

INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS: DISTRIBUTION OF TRIPLES

JÜRGEN EICHENAUER–HERRMANN AND HARALD NIEDERREITER

ABSTRACT. This paper deals with the inversive congruential method with power of two modulus m for generating uniform pseudorandom numbers. Statistical independence properties of the generated sequences are studied based on the distribution of triples of successive pseudorandom numbers. It is shown that, on the average over the parameters in the inversive congruential method, the discrepancy of the corresponding point sets in the unit cube is of an order of magnitude between $m^{-1/2}$ and $m^{-1/2}(\log m)^3$. The method of proof relies on a detailed discussion of the properties of certain exponential sums.

1. INTRODUCTION

Nonlinear congruential methods of generating uniform pseudorandom numbers in the interval $[0, 1)$ have been studied intensively during the last years. Reviews of the development of this area can be found in the survey articles [2, 3, 11, 15, 17] and in the monograph [16]. A very promising nonlinear congruential approach is the (*recursive*) *inversive congruential method*. The present paper concentrates on the particularly important case of a power of two modulus, which received considerable attention [1, 4, 5, 7, 8, 9, 14]. Let $m = 2^\omega$ with some integer $\omega \geq 5$. Let $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ for integers $n \geq 1$, and write \mathbb{Z}_n^* for the set of all odd integers in \mathbb{Z}_n . For $y_0 \in \mathbb{Z}_m^*$ and parameters $a, c \in \mathbb{Z}_m$ with $a \equiv 1 \pmod{4}$ and $c \equiv 2 \pmod{4}$, an *inversive congruential sequence* $(y_n)_{n \geq 0}$ of elements of \mathbb{Z}_m^* is defined by

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

where z^{-1} denotes the multiplicative inverse of z in the group \mathbb{Z}_m^* . A sequence $(x_n)_{n \geq 0}$ of *inversive congruential pseudorandom numbers* in the interval $[0, 1)$ is obtained by $x_n = y_n/m$ for $n \geq 0$. It follows from [1], [16, Theorem 8.9] that the sequences $(x_n)_{n \geq 0}$ and $(y_n)_{n \geq 0}$ are purely periodic with the maximum possible period length $m/2$. The low-order bits of the pseudorandom numbers generated by this method have a short period length. The referee has pointed out that this fact may be viewed as a deficiency of this method. Statistical independence properties of the generated sequences, which are very important for their usability in a stochastic simulation, can be analysed based on the discrepancy of s -tuples of successive pseudorandom numbers with $s \geq 2$. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1} \in$

Received by the editor April 12, 1996 and, in revised form, August 23, 1996.

1991 *Mathematics Subject Classification*. Primary 65C10; Secondary 11K45.

Key words and phrases. Uniform pseudorandom numbers, inversive congruential method, statistical independence, discrepancy of triples, exponential sums.

$[0, 1]^s$ the *discrepancy* is defined by

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

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 $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ falling into J , and $V(J)$ denotes the s -dimensional volume of J . Observe that the discrepancy of N true random points in $[0, 1]^s$ is almost always of an order of magnitude $N^{-1/2}(\log \log N)^{1/2}$ according to the law of the iterated logarithm for discrepancies [10]. Subsequently, the abbreviations

$$\mathbf{x}_n = (x_n, x_{n+1}, \dots, x_{n+s-1}) \in [0, 1]^s, \quad n \geq 0,$$

and

$$D_{m/2;a,c}^{(s)} = D_{m/2}(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{(m/2)-1})$$

are used. In [5, 7, 14] upper and lower bounds for the discrepancy $D_{m/2;a,c}^{(2)}$ of pairs are established, which are basically in accordance with the law of the iterated logarithm for the discrepancy of true random points in $[0, 1]^2$. In the present paper, the discrepancy $D_{m/2;a,c}^{(3)}$ of triples is studied. In the fourth section, the main results are established and discussed. Their proof relies on the analysis of certain exponential sums, which is carried out in the third section. The reader is referred to [12] for an introduction to the theory of exponential sums. The second section contains some basic auxiliary results.

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

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

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 $e(t) = e^{2\pi it}$ is used, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$. Subsequently, two known general results for estimating discrepancies are stated which follow from [5, Lemma 1] and [16, Corollary 3.17], respectively.

Lemma 1. *Let $N \geq 1$ and $q \geq 2$ be integers. Let d be a divisor of q with $1 \leq d < q$. Let $\mathbf{c} \in \mathbb{Z}_d^k$ and $\mathbf{y}_n \in \mathbb{Z}_q^k$ with $\mathbf{y}_n \equiv \mathbf{c} \pmod{d}$ for $0 \leq n < N$. Then the discrepancy of the points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ with $\mathbf{t}_n = \mathbf{y}_n/q \in [0, 1]^k$ satisfies*

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

Remark. The bound in Lemma 1 can also be derived from [16, Theorem 3.10] by noting that the proof of this result remains valid for the discrepancy $\bar{D}_N(\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1})$ extended over all intervals modulo 1 in $[0, 1]^k$ and that both

$\tilde{D}_N(\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1})$ and the absolute values of the exponential sums in the bound in Lemma 1 are invariant under shifts modulo 1 of the point set by a constant vector.

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

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}) \geq \frac{\pi}{2N((\pi + 1)^\ell - 1) \prod_{j=1}^k \max(1, |h_j|)} \left| \sum_{n=0}^{N-1} \epsilon(\mathbf{h} \cdot \mathbf{t}_n) \right|$$

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

The first part of the result below follows from [13, Lemma 2.3]; its other parts can be deduced from [5, Lemma 2(a)] by some short calculations.

Lemma 3. *Let $\alpha \geq 3$ and $d \equiv 1 \pmod{2}$ be integers. Then*

$$\begin{aligned} \sum_{h \in C_1(2^\alpha)} \frac{1}{r(h, 2^\alpha)} &< \frac{2}{\pi} \log 2^\alpha + \frac{2}{5}, \\ \sum_{\substack{h \in C_1(2^\alpha) \\ h \equiv 1 \pmod{2}}} \frac{1}{r(h, 2^\alpha)} &< \frac{1}{\pi} \log 2^\alpha + \frac{4}{15}, \\ \sum_{\substack{h \in C_1(2^\alpha) \\ h \equiv d \pmod{4}}} \frac{1}{r(h, 2^\alpha)} &< \frac{1}{2\pi} \log 2^\alpha + \frac{2}{15}, \end{aligned}$$

and

$$\sum_{\substack{h \in C_1(2^\alpha) \\ h \equiv d \pmod{8}}} \frac{1}{r(h, 2^\alpha)} < \frac{1}{4\pi} \log 2^\alpha + \frac{1}{6}.$$

The following technical result is used in the proof of Lemma 7. A proof is added for the sake of completeness.

Lemma 4. *Let u, v, w, a, c be integers with $u \equiv w \equiv 1 \pmod{2}$, $v \equiv 0 \pmod{4}$, $u - v + w \equiv 0 \pmod{8}$, $a \equiv 1 \pmod{4}$, and $c \equiv 2 \pmod{4}$. Let*

$$P(x) = u(x + c)^2 - vax^2(x + c)^2 + wx^2$$

for $x \in \mathbb{Z}$. Then, for any integer $\beta \geq 1$, there exists exactly one integer $x \in \mathbb{Z}_{2^\beta}^*$ with $P(x) \equiv 0 \pmod{2^{\beta+2}}$.

Proof. The lemma is proved by induction on β . The desired result is obvious for $\beta = 1$. Now, suppose that for some integer $\beta \geq 1$ there exists exactly one integer $x_0 \in \mathbb{Z}_{2^\beta}^*$ with $P(x_0) \equiv 0 \pmod{2^{\beta+2}}$. Then a short calculation shows that

$$\begin{aligned} P(x_0 + 2^\beta) &\equiv u(x_0 + c + 2^\beta)^2 - va(x_0 + 2^\beta)^2(x_0 + c + 2^\beta)^2 + w(x_0 + 2^\beta)^2 \\ &\equiv P(x_0) + 2^{\beta+1}(u(x_0 + c) + wx_0) + 2^{2\beta}(u + w) \\ &\equiv P(x_0) + 2^{\beta+2} \pmod{2^{\beta+3}}, \end{aligned}$$

which implies that there exists exactly one integer $x \in \mathbb{Z}_{2^{\beta+1}}^*$, namely x_0 or $x_0 + 2^\beta$, with $P(x) \equiv 0 \pmod{2^{\beta+3}}$. □

Lemmas 1 and 2 indicate that a crucial role for the analysis of the discrepancy $D_{m/2;a,c}^{(3)}$ of triples is played by the exponential sums $\sum_{n=0}^{(m/2)-1} e(\mathbf{h} \cdot \mathbf{x}_n)$ for $\mathbf{h} \in \mathbb{Z}^3$. These sums are studied in Lemma 5, which leads to the definition of the exponential sums in the third section.

Lemma 5. *Let $\mathbf{h} = (h_1, h_2, h_3) \in \mathbb{Z}^3$. Then*

$$\left| \sum_{n=0}^{(m/2)-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = \left| \sum_{z \in \mathbb{Z}_m^*} e\left((h_1 z^{-1} + h_2 a z + h_3(z+c)^{-1})/m\right) \right|,$$

where $a, c \in \mathbb{Z}_m$ are the parameters in the inversive congruential method.

Proof. It follows from $\mathbf{x}_n = (y_n, y_{n+1}, y_{n+2})/m$, $y_{n+1} \equiv a(y_n^{-1} + c) \pmod{m}$, and $y_{n+2} \equiv (y_n^{-1} + c)^{-1} + ac \pmod{m}$ for $n \geq 0$ that

$$\left| \sum_{n=0}^{(m/2)-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = \left| \sum_{n=0}^{(m/2)-1} e\left((h_1 y_n + h_2 a y_n^{-1} + h_3(y_n^{-1} + c)^{-1})/m\right) \right|.$$

Since $\{y_0, y_1, \dots, y_{(m/2)-1}\} = \mathbb{Z}_m^*$, one obtains

$$\left| \sum_{n=0}^{(m/2)-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = \left| \sum_{y \in \mathbb{Z}_m^*} e\left((h_1 y + h_2 a y^{-1} + h_3(y^{-1} + c)^{-1})/m\right) \right|.$$

Hence, the transformation $z \equiv y^{-1} \pmod{m}$ yields the desired result. □

3. EXPONENTIAL SUMS

For integers u, v, w , and $\alpha \geq 1$ an *exponential sum* is defined by

$$S(u, v, w; a; 2^\alpha) = \sum_{z \in \mathbb{Z}_{2^\alpha}^*} e\left((uz^{-1} + vaz + w(z+c)^{-1})/2^\alpha\right),$$

where $a, c \in \mathbb{Z}$ with $a \equiv 1 \pmod{4}$ and $c \equiv 2 \pmod{4}$. Some relevant properties of these sums are collected in the following three lemmas. First, a short calculation yields

$$|S(u, v, w; a; 4)| = \begin{cases} 2 & \text{for } u + v + w \equiv 0 \pmod{2}, \\ 0 & \text{for } u + v + w \not\equiv 0 \pmod{2}, \end{cases}$$

and

$$|S(u, v, w; a; 8)| = \begin{cases} 4 & \text{for } u + v + w \equiv 0 \pmod{4}, \\ 0 & \text{for } u + v + w \not\equiv 0 \pmod{4}. \end{cases}$$

Lemma 6. *Let u, v, w, α be integers.*

(a) *If $u \equiv v \equiv w \equiv 0 \pmod{2}$ and $\alpha \geq 2$, then*

$$S(u, v, w; a; 2^\alpha) = 2 S(u/2, v/2, w/2; a; 2^{\alpha-1}).$$

(b) If $u - v + w \not\equiv 0 \pmod{4}$ and $\alpha \geq 4$, then

$$S(u, v, w; a; 2^\alpha) = 0.$$

(c) If $v \equiv 0 \pmod{2}$, $u - v + w \not\equiv 0 \pmod{8}$, and $\alpha \geq 5$, then

$$S(u, v, w; a; 2^\alpha) = 0.$$

Proof. (a) It follows at once from $u \equiv v \equiv w \equiv 0 \pmod{2}$ that

$$\begin{aligned} S(u, v, w; a; 2^\alpha) &= 2 \sum_{z \in \mathbb{Z}_{2^{\alpha-1}}^*} e\left((uz^{-1} + vaz + w(z+c)^{-1})/2^\alpha\right) \\ &= 2S(u/2, v/2, w/2; a; 2^{\alpha-1}). \end{aligned}$$

(b) A short calculation shows that

$$\begin{aligned} S(u, v, w; a; 2^\alpha) &= \sum_{z \in \mathbb{Z}_{2^{\alpha-2}}^*} \sum_{\zeta \in \mathbb{Z}_4} e\left((u(z + 2^{\alpha-2}\zeta)^{-1} + va(z + 2^{\alpha-2}\zeta) + w(z + c + 2^{\alpha-2}\zeta)^{-1})/2^\alpha\right) \\ &= \sum_{z \in \mathbb{Z}_{2^{\alpha-2}}^*} \sum_{\zeta \in \mathbb{Z}_4} e\left((u(z^{-1} - 2^{\alpha-2}\zeta) + v(az + 2^{\alpha-2}\zeta) + w((z+c)^{-1} - 2^{\alpha-2}\zeta))/2^\alpha\right) \\ &= \sum_{z \in \mathbb{Z}_{2^{\alpha-2}}^*} e\left((uz^{-1} + vaz + w(z+c)^{-1})/2^\alpha\right) \sum_{\zeta \in \mathbb{Z}_4} e\left(- (u - v + w)\zeta/4\right) = 0. \end{aligned}$$

(c) If $u - v + w \not\equiv 0 \pmod{4}$, then $S(u, v, w; a; 2^\alpha) = 0$ follows from part (b). Hence, $u - v + w \equiv 4 \pmod{8}$ can be assumed, which implies that $u + w \equiv 0 \pmod{2}$. Then a short calculation yields

$$\begin{aligned} S(u, v, w; a; 2^\alpha) &= \sum_{z \in \mathbb{Z}_{2^{\alpha-3}}^*} \sum_{\zeta \in \mathbb{Z}_8} e\left((u(z + 2^{\alpha-3}\zeta)^{-1} + va(z + 2^{\alpha-3}\zeta) + w(z + c + 2^{\alpha-3}\zeta)^{-1})/2^\alpha\right) \\ &= \sum_{z \in \mathbb{Z}_{2^{\alpha-3}}^*} \sum_{\zeta \in \mathbb{Z}_8} e\left((u(z^{-1} - 2^{\alpha-3}\zeta + 2^{2\alpha-6}\zeta^2) + v(az + 2^{\alpha-3}\zeta) \right. \\ &\quad \left. + w((z+c)^{-1} - 2^{\alpha-3}\zeta + 2^{2\alpha-6}\zeta^2))/2^\alpha\right) \\ &= \sum_{z \in \mathbb{Z}_{2^{\alpha-3}}^*} e\left((uz^{-1} + vaz + w(z+c)^{-1})/2^\alpha\right) \sum_{\zeta \in \mathbb{Z}_8} e\left(- (u - v + w)\zeta/8\right) = 0, \end{aligned}$$

which completes the proof. □

Lemma 7. Let u, v, w, α be integers with $u \equiv w \equiv 1 \pmod{2}$, $v \equiv 0 \pmod{4}$, $u - v + w \equiv 0 \pmod{8}$, and $\alpha \geq 5$. Then

$$|S(u, v, w; a; 2^\alpha)| = 2^{(\alpha+2)/2}.$$

Proof. Let $\beta = \lceil(\alpha - 3)/2\rceil$ and observe that $4\beta \geq \alpha$ for $\beta \geq 2$. Hence, straightforward calculations show that

$$\begin{aligned} S(u, v, w; a; 2^\alpha) &= \sum_{x \in \mathbb{Z}_{2^\beta}^*} \sum_{y \in \mathbb{Z}_{2^{\alpha-\beta}}} e\left(\frac{(u(x + 2^\beta y)^{-1} + va(x + 2^\beta y) + w(x + c + 2^\beta y)^{-1})}{2^\alpha}\right) \\ &= \sum_{x \in \mathbb{Z}_{2^\beta}^*} \sum_{y \in \mathbb{Z}_{2^{\alpha-\beta}}} e\left(\frac{(u(x^{-1} - 2^\beta x^{-2}y + 2^{2\beta}xy^2 - 2^{3\beta}y^3 + 2^{4\beta}y^4 - 2^{5\beta}y^5) \right. \\ &\quad \left. + va(x + 2^\beta y) + w((x + c)^{-1} - 2^\beta(x + c)^{-2}y \right. \\ &\quad \left. + 2^{2\beta}(x + c)y^2 - 2^{3\beta}y^3 - 2^{4\beta}y^4 - 2^{5\beta}y^5))}{2^\alpha}\right) \\ &= \sum_{x \in \mathbb{Z}_{2^\beta}^*} e\left(\frac{(ux^{-1} + vax + w(x + c)^{-1})}{2^\alpha}\right) \sum_{y \in \mathbb{Z}_{2^{\alpha-\beta}}} e\left(\frac{(-(ux^{-2} - va + w(x + c)^{-2})y \right. \\ &\quad \left. + 2^\beta(ux + w(x + c))y^2 - 2^{2\beta}(u + w)y^3 + 2^{3\beta+1}y^4)}{2^{\alpha-\beta}}\right) \\ &= \sum_{x \in \mathbb{Z}_{2^\beta}^*} e\left(\frac{(ux^{-1} + vax + w(x + c)^{-1})}{2^\alpha}\right) \mathbf{S}(x), \end{aligned}$$

where the abbreviation

$$\begin{aligned} \mathbf{S}(x) &= \sum_{y \in \mathbb{Z}_{2^{\alpha-\beta}}} e\left(\frac{(-(ux^{-2} - va + w(x + c)^{-2} + 2^{2\beta}(u + w) + 2^{3\beta+1})y \right. \\ &\quad \left. + 2^\beta(ux + w(x + c))y^2)}{2^{\alpha-\beta}}\right) \end{aligned}$$

has been used. Since $\gcd(2^\beta(ux + w(x + c)), 2^{\alpha-\beta}) = 2^{\beta+1}$ and $\beta + 1 \leq \alpha - \beta - 2$, it follows from [6, Lemma 6] that

$$\begin{aligned} |\mathbf{S}(x)| &= \begin{cases} 2^{(\alpha+2)/2} & \text{for } ux^{-2} - va + w(x + c)^{-2} \equiv 0 \pmod{2^{\beta+2}}, \\ 0 & \text{for } ux^{-2} - va + w(x + c)^{-2} \not\equiv 0 \pmod{2^{\beta+2}}, \end{cases} \\ &= \begin{cases} 2^{(\alpha+2)/2} & \text{for } P(x) \equiv 0 \pmod{2^{\beta+2}}, \\ 0 & \text{for } P(x) \not\equiv 0 \pmod{2^{\beta+2}}, \end{cases} \end{aligned}$$

where $P(x) = u(x + c)^2 - vax^2(x + c)^2 + wx^2$ for $x \in \mathbb{Z}$. Now, Lemma 4 implies that there exists exactly one integer $x \in \mathbb{Z}_{2^\beta}^*$ with $P(x) \equiv 0 \pmod{2^{\beta+2}}$, which yields the desired result. \square

Lemma 8. *Let u, v, w, α be integers with $\alpha \geq 5$.*

(a) *If $v \equiv 1 \pmod{2}$ and $u - v + w \equiv 0 \pmod{4}$, then*

$$\sum_{\substack{a \in \mathbb{Z}_{2^\alpha} \\ a \equiv 1 \pmod{4}}} |S(u, v, w; a; 2^\alpha)|^2 = 2^{2\alpha-1}.$$

(b) If $v \equiv 2 \pmod{4}$ and $u - v + w \equiv 0 \pmod{8}$, then

$$\sum_{\substack{a \in \mathbb{Z}_{2^\alpha} \\ a \equiv 1 \pmod{4}}} |S(u, v, w; a; 2^\alpha)|^2 = 2^{2\alpha}.$$

Proof. Let $\gcd(v, 4) = 2^\nu$ with $\nu \in \{0, 1\}$. Straightforward calculations show that

$$\begin{aligned} & \sum_{\substack{a \in \mathbb{Z}_{2^\alpha} \\ a \equiv 1 \pmod{4}}} |S(u, v, w; a; 2^\alpha)|^2 \\ &= \sum_{\substack{a \in \mathbb{Z}_{2^\alpha} \\ a \equiv 1 \pmod{4}}} \sum_{y, z \in \mathbb{Z}_{2^\alpha}^*} e\left(\frac{(u(z^{-1} - y^{-1}) + va(z - y) + w((z + c)^{-1} - (y + c)^{-1}))}{2^\alpha}\right) \\ &= \sum_{y, z \in \mathbb{Z}_{2^\alpha}^*} \sum_{\substack{a \in \mathbb{Z}_{2^\alpha} \\ a \equiv 1 \pmod{4}}} e\left(\frac{(uy^{-1}z^{-1}(y - z) - va(y - z) + w(y + c)^{-1}(z + c)^{-1}(y - z))}{2^\alpha}\right) \\ &= \sum_{y, z \in \mathbb{Z}_{2^\alpha}^*} e\left(\frac{(uy^{-1}z^{-1}(y - z) - v(y - z) + w(y + c)^{-1}(z + c)^{-1}(y - z))}{2^\alpha}\right) \cdot \\ & \quad \cdot \sum_{d \in \mathbb{Z}_{2^{\alpha-2}}} e\left(\frac{v(z - y)d}{2^{\alpha-2}}\right) \\ &= 2^{\alpha-2} \sum_{\substack{y, z \in \mathbb{Z}_{2^\alpha}^* \\ y \equiv z \pmod{2^{\alpha-\nu-2}}} e\left(\frac{(uy^{-1}z^{-1}(y - z) - v(y - z) + w(y + c)^{-1}(z + c)^{-1}(y - z))}{2^\alpha}\right) \\ &= 2^{\alpha-2} \sum_{\substack{y, z \in \mathbb{Z}_{2^\alpha}^* \\ y \equiv z \pmod{2^{\alpha-\nu-2}}} e\left(\frac{(uyz - v + wyz)(y - z)}{2^\alpha}\right) \\ &= 2^{\alpha-2} \sum_{\substack{y, z \in \mathbb{Z}_{2^\alpha}^* \\ y \equiv z \pmod{2^{\alpha-\nu-2}}} e\left(\frac{(u - v + w)(y - z)}{2^\alpha}\right) = 2^{2\alpha+\nu-1}, \end{aligned}$$

which yields the desired result. □

4. DISCREPANCY OF TRIPLES

In this final section, the discrepancy $D_{m/2; a, c}^{(3)}$ of the triples

$$\mathbf{x}_n = (x_n, x_{n+1}, x_{n+2}) \in [0, 1)^3, \quad 0 \leq n < m/2,$$

of successive inversive congruential pseudorandom numbers is studied. The main result of the present paper is Theorem 1, which provides an upper bound for the average value of the discrepancy of triples over the parameter a . Theorem 2 is an immediate consequence of this result. A proof is added for the sake of completeness. Finally, a lower bound for the discrepancy of triples is stated in Theorem 3.

Theorem 1. *The average value of the discrepancy $D_{m/2;a,c}^{(3)}$ of triples in the inverse congruential method over $a \in \mathbb{Z}_m$ with $a \equiv 1 \pmod{4}$ satisfies*

$$\frac{4}{m} \sum_{\substack{a \in \mathbb{Z}_m \\ a \equiv 1 \pmod{4}}} D_{m/2;a,c}^{(3)} < \frac{4(12 + 17\sqrt{2})}{31} m^{-1/2} \left(\frac{1}{\pi} \log m + \frac{7}{17} \right)^3 + \frac{6}{m}$$

for any parameter $c \equiv 2 \pmod{4}$.

Proof. First, Lemma 1 is applied with $k = 3$, $N = m/2$, $q = m$, $d = 2$, $\mathbf{c} = (1, 1, 1)$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < m/2$. This yields

$$\begin{aligned} D_{m/2;a,c}^{(3)} &\leq \frac{6}{m} + \frac{2}{m} \sum_{\mathbf{h} \in C_3(m/2)} \frac{1}{r(\mathbf{h}, m/2)} \left| \sum_{n=0}^{(m/2)-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \\ &= \frac{6}{m} + \frac{2}{m} \sum_{\mathbf{h}=(h_1,h_2,h_3) \in C_3(m/2)} \frac{1}{r(\mathbf{h}, m/2)} |S(h_1, h_2, h_3; a; m)| \\ &= \frac{6}{m} + \frac{2}{m} \sum_{\nu=0}^{\omega-2} \sum_{\substack{\mathbf{h}=(h_1,h_2,h_3) \in C_3(m/2) \\ \gcd(h_1,h_2,h_3,m)=2^\nu}} \frac{1}{r(\mathbf{h}, m/2)} |S(h_1, h_2, h_3; a; m)| \\ &= \frac{6}{m} + \frac{2}{m} \sum_{\nu=0}^{\omega-2} 2^\nu \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ \gcd(g_1,g_2,g_3,2)=1}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})|, \end{aligned}$$

where the second step follows from Lemma 5 and in the last step Lemma 6(a) was applied. Straightforward calculations show that

$$\begin{aligned} &\frac{2}{m} 2^{\omega-2} \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2) \\ \gcd(g_1,g_2,g_3,2)=1}} \frac{1}{r(2^{\omega-2} \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 4)| \\ &= \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2) \\ g_1+g_2+g_3 \equiv 0 \pmod{2}}} \frac{1}{r(2^{\omega-2} \mathbf{g}, m/2)} = \frac{3}{(r(m/4, m/2))^2} = \frac{12}{m^2}, \end{aligned}$$

$$\begin{aligned} &\frac{2}{m} 2^{\omega-3} \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(4) \\ \gcd(g_1,g_2,g_3,2)=1}} \frac{1}{r(2^{\omega-3} \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 8)| \\ &= \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(4) \\ \gcd(g_1,g_2,g_3,2)=1 \\ g_1+g_2+g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^{\omega-3} \mathbf{g}, m/2)} \\ &= 6 \left(1 + \frac{1}{r(m/4, m/2)} \right) \frac{1}{(r(m/8, m/2))^2} = \frac{48}{m^2} + \frac{96}{m^3}, \end{aligned}$$

and

$$\begin{aligned} & \frac{2}{m} 2^{\omega-4} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(8) \\ \gcd(g_1, g_2, g_3, 2)=1}} \frac{1}{r(2^{\omega-4} \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 16)| \\ & \leq \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(8) \\ \gcd(g_1, g_2, g_3, 2)=1 \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^{\omega-4} \mathbf{g}, m/2)} \\ & = 6 \left(1 + \frac{2}{r(m/8, m/2)} + \frac{1}{r(m/4, m/2)} \right) \left(\frac{1}{r(m/16, m/2)} + \frac{1}{r(3m/16, m/2)} \right)^2 \\ & = \frac{96(2 + \sqrt{2})}{m^2} + \frac{192(6 + 5\sqrt{2})}{m^3}, \end{aligned}$$

which implies that

$$\begin{aligned} D_{m/2; a, c}^{(3)} & \leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\ & \quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 0 \pmod{4} \\ \gcd(g_1, g_3, 2)=1}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \\ & \quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 2 \pmod{4} \\ \gcd(g_1, g_3, 2)=1}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \\ & \quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})|. \end{aligned}$$

Now, it follows from Lemma 6(b,c) that

$$\begin{aligned} D_{m/2; a, c}^{(3)} & \leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\ & \quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \\ & \quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 2 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \\ & \quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})|. \end{aligned}$$

Hence, Lemma 7 can be used in order to obtain

$$\begin{aligned}
 D_{m/2;a,c}^{(3)} &\leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 2 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \\
 &\quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})|.
 \end{aligned}$$

Therefore the average value of the discrepancy $D_{m/2;a,c}^{(3)}$ over all $a \in \mathbb{Z}_m$ with $a \equiv 1 \pmod{4}$ satisfies

$$\begin{aligned}
 \frac{4}{m} \sum_{\substack{a \in \mathbb{Z}_m \\ a \equiv 1 \pmod{4}}} D_{m/2;a,c}^{(3)} &\leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 2 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \cdot \\
 &\quad \cdot \left(\frac{1}{2^{\omega-\nu-2}} \sum_{\substack{a \in \mathbb{Z}_{2^{\omega-\nu}} \\ a \equiv 1 \pmod{4}}} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \right) \\
 &\quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1,g_2,g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \cdot \\
 &\quad \cdot \left(\frac{1}{2^{\omega-\nu-2}} \sum_{\substack{a \in \mathbb{Z}_{2^{\omega-\nu}} \\ a \equiv 1 \pmod{4}}} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})| \right)
 \end{aligned}$$

$$\begin{aligned}
 &\leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 2 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \cdot \\
 &\quad \cdot \sqrt{\frac{1}{2^{\omega-\nu-2}} \sum_{\substack{a \in \mathbb{Z}_{2^{\omega-\nu}} \\ a \equiv 1 \pmod{4}}} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})|^2} \\
 &\quad + \frac{2}{m} \sum_{\nu=0}^{\omega-5} 2^\nu \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \cdot \\
 &\quad \cdot \sqrt{\frac{1}{2^{\omega-\nu-2}} \sum_{\substack{a \in \mathbb{Z}_{2^{\omega-\nu}} \\ a \equiv 1 \pmod{4}}} |S(g_1, g_2, g_3; a; 2^{\omega-\nu})|^2},
 \end{aligned}$$

where in the last step the Cauchy–Schwarz inequality was applied. Now, Lemma 8 can be used in order to obtain

$$\begin{aligned}
 \frac{4}{m} \sum_{\substack{a \in \mathbb{Z}_m \\ a \equiv 1 \pmod{4}}} D_{m/2; a, c}^{(3)} &\leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 2 \pmod{4} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{2\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)}
 \end{aligned}$$

$$\begin{aligned}
 &= \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv g_3 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{2\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2} \\ g_1 - g_2 + g_3 \equiv 0 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &= \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv 1 \pmod{2} \\ g_2 \equiv 0 \pmod{2} \\ g_3 \equiv g_2 - g_1 \pmod{8}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &\quad + \frac{4\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{\nu/2} \sum_{\substack{\mathbf{g}=(g_1, g_2, g_3) \in C_3(2^{\omega-\nu-1}) \\ g_1 \equiv 0 \pmod{2} \\ g_2 \equiv 1 \pmod{2} \\ g_3 \equiv g_2 - g_1 \pmod{4}}} \frac{1}{r(2^\nu \mathbf{g}, m/2)} \\
 &= \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &\quad + \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \sum_{\substack{g_2 \in C_1(2^{\omega-\nu-1}) \cup \{0\} \\ g_2 \equiv 0 \pmod{2}}} \frac{1}{r(2^\nu g_2, m/2)} \\
 &\quad \cdot \sum_{\substack{g_1 \in C_1(2^{\omega-\nu-1}) \\ g_1 \equiv 1 \pmod{2}}} \frac{1}{r(g_1, 2^{\omega-\nu-1})} \sum_{\substack{g_3 \in C_1(2^{\omega-\nu-1}) \\ g_3 \equiv g_2 - g_1 \pmod{8}}} \frac{1}{r(g_3, 2^{\omega-\nu-1})} \\
 &\quad + \frac{4\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \sum_{\substack{g_1 \in C_1(2^{\omega-\nu-1}) \cup \{0\} \\ g_1 \equiv 0 \pmod{2}}} \frac{1}{r(2^\nu g_1, m/2)} \\
 &\quad \cdot \sum_{\substack{g_2 \in C_1(2^{\omega-\nu-1}) \\ g_2 \equiv 1 \pmod{2}}} \frac{1}{r(g_2, 2^{\omega-\nu-1})} \sum_{\substack{g_3 \in C_1(2^{\omega-\nu-1}) \\ g_3 \equiv g_2 - g_1 \pmod{4}}} \frac{1}{r(g_3, 2^{\omega-\nu-1})} .
 \end{aligned}$$

Hence, it follows from Lemma 3 that

$$\begin{aligned}
 \frac{4}{m} \sum_{\substack{a \in \mathbb{Z}_m \\ a \equiv 1 \pmod{4}}} D_{m/2;a,c}^{(3)} &\leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &+ \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \sum_{\substack{g_2 \in C_1(2^{\omega-\nu-1}) \cup \{0\} \\ g_2 \equiv 0 \pmod{2}}} \frac{1}{r(2^\nu g_2, m/2)} \cdot \\
 &\cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1}{4\pi} \log 2^{\omega-\nu-1} + \frac{1}{6} \right) \\
 &+ \frac{4\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \sum_{\substack{g_1 \in C_1(2^{\omega-\nu-1}) \cup \{0\} \\ g_1 \equiv 0 \pmod{2}}} \frac{1}{r(2^\nu g_1, m/2)} \cdot \\
 &\cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1}{2\pi} \log 2^{\omega-\nu-1} + \frac{2}{15} \right) \\
 &= \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &+ \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \left(1 + 2^{-\nu-1} \sum_{h \in C_1(2^{\omega-\nu-2})} \frac{1}{r(h, 2^{\omega-\nu-2})} \right) \cdot \\
 &\cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1}{4\pi} \log 2^{\omega-\nu-1} + \frac{1}{6} \right) \\
 &+ \frac{4\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \left(1 + 2^{-\nu-1} \sum_{h \in C_1(2^{\omega-\nu-2})} \frac{1}{r(h, 2^{\omega-\nu-2})} \right) \cdot \\
 &\cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1}{2\pi} \log 2^{\omega-\nu-1} + \frac{2}{15} \right) \\
 &< \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
 &+ \frac{4}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \left(1 + 2^{-\nu} \left(\frac{1}{\pi} \log 2^{\omega-\nu-2} + \frac{1}{5} \right) \right) \cdot \\
 &\cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1}{4\pi} \log 2^{\omega-\nu-1} + \frac{1}{6} \right) \\
 &+ \frac{4\sqrt{2}}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \left(1 + 2^{-\nu} \left(\frac{1}{\pi} \log 2^{\omega-\nu-2} + \frac{1}{5} \right) \right) \cdot \\
 &\cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1}{2\pi} \log 2^{\omega-\nu-1} + \frac{2}{15} \right)
 \end{aligned}$$

$$\begin{aligned}
&= \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
&\quad + \frac{1}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \left(1 + 2^{-\nu} \left(\frac{1}{\pi} \log 2^{\omega-\nu-2} + \frac{1}{5} \right) \right) \\
&\quad \cdot \left(\frac{1}{\pi} \log 2^{\omega-\nu-1} + \frac{4}{15} \right) \left(\frac{1 + 2\sqrt{2}}{\pi} \log 2^{\omega-\nu-1} + \frac{2(5 + 4\sqrt{2})}{15} \right) \\
&\leq \frac{6}{m} + \frac{12(21 + 8\sqrt{2})}{m^2} + \frac{96(13 + 10\sqrt{2})}{m^3} \\
&\quad + \frac{1}{m^{1/2}} \sum_{\nu=0}^{\omega-5} 2^{-3\nu/2} \left(1 + 2^{-\nu} \left(\frac{1}{\pi} \log 2^{\omega-2} + \frac{1}{5} \right) \right) \\
&\quad \cdot \left(\frac{1}{\pi} \log 2^{\omega-1} + \frac{4}{15} \right) \left(\frac{1 + 2\sqrt{2}}{\pi} \log 2^{\omega-1} + \frac{2(5 + 4\sqrt{2})}{15} \right) \\
&< \frac{6}{m} + \frac{1}{m^{1/2}} \left(\sum_{\nu=0}^{\infty} (2^{-3/2})^\nu + \sum_{\nu=0}^{\infty} (2^{-5/2})^\nu \left(\frac{1}{\pi} \log m + \frac{1}{5} - \frac{\log 4}{\pi} \right) \right) \\
&\quad \cdot \left(\frac{1}{\pi} \log m + \frac{4}{15} - \frac{\log 2}{\pi} \right) \left(\frac{1 + 2\sqrt{2}}{\pi} (\log m - \log 2) + \frac{2(5 + 4\sqrt{2})}{15} \right) \\
&= \frac{6}{m} + \frac{1}{m^{1/2}} \left(\frac{2(4 + \sqrt{2})}{7} + \frac{4(8 + \sqrt{2})}{31} \left(\frac{1}{\pi} \log m + \frac{1}{5} - \frac{\log 4}{\pi} \right) \right) \\
&\quad \cdot \left(\frac{1}{\pi} \log m + \frac{4}{15} - \frac{\log 2}{\pi} \right) \left(\frac{1 + 2\sqrt{2}}{\pi} (\log m - \log 2) + \frac{2(5 + 4\sqrt{2})}{15} \right) \\
&= \frac{6}{m} + \frac{4(12 + 17\sqrt{2})}{31m^{1/2}} \left(\frac{1}{\pi} \log m + \frac{1}{5} - \frac{\log 4}{\pi} + \frac{15 + 2\sqrt{2}}{14} \right) \\
&\quad \cdot \left(\frac{1}{\pi} \log m + \frac{4}{15} - \frac{\log 2}{\pi} \right) \left(\frac{1}{\pi} \log m + \frac{2(11 + 6\sqrt{2})}{105} - \frac{\log 2}{\pi} \right) \\
&< \frac{6}{m} + \frac{4(12 + 17\sqrt{2})}{31m^{1/2}} \left(\frac{1}{\pi} \log m + \frac{7}{17} \right)^3,
\end{aligned}$$

which is the desired result. \square

Theorem 2. *Let the parameter $c \equiv 2 \pmod{4}$ be fixed. Let $0 < \alpha \leq 1$. Then there exist more than $(1 - \alpha)m/4$ values of $a \in \mathbb{Z}_m$ with $a \equiv 1 \pmod{4}$ such that the discrepancy $D_{m/2;a,c}^{(3)}$ of triples in the inversive congruential method satisfies*

$$D_{m/2;a,c}^{(3)} < \frac{1}{\alpha} \left(\frac{4(12 + 17\sqrt{2})}{31} m^{-1/2} \left(\frac{1}{\pi} \log m + \frac{7}{17} \right)^3 + \frac{6}{m} \right).$$

Proof. Subsequently, the abbreviation

$$M = \frac{4(12 + 17\sqrt{2})}{31} m^{-1/2} \left(\frac{1}{\pi} \log m + \frac{7}{17} \right)^3 + \frac{6}{m}$$

is used. Suppose that there exist at most $(1 - \alpha)m/4$ values of $a \in \mathbb{Z}_m$ with $a \equiv 1 \pmod{4}$ and $D_{m/2;a,c}^{(3)} < \alpha^{-1}M$, i.e., there exist at least $\alpha m/4$ values of $a \in \mathbb{Z}_m$ with $a \equiv 1 \pmod{4}$ and $D_{m/2;a,c}^{(3)} \geq \alpha^{-1}M$. Hence, one obtains

$$\sum_{\substack{a \in \mathbb{Z}_m \\ a \equiv 1 \pmod{4}}} D_{m/2;a,c}^{(3)} \geq \frac{Mm}{4},$$

which contradicts Theorem 1. □

Theorem 3. *The discrepancy $D_{m/2;a,c}^{(3)}$ of triples in the inversive congruential method satisfies*

$$D_{m/2;a,c}^{(3)} \geq \frac{2}{\pi + 2} m^{-1/2}$$

for any parameters $a \equiv 1 \pmod{4}$ and $c \equiv 2 \pmod{4}$.

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

$$D_{m/2;a,c}^{(3)} \geq \frac{1}{(\pi + 2)m} \left| \sum_{n=0}^{(m/2)-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = \frac{1}{(\pi + 2)m} |S(1, 0, -1; a; m)|,$$

where in the second step Lemma 5 has been used. Hence, it follows from Lemma 7 that

$$D_{m/2;a,c}^{(3)} \geq \frac{1}{(\pi + 2)m} 2^{(\omega+2)/2} = \frac{2}{\pi + 2} m^{-1/2},$$

which completes the proof. □

Theorem 1 shows that for any parameter c the discrepancy $D_{m/2;a,c}^{(3)}$, on the average over the parameter a , has an order of magnitude at most $m^{-1/2}(\log m)^3$. In particular, this upper bound for the average value is independent of the specific choice of the parameter c in the inversive congruential method, provided the condition $c \equiv 2 \pmod{4}$ is met. Theorem 3 implies that the upper bound for the average value is best possible up to the logarithmic factor, since the discrepancy $D_{m/2;a,c}^{(3)}$ of any inversive congruential generator with $a \equiv 1 \pmod{4}$ and $c \equiv 2 \pmod{4}$ has an order of magnitude at least $m^{-1/2}$. Altogether, these results show that the average value of the discrepancy of triples is of an order of magnitude between $m^{-1/2}$ and $m^{-1/2}(\log m)^3$, which fits the law of the iterated logarithm for the discrepancy of true random points in $[0, 1]^3$ shown in [10]. Theorem 2 provides even more information, since it implies that for any parameter c only an arbitrarily small percentage of the parameters a may lead to a discrepancy of triples with an order of magnitude greater than $m^{-1/2}(\log m)^3$. In this connection, it should be mentioned that according to a recent result in [9] it can happen that for certain parameters a and c the discrepancy of triples is at least of the order of magnitude $m^{-1/3}$, which is too large to fit the law of the iterated logarithm. Thus, the parameters in the inversive congruential method with power of two modulus have to be chosen with some care.

ACKNOWLEDGMENT

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

REFERENCES

1. J. Eichenauer, J. Lehn, and A. Topuzoğlu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51** (1988), 757–759. MR **89i**:65007
2. J. Eichenauer–Herrmann, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
3. ———, *Pseudorandom number generation by nonlinear methods*, Internat. Statist. Rev. **63** (1995), 247–255.
4. ———, *Equidistribution properties of inversive congruential pseudorandom numbers with power of two modulus*, Metrika **44** (1996), 199–205. CMP 97:04
5. ———, *Improved upper bounds for the discrepancy of pairs of inversive congruential pseudorandom numbers with power of two modulus*, Preprint.
6. J. Eichenauer–Herrmann and H. Niederreiter, *On the discrepancy of quadratic congruential pseudorandom numbers*, J. Comput. Appl. Math. **34** (1991), 243–249. MR **92c**:65010
7. ———, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus*, Math. Comp. **58** (1992), 775–779. MR **92i**:65018
8. ———, *Kloosterman–type sums and the discrepancy of nonoverlapping pairs of inversive congruential pseudorandom numbers*, Acta Arith. **65** (1993), 185–194. MR **94f**:11071
9. ———, *Lower bounds for the discrepancy of triples of inversive congruential pseudorandom numbers with power of two modulus*, Monatsh. Math. (to appear).
10. 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. MR **24**:A1732
11. P. L’Ecuyer, *Uniform random number generation*, Ann. Oper. Res. **53** (1994), 77–120. MR **95k**:65007
12. R. Lidl and H. Niederreiter, *Finite fields*, Addison–Wesley, Reading, MA, 1983. MR **86c**:11106
13. H. Niederreiter, *Pseudo–random numbers and optimal coefficients*, Adv. Math. **26** (1977), 99–181. MR **57**:16238
14. ———, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144. MR **90e**:65008
15. ———, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345. MR **92h**:65010
16. ———, *Random number generation and quasi–Monte Carlo methods*, SIAM, Philadelphia, PA, 1992. MR **93h**:65008
17. ———, *New developments in uniform pseudorandom number and vector generation*, Monte Carlo and Quasi–Monte Carlo Methods in Scientific Computing (H. Niederreiter and P.J.-S. Shiue, eds.), Lecture Notes in Statistics, vol. 106, Springer, New York, 1995, pp. 87–120.

FACHBEREICH MATHEMATIK, TECHNISCHE HOCHSCHULE, SCHLOSSGARTENSTRASSE 7, D–64289 DARMSTADT, GERMANY

INSTITUT FÜR INFORMATIONSVERARBEITUNG, ÖSTERR. AKADEMIE DER WISSENSCHAFTEN, SONNENFELSGASSE 19, A–1010 WIEN, AUSTRIA

E-mail address: `niederreiter@oeaw.ac.at`