \omega-\nu)}$$

and

$$\gcd(2^{\nu-1}\lambda R''(x), 2^{\omega-\nu}) = 2^{\min(\nu+\xi+\lambda+1, \omega-\nu)}.$$

If $\xi \le \nu$, then $2\xi + \lambda < \nu + \xi + \lambda + 1 \le \omega - \nu$, and Lemma 6 implies that

$$G(2^{\nu-1}\lambda R''(x), \lambda R'(x); 2^{\omega-\nu}) = 0.$$

If $\xi = \nu + 1$, then $\lambda R'(x) \equiv 2^{\nu-1}\lambda R''(x) \equiv 0 \pmod{2^{\omega-\nu}}$, and hence

$$G(2^{\nu-1}\lambda R''(x), \lambda R'(x); 2^{\omega-\nu}) = 2^{\omega-\nu}.$$

Since there exists exactly one $x \in \mathbb{Z}_{2^\nu}^*$ with $ax + 2 \equiv 0 \pmod{2^{\nu+1}}$, i.e., $\xi = \nu + 1$, one obtains

$$\left| \sum_{z \in \mathbb{Z}_m^*} \chi_\omega(\lambda R(z)) \right| = 2^{\omega-\nu}.$$

This yields

$$D_{m/2}^{(k)} \ge \frac{2^{\omega-\nu}}{54\lambda^3(\pi^2+3\pi+3)m} = \frac{2^{(\mu-1)/3}}{27\lambda^3(\pi^2+3\pi+3)} m^{-1/3}$$

for all dimensions $k \ge 3$. □

4. Conclusions

Theorem 1 shows that $D_{m/2}^{(2)} = O(m^{-1/2}(\log m)^2)$ for any explicit inversive congruential sequence, where the implied constant is absolute. It should be observed that this bound is independent of the specific choice of the parameters a (and b) in the explicit inversive congruential method. Theorem 2 implies that the upper bound is best possible, up to the logarithmic factor, since the discrepancy $D_{m/2}^{(2)}$ of any explicit inversive congruential generator has an order of magnitude at least $m^{-1/2}$. Hence, Theorems 1 and 2 show that the discrepancy $D_{m/2}^{(2)}$ is in accordance with the law of the iterated logarithm for discrepancies. In this sense, explicit inversive congruential pseudorandom numbers behave like true random numbers.

However, Theorem 3 implies that any explicit inversive congruential sequence fails the serial test for all dimensions $k \ge 3$, since the corresponding discrepancy $D_{m/2}^{(k)}$ is of an order of magnitude at least $m^{-1/3}$. Consequently, an upper bound for the discrepancy $D_{m/2}^{(k)}$ with $k \ge 3$, which is basically in accordance with the law of the iterated logarithm, cannot be obtained, since the order of magnitude $m^{-1/3}$ is already too large. This behavior of the explicit inversive congruential method with *power of two modulus* is a serious disadvantage compared to the situation for a *prime modulus*, where the discrepancy of k-tuples

fits to the law of the iterated logarithm for any dimension $k \geq 2$ (cf. [7, 21, 22]).

ACKNOWLEDGMENT

The authors would like to thank the referee for most valuable comments.

BIBLIOGRAPHY

1. J. Eichenauer and J. Lehn, *A non-linear congruential pseudorandom number generator*, Statist. Papers **27** (1986), 315–326.
2. J. Eichenauer, J. Lehn, and A. Topuzoğlu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51** (1988), 757–759.
3. J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers*, Z. Angew. Math. Mech. **73** (1993), T644–T647.
4. ———, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
5. ———, *Inversive congruential pseudorandom numbers avoid the planes*, Math. Comp. **56** (1991), 297–301.
6. ———, *On the autocorrelation structure of inversive congruential pseudorandom number sequences*, Statist. Papers **33** (1992), 261–268.
7. ———, *Statistical independence of a new class of inversive congruential pseudorandom numbers*, Math. Comp. **60** (1993), 375–384.
8. 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.
9. 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.
10. ———, *On the discrepancy of quadratic congruential pseudorandom numbers*, J. Comput. Appl. Math. **34** (1991), 243–249.
11. 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.
12. 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.
13. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
14. H. Niederreiter, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144.
15. ———, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287.
16. ———, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345.
17. ———, *Finite fields and their applications*, Contributions to General Algebra, vol. 7, Teubner, Stuttgart, 1991, pp. 251–264.
18. ———, *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.
19. ———, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992.
20. ———, *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.

21. ———, *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.

22. ———, *Pseudorandom numbers and quasirandom points*, Z. Angew. Math. Mech. **73** (1993), T648–T652.

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