MATHEMATICS OF COMPUTATION
VOLUME 52, NUMBER 185
JANUARY 1989, PAGES 135-144

The Serial Test for Congruential Pseudorandom Numbers Generated by Inversions

By Harald Niederreiter

Abstract. Two types of congruential pseudorandom number generators based on inversions were introduced recently. We analyze the statistical independence properties of these pseudorandom numbers by means of the serial test. The results show that these pseudorandom numbers perform satisfactorily under the serial test. The methods of proof rely heavily on bounds for character sums such as the Weil-Stepanov bound for character sums over finite fields.

1. Introduction. A standard method of generating uniform pseudorandom numbers in the interval $[0,1)$ is the linear congruential method. For a large modulus m a sequence $y_0, y_1, \ldots$ of integers in $[0,m)$ is generated by the linear recursion $y_{n+1} \equiv \lambda y_n + r \bmod m$ for $n = 0,1,\ldots$, where λ and r are suitable integers. Then linear congruential pseudorandom numbers are obtained by the normalization $x_n = y_n/m$. If the parameters in this method are chosen appropriately, then linear congruential pseudorandom numbers have attractive statistical independence properties [6], [7], [9]. However, the linearity of the recursion yields an undesirable lattice structure of these pseudorandom numbers [4, Chapter 3], and this feature can render them useless for certain simulation purposes [2]. This state of affairs provided the motivation for several recent proposals of nonlinear congruential generators [1], [2], [3].

We consider here the case where nonlinearity is achieved by using the operation of inversion modulo m. Two types of generators that were introduced recently are based on this approach, one by Eichenauer and Lehn [2] with prime modulus m, and one by Eichenauer, Lehn, and Topuzoğlu [3] with m a power of 2. The detailed descriptions of these generators will be given in Sections 2 and 3, respectively. The papers [2], [3] contain a discussion of the periodicity properties of these generators, but no theoretical statistical analysis. The lattice structure of the generator with prime modulus is investigated in [1], [11].

In the present paper we study statistical independence properties of the pseudorandom numbers obtained from the two types of generators mentioned above. A reliable test for the statistical independence of successive terms in a sequence of uniform pseudorandom numbers is the *serial test* [4, Chapter 3], [7]. For a given dimension $k \geq 2$ and for N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0,1)^k$ we define the *discrepancy*

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

Received March 1, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C10; Secondary 11K38, 11K45.

where the supremum is extended over all subintervals J of $[0,1)^k$, $F_N(J)$ is N^{-1} times the number of terms among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the k-dimensional volume of J. If $x_0, x_1, \ldots$ is a sequence of uniform pseudorandom numbers in $[0,1)$ which is purely periodic with period length τ, then we consider the points

$$\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+k-1}) \in [0,1)^k \quad \text{for } n = 0, 1, \ldots, \tau - 1$$

and we write

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

for their discrepancy. The pseudorandom numbers x_n pass the k-dimensional serial test (over the full period) if $D_\tau^{(k)}$ is small.

We establish upper bounds for the discrepancy $D_\tau^{(k)}$ in the case where $x_0, x_1, \ldots$ are pseudorandom numbers obtained from a congruential generator based on inversions. It should be noted that upper bounds for $D_\tau^{(k)}$ yield error bounds for quasi-Monte Carlo integration [7, Section 2] and upper bounds for statistical quantities such as serial correlation coefficients [8]. Results on the serial test for other nonlinear congruential generators have been obtained in [10].

2. Prime Modulus. We first describe the generator introduced by Eichenauer and Lehn [2] for a prime modulus $p \geq 5$. It will be convenient to identify the set $F_p = \{0, 1, \ldots, p-1\}$ of integers with the finite field of order p. For $c \in F_p$, $c \neq 0$, let $\bar{c}$ be the multiplicative inverse of c in F_p, and put $\bar{0} = 0$. Choose $a, b \in F_p$ with $ab \neq 0$ in such a way that $x^2 - bx - a$ is a primitive polynomial over F_p in the sense of [5, Definition 3.15]. Now generate a sequence $y_0, y_1, \ldots$ of elements of F_p by the recursion

$$y_{n+1} \equiv a\bar{y}_n + b \bmod p \quad \text{for } n = 0, 1, \ldots. \tag{1}$$

It was shown in [2] that the sequence $y_0, y_1, \ldots$ is purely periodic with period length p and that $\{y_0, y_1, \ldots, y_{p-1}\} = F_p$. We derive a sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers by setting $x_n = y_n/p$.

We collect some preparatory results. For integers $m \geq 2$ and $k \geq 1$ let $C_k(m)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbb{Z}^k$ with $-m/2 < h_j \leq m/2$ for $1 \leq j \leq k$. We put

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

and for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(m)$ we define

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

For real t we write $e(t) = e^{2\pi i t}$. Furthermore, $\mathbf{x} \cdot \mathbf{y}$ denotes the standard inner product of $\mathbf{x}, \mathbf{y} \in \mathbb{R}^k$. The following two lemmas are from [6, Section 2].

LEMMA 1. *Let $m \geq 2$ be an integer and let $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1} \in \mathbb{Z}^k$, $k \geq 2$, be lattice points all of whose coordinates are in $[0, m)$. Then the discrepancy of the*

points $\mathbf{t}_n = m^{-1}\mathbf{y}_n$, $0 \le n \le N-1$, *satisfies*

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

LEMMA 2. *For any integer* $m \ge 2$ *we have*

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

We also need bounds for certain character sums over the finite field F_p. Let χ be the canonical additive character of F_p defined by $\chi(n) = e(n/p)$ for $n \in F_p$. The following lemma is a special case of a classical result of Weil [14] (see also Stepanov [13] for a proof that does not use algebraic geometry).

LEMMA 3. *For polynomials* $Q, R \in F_p[x]$ *with* $1 \le \deg(R) < \deg(Q) < p$ *we have*

$$\left| \sum_{\substack{n \in F_p \\ R(n) \ne 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| \le \left(r - 2 + \sum_{i=1}^{r} m_i\right) p^{1/2},$$

where r *is the number of distinct poles of* Q/R *in the algebraic closure* $\overline{F}_p$ *(including the point at infinity) and* $m_1, \ldots, m_r$ *are the multiplicities of the poles.*

THEOREM 1. *For pseudorandom numbers derived from the generator* (1) *and for* $2 \le k < p$ *we have*

$$D_p^{(k)} < 2p^{-1/2} \left(\frac{2}{\pi} \log p + \frac{7}{5}\right)^{k-1} \left(\frac{2k-2}{\pi} \log p + \frac{2k-7}{5}\right) + 2p^{-1/2}$$
$$+ \frac{1}{p} \left(\frac{2}{\pi} \log p + \frac{7}{5}\right)^{k-1} \left(\frac{2k-2}{\pi} \log p + \frac{12k-7}{5}\right).$$

Proof. Let $\psi\colon F_p \to F_p$ be defined by $\psi(n) = a\bar{n} + b$ for $n \in F_p$ and let ψ^j be the jth iterate of ψ, with $\psi^0(n) = n$. Then

$$\{(y_n, y_{n+1}, \ldots, y_{n+k-1})\colon 0 \le n \le p-1\}$$
$$= \{(\psi^0(n), \psi^1(n), \ldots, \psi^{k-1}(n))\colon 0 \le n \le p-1\},$$

and so Lemma 1 yields

$$D_p^{(k)} \le \frac{k}{p} + \frac{1}{p} \sum_{\mathbf{h} \in C_k(p)} \frac{1}{r(\mathbf{h}, p)} |S(\mathbf{h})|, \tag{2}$$

where for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(p)$ we have

$$S(\mathbf{h}) = \sum_{n \in F_p} \chi\left(\sum_{j=1}^{k} h_j \psi^{j-1}(n)\right).$$

For fixed $\mathbf{h} \in C_k(p)$ let m be the number of nonzero coordinates in $\mathbf{h}$; then $1 \le m \le k$. If $m = 1$, then since each ψ^j is a permutation of F_p, we get $S(\mathbf{h}) = 0$. If

$2 \le m \le k$, let $1 \le i_1 < i_2 < \cdots < i_m \le k$ be such that $h_{i_1} \ne 0$, $h_{i_2} \ne 0, \ldots, h_{i_m} \ne 0$. Then

$$S(\mathbf{h}) = \sum_{n \in F_p} \chi\left(\sum_{t=1}^{m} h_{i_t} \psi^{i_t - 1}(n)\right) = \sum_{n \in F_p} \chi\left(\sum_{t=1}^{m} h_{i_t} \psi^{i_t - i_1}(n)\right), \tag{3}$$

where we introduced the new summation variable $\psi^{i_1-1}(n)$ and called it again n. Let $c_j \in F_p$ be defined by $c_0 = 0$, $c_1 = 1$, $c_{j+2} = bc_{j+1} + ac_j$ for $j \ge 0$. Since $x^2 - bx - a$ is primitive over F_p, we have $c_j \ne 0$ for $1 \le j \le p$ by [2, p. 321]. By induction one shows that for $1 \le j \le p$ we have

$$\psi^j(n) = \frac{nc_{j+1} + ac_j}{nc_j + ac_{j-1}},$$

where $n \ne -ac_{i-1}\bar{c}_i$ for $1 \le i \le j$. We introduce the rational function

$$\frac{Q(x)}{R(x)} = h_{i_1} x + \sum_{t=2}^{m} h_{i_t} \frac{xc_{i_t - i_1 + 1} + ac_{i_t - i_1}}{xc_{i_t - i_1} + ac_{i_t - i_1 - 1}}$$

with

$$R(x) = \prod_{t=2}^{m} (xc_{i_t - i_1} + ac_{i_t - i_1 - 1}).$$

Then we get from (3),

$$|S(\mathbf{h})| \le i_m - i_1 + \left| \sum_{n \in F_p}^{*} \chi\left(\frac{Q(n)}{R(n)}\right) \right|, \tag{4}$$

where the asterisk indicates that $n \ne -ac_{i-1}\bar{c}_i$ for $1 \le i \le i_m - i_1$. We note that for all $j \ge 0$ we have

$$\begin{pmatrix} c_{j+1} \\ c_{j+2} \end{pmatrix} = A \begin{pmatrix} c_j \\ c_{j+1} \end{pmatrix} \quad \text{with } A = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}.$$

We claim that the elements $-ac_{i-1}\bar{c}_i$, $1 \le i \le p$, are all distinct. For otherwise there exist $1 \le r < s \le p$ and $d \in F_p$ such that

$$\begin{pmatrix} c_{s-1} \\ c_s \end{pmatrix} = d \begin{pmatrix} c_{r-1} \\ c_r \end{pmatrix},$$

or equivalently

$$A^{s-1} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = dA^{r-1} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Premultiplying by A^{1-r}, we get

$$\begin{pmatrix} c_{s-r} \\ c_{s-r+1} \end{pmatrix} = \begin{pmatrix} 0 \\ d \end{pmatrix},$$

hence $c_{s-r} = 0$, a contradiction. Going back to (4), we obtain

$$|S(\mathbf{h})| \le 2(i_m - i_1) - (m-1) + \left| \sum_{\substack{n \in F_p \\ R(n) \ne 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right|.$$

Now Q/R has at most $\deg(R) = m - 1$ finite poles, and since $\deg(Q) = \deg(R) + 1$, it has a pole at the point at infinity with multiplicity 1. Furthermore, we have

$\deg(R) < \deg(Q) = m \le k < p$, so that we can apply Lemma 3. Using also $i_m - i_1 \le k - 1$, we obtain

$$|S(\mathbf{h})| \le (2m-2)p^{1/2} + 2k - m - 1.$$

This implies

$$\begin{aligned}\Sigma &:= \sum_{\mathbf{h}\in C_k(p)} \frac{1}{r(\mathbf{h},p)}|S(\mathbf{h})| \\ &\le \sum_{m=2}^{k} \sum_{1\le i_1<i_2<\cdots<i_m\le k} \left(\sum_{h\in C_1(p)} \frac{1}{r(h,p)}\right)^m ((2m-2)p^{1/2} + 2k - m - 1) \\ &< \sum_{m=2}^{k} \binom{k}{m} \left(\frac{2}{\pi}\log p + \frac{2}{5}\right)^m ((2m-2)p^{1/2} + 2k - m - 1),\end{aligned}$$

where we applied Lemma 2 in the last step. Simple manipulations show that

$$\begin{aligned}\Sigma < (2p^{1/2}-1) \sum_{m=1}^{k} m\binom{k}{m} \left(\frac{2}{\pi}\log p + \frac{2}{5}\right)^m - 2p^{1/2}\left(\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^k - 1\right) \\ + (2k-1)\left(\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^k - 1\right).\end{aligned}$$

For any real z we have

$$\sum_{m=1}^{k} m\binom{k}{m} z^m = kz \sum_{m=1}^{k} \binom{k-1}{m-1} z^{m-1} = kz(z+1)^{k-1},$$

therefore

$$\begin{aligned}\Sigma < 2p^{1/2}\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p + \frac{2k-7}{5}\right) + 2p^{1/2} \\ + \left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p + \frac{12k-7}{5}\right) - 2k + 1.\end{aligned}$$

Together with (2) this yields the desired result. □

3. Power of 2 Modulus. A generator analogous to (1), but with a modulus which is a power of 2, was introduced by Eichenauer, Lehn, and Topuzoğlu [3]. For $q = 2^w$, $w \ge 1$, we write G_q for the set of all odd integers c with $1 \le c < q$. For $c \in G_q$ let $\bar{c} \in G_q$ be the multiplicative inverse of c modulo q, i.e., $\bar{c}$ is the unique element of G_q with $c\bar{c} \equiv 1 \bmod q$. Now let $m = 2^w$, $w \ge 3$, be the modulus of the generator and let $a \equiv 1 \bmod 4$ and $b \equiv 2 \bmod 4$. We define a sequence $y_0, y_1, \ldots$ of elements of G_m by the recursion

$$y_{n+1} \equiv a\bar{y}_n + b \bmod m \quad \text{for } n = 0, 1, \ldots. \tag{5}$$

It was shown in [3] that under the conditions above the sequence $y_0, y_1, \ldots$ is purely periodic with period length 2^{w-1} and that $\{y_0, y_1, \ldots, y_{(m/2)-1}\} = G_m$. A sequence $x_0, x_1, \ldots$ of uniform pseudorandom numbers is derived by setting $x_n = y_n/m$. The generator (5) may also be defined for arbitrary $m \ge 2$, but it is an easy exercise in elementary number theory to show that if exactly all reduced residues mod m

(i.e., all residues coprime to m) appear in the period, then m cannot have a prime divisor ≥ 5. Powers of 2 represent the most interesting case in this class of moduli m.

We consider the 2-dimensional serial test for the full period of the pseudorandom numbers x_n. A crucial role is played by certain character sums, namely Kloosterman sums. For $q = 2^w$, $w \geq 1$, and arbitrary integers u, v we define

$$S(u,v;q) = \sum_{n \in G_q} e\left(\frac{1}{q}(un + v\bar{n})\right).$$

These Kloosterman sums were studied in detail by Salié [12]. We collect some relevant formulas from [12]:

(6) $S(u,v;q) = S(1,uv;q)$ if u odd,

(7) $S(u,v;q) = 0$ if $u + v \equiv 1 \bmod 2$,

(8) $S(u,v;q) = 2^d S\left(\frac{u}{2^d}, \frac{v}{2^d}; 2^{w-d}\right)$ if $u \equiv v \equiv 0 \bmod 2^d$ and $1 \leq d < w$,

where in (7) and (8) we assume that $w \geq 2$. For $3 \leq w \leq 5$, straightforward calculations show that

(9) $$|S(1,v;8)| = \begin{cases} 4 & \text{if } v \equiv 3 \bmod 4, \\ 0 & \text{if } v \not\equiv 3 \bmod 4, \end{cases}$$

(10) $$|S(1,v;16)| = \begin{cases} 4\sqrt{2} & \text{if } v \equiv 1 \bmod 4, \\ 0 & \text{if } v \not\equiv 1 \bmod 4, \end{cases}$$

(11) $$|S(1,v;32)| \leq \begin{cases} 8\sqrt{2+\sqrt{2}} & \text{if } v \equiv 5 \bmod 8, \\ 0 & \text{if } v \not\equiv 5 \bmod 8. \end{cases}$$

For $w \geq 6$ it follows from results of Salié [12] that

(12) $$|S(1,v;2^w)| \leq \begin{cases} 2^{(w+3)/2} & \text{if } v \equiv 1 \bmod 8, \\ 0 & \text{if } v \not\equiv 1 \bmod 8. \end{cases}$$

We also need the following bounds.

LEMMA 4. *For $t \geq 6$ and c odd we have*

(13) $$\sum_{\substack{k \in C_1(2^t) \\ k \equiv c \bmod 8}} \csc \frac{\pi|k|}{2^t} < \frac{(t+1)\log 2}{4\pi} 2^t + (0.2126)2^t,$$

and for $t \geq 3$ we have

(14) $$\sum_{\substack{k \in C_1(2^t) \\ k \text{ odd}}} \csc \frac{\pi|k|}{2^t} < \frac{(t+1)\log 2}{\pi} 2^t + (0.3024)2^t.$$

Proof. We only prove (13) since (14) can be shown similarly. It suffices to consider $c \in G_8$. We have

$$\sum_{\substack{k=1 \\ k \equiv c \bmod 8}}^{2^{t-1}} \csc \frac{\pi k}{2^t} = \sum_{h=0}^{2^{t-4}-1} \csc \frac{\pi(8h+c)}{2^t} \leq \csc \frac{\pi c}{2^t} + \int_0^{2^{t-4}-1} \csc \frac{\pi(8x+c)}{2^t}\, dx$$

$$< \csc \frac{\pi c}{2^t} + \frac{1}{\pi} 2^{t-3} \log \cot \frac{\pi c}{2^{t+1}} < \frac{2^t}{3c} + \frac{1}{\pi} 2^{t-3} \log \frac{2^{t+1}}{\pi c}.$$

Therefore,

$$\sum_{\substack{k\in C_1(2^t)\\ k\equiv c \bmod 8}} \csc\frac{\pi|k|}{2^t} = \sum_{k\equiv c \bmod 8}^{2^{t-1}} \csc\frac{\pi k}{2^t} + \sum_{k\equiv 8-c \bmod 8}^{2^{t-1}} \csc\frac{\pi k}{2^t}$$

$$< \frac{1}{\pi}2^{t-2}(\log 2^{t+1} - \log\pi) + \frac{2^t}{3c} + \frac{2^t}{3(8-c)} - \frac{1}{\pi}2^{t-3}(\log c + \log(8-c)),$$

and by calculating the maximum of this expression for $c \in G_8$ we get the desired bound. □

THEOREM 2. *For pseudorandom numbers derived from the generator* (5) *with* $m = 2^w$, $w \geq 6$, *we have*

$$D^{(2)}_{m/2} < \frac{4}{(2^{3/2}-1)\pi^2} m^{-1/2}(\log m)^2 + (1.12)m^{-1/2}\log m + (1.35)m^{-1/2} + \frac{4}{m}.$$

Proof. Since $\{y_0, y_1, \ldots, y_{(m/2)-1}\} = G_m$, we have

$$\left\{(y_n, y_{n+1}) : 0 \leq n \leq \frac{m}{2} - 1\right\} = \{(n, a\bar{n} + b) : n \in G_m\},$$

where $a\bar{n}+b$ is regarded as an element of G_m by considering it modulo m. Therefore Lemma 1 yields

$$D^{(2)}_{m/2} \leq \frac{2}{m} + \frac{2}{m}\sum_{\mathbf{h}\in C_2(m)} \frac{1}{r(\mathbf{h}, m)}|S(\mathbf{h})|, \tag{15}$$

where for $\mathbf{h} = (h_1, h_2) \in C_2(m)$ we have

$$|S(\mathbf{h})| = \left|\sum_{n\in G_m} e\left(\frac{1}{m}(h_1 n + h_2 a\bar{n} + h_2 b)\right)\right| = |S(h_1, h_2 a; m)|.$$

Now $\gcd(h_1, h_2, m) = 2^d$ with $0 \leq d \leq w-1$, so by splitting up the following sum according to the value of d we get

$$\Sigma := \sum_{\mathbf{h}\in C_2(m)} \frac{1}{r(\mathbf{h}, m)}|S(\mathbf{h})| = \sum_{d=0}^{w-1} T_d$$

with

$$T_d = \sum_{\mathbf{h}} \frac{1}{r(\mathbf{h}, m)}|S(h_1, h_2 a; m)|,$$

where the last sum is extended over all $\mathbf{h} = (h_1, h_2) \in C_2(m)$ with $\gcd(h_1, h_2, m) = 2^d$. Using (8) it follows immediately that

$$T_{w-1} = 1 + \frac{1}{2m}. \tag{16}$$

Now we consider $0 \leq d \leq w-2$. If one of $h_1/2^d$ or $h_2/2^d$ is even, then (7) and (8) imply $S(h_1, h_2 a; m) = 0$. If both $h_1/2^d$ and $h_2/2^d$ are odd, then (6) and (8) yield

$$S(h_1, h_2 a; m) = 2^d S\left(1, \frac{h_1 h_2 a}{2^{2d}}; 2^{w-d}\right).$$

Thus, writing $h_j = k_j 2^d$ for $j = 1, 2$, we obtain

$$T_d = 2^d \sum_{\substack{k_1,k_2 \in C_1(2^{w-d}) \\ k_1,k_2 \text{ odd}}} \frac{|S(1, k_1 k_2 a; 2^{w-d})|}{r(k_1 2^d, m) r(k_2 2^d, m)}. \tag{17}$$

For $0 \le d \le w-6$ we use (12) to get

$$\begin{aligned} T_d &\le 2^{(w+d+3)/2} \sum_{\substack{k_1,k_2 \in C_1(2^{w-d}) \\ k_1 k_2 \equiv a \bmod 8}} \frac{1}{r(k_1 2^d, m) r(k_2 2^d, m)} \\ &= 2^{(-3w+d+3)/2} \sum_{\substack{k_1 \in C_1(2^{w-d}) \\ k_1 \text{ odd}}} \csc \frac{\pi |k_1|}{2^{w-d}} \sum_{\substack{k_2 \in C_1(2^{w-d}) \\ k_2 \equiv a k_1 \bmod 8}} \csc \frac{\pi |k_2|}{2^{w-d}}. \end{aligned}$$

Together with (13) and (14) this yields

$$\begin{aligned} T_d &< 2^{(w-3d+3)/2} \left(\frac{\log 2}{4\pi} (w-d+1) + 0.2126 \right) \left(\frac{\log 2}{\pi} (w-d+1) + 0.3024 \right) \\ &< 2^{(w-3d+3)/2} \left(\frac{1}{4\pi^2} (\log m)^2 + (0.127) \log m + 0.1401 + (0.0122)\, d^2 \right). \end{aligned}$$

Applying the differential operator $z \frac{d}{dz}$ twice to the identity $\sum_{d=0}^{\infty} z^d = (1-z)^{-1}$, we get

$$\sum_{d=0}^{\infty} d^2 z^d = \frac{z + z^2}{(1-z)^3} \quad \text{for } |z| < 1,$$

hence

$$\sum_{d=0}^{w-6} d^2 2^{-3d/2} < \sum_{d=0}^{\infty} d^2 2^{-3d/2} = \frac{8 + 2^{3/2}}{(2^{3/2} - 1)^3}.$$

Therefore,

$$\begin{aligned} \sum_{d=0}^{w-6} T_d &< 2^{3/2} m^{1/2} \left(\frac{1}{4\pi^2} (\log m)^2 + (0.127) \log m + 0.1401 \right) \sum_{d=0}^{w-6} 2^{-3d/2} \\ &\quad + 2^{3/2} (0.0122) m^{1/2} \sum_{d=0}^{w-6} d^2 2^{-3d/2} \\ &< \left(\frac{8 m^{1/2}}{2^{3/2} - 1} - \frac{1024\sqrt{2}}{(2^{3/2} - 1) m} \right) \left(\frac{1}{4\pi^2} (\log m)^2 + (0.127) \log m + 0.1401 \right) \\ &\quad + (0.0612) m^{1/2}. \end{aligned}$$

Using $m \ge 64$, we obtain

$$\sum_{d=0}^{w-6} T_d < m^{1/2} \left(\frac{2}{(2^{3/2} - 1)\pi^2} (\log m)^2 + (0.56) \log m + 0.675 \right) - \frac{876}{m}. \tag{18}$$

For $d = w - 5$ we get from (11) and (17),

$$T_{w-5} \le 2^{-w-2} \sqrt{2 + \sqrt{2}} \sum_{\substack{k_1 \in C_1(32) \\ k_1 \text{ odd}}} \csc \frac{\pi |k_1|}{32} \sum_{\substack{k_2 \in C_1(32) \\ k_2 \equiv 5 a k_1 \bmod 8}} \csc \frac{\pi |k_2|}{32},$$

and by distinguishing between the cases $a \equiv 1 \bmod 8$ and $a \equiv 5 \bmod 8$ we find that

$$T_{w-5} < \frac{240}{m}. \tag{19}$$

Similarly, using (9), (10), and (17), we get

$$T_{w-4} < \frac{60}{m}, \qquad T_{w-3} < \frac{14}{m}. \tag{20}$$

Since $|S(1, v; 4)| = 2$ for v odd, it follows from (17) that

$$T_{w-2} = \frac{4}{m}. \tag{21}$$

By combining (16), (18), (19), (20), and (21) we get

$$\Sigma = \sum_{d=0}^{w-1} T_d < m^{1/2} \left(\frac{2}{(2^{3/2} - 1)\pi^2} (\log m)^2 + (0.56) \log m + 0.675 \right) + 1,$$

and the desired result follows now from (15). □

The method in the proof of Theorem 2 can in principle be extended to treat $D_{m/2}^{(k)}$ for $k \geq 3$, but this would require a detailed study of the corresponding exponential sums (compare with Section 2).

4. Discussion. Theorem 1 shows that for the generator (1) with prime modulus p we have $D_p^{(k)} = O(p^{-1/2}(\log p)^k)$ for $2 \leq k < p$, where the implied constant is absolute. It should be noted that this bound is independent of the specific choice of the parameters $a, b \in F_p$ (only the basic requirements that $ab \neq 0$ and $x^2 - bx - a$ is primitive over F_p have to be met). We compare this behavior under the serial test with that for linear congruential generators $y_{n+1} \equiv \lambda y_n + r \bmod p$ with prime modulus p. For these generators it is known [6, Section 3] that for every prime p and every $k \geq 2$ there is a choice of the parameters λ and r such that we get period length $p - 1$ and discrepancy $D_{p-1}^{(k)} = O(p^{-1}(\log p)^k \log\log p)$. However, the choice of these parameters depends strongly on the dimension k. Therefore, linear congruential generators perform better under the serial test than the nonlinear generator (1) if a judicious choice of parameters (which varies with k) is made, while the nonlinear generator shows a uniformly acceptable (though not excellent) behavior under the serial test for any choice of parameters satisfying the definition of the generator. On the other hand, a bad choice of parameters in the linear congruential method can lead to a behavior under the serial test that is worse than that of the nonlinear generator [7, pp. 1026–1027].

Analogous remarks apply to the generator (5) for which Theorem 2 shows that $D_{m/2}^{(2)} = O(m^{-1/2}(\log m)^2)$. For higher dimensions there are technical difficulties in this case, but it seems likely that bounds similar to those in Theorem 1 are valid.

Mathematical Institute
Austrian Academy of Sciences
Dr.-Ignaz-Seipel-Platz 2
A-1010 Vienna, Austria

1. J. EICHENAUER, H. GROTHE & J. LEHN, "Marsaglia's lattice test and non-linear congruential pseudo random number generators," *Metrika*, v. 35, 1988, pp. 241–250.

2. J. EICHENAUER & J. LEHN, "A non-linear congruential pseudo random number generator," *Statist. Papers*, v. 27, 1986, pp. 315–326.

3. J. EICHENAUER, J. LEHN & A. TOPUZOĞLU, "A nonlinear congruential pseudorandom number generator with power of two modulus," *Math. Comp.*, v. 51, 1988, pp. 757–759.

4. D. E. KNUTH, *The Art of Computer Programming*, vol. 2: *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

5. R. LIDL & H. NIEDERREITER, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

6. H. NIEDERREITER, "Pseudo-random numbers and optimal coefficients," *Adv. in Math.*, v. 26, 1977, pp. 99–181.

7. H. NIEDERREITER, "Quasi-Monte Carlo methods and pseudo-random numbers," *Bull. Amer. Math. Soc.*, v. 84, 1978, pp. 957–1041.

8. H. NIEDERREITER, "Number-theoretic problems in pseudorandom number generation," in *Proc. Sympos. on Applications of Number Theory to Numerical Analysis*, Lecture Notes No. 537, Research Inst. of Math. Sciences, Kyoto, 1984, pp. 18–28.

9. H. NIEDERREITER, "The serial test for pseudo-random numbers generated by the linear congruential method," *Numer. Math.*, v. 46, 1985, pp. 51–68.

10. H. NIEDERREITER, "Statistical independence of nonlinear congruential pseudorandom numbers," *Monatsh. Math.* (To appear.)

11. H. NIEDERREITER, "Remarks on nonlinear congruential pseudorandom numbers," *Metrika* (To appear.)

12. H. SALIÉ, "Über die Kloostermanschen Summen $S(u, v; q)$," *Math. Z.*, v. 34, 1932, pp. 91–109.

13. S. A. STEPANOV, "On estimating rational trigonometric sums with prime denominator," *Trudy Mat. Inst. Steklov.*, v. 112, 1971, pp. 346–371. (Russian)

14. A. WEIL, "On some exponential sums," *Proc. Nat. Acad. Sci. U.S.A.*, v. 34, 1948, pp. 204–207.