On the Distribution of Nonlinear Congruential Pseudorandom Numbers of Higher Orders in Residue Rings

Edwin D. El-Mahassni[1] and Domingo Gomez[2,⋆]

[1] Department of Computing, Macquarie University
North Ryde, NSW 2109, Australia
edwinelm@ics.mq.edu.au
[2] Faculty of Science, University of Cantabria
E-39071 Santander, Spain
domingo.gomez@unican.es

Abstract. The nonlinear congruential method is an attractive alternative to the classical linear congruential method for pseudorandom number generation. In this paper we present new discrepancy bounds for sequences of s-tuples of successive nonlinear congruential pseudorandom numbers of higher orders modulo a composite integer M.

1 Background

For an integer $M > 1$, we denote by $\mathbb{Z}_M$ the residue ring modulo M. In this paper we present some distribution properties of a generalization of pseudorandom number generators, first introduced in [7], defined by a recurrence

$$u_{n+1} \equiv f(g_1(u_n, \ldots, u_{n-r+1}), \ldots, g_r(u_n, \ldots, u_{n-r+1})) \pmod{M}, \quad (1)$$

where

$$f(X_1, \ldots, X_r),\ g_1(X_1, \ldots, X_r), \ldots,\ g_r(X_1, \ldots, X_r) \in \mathbb{Z}_M[X_1, \ldots, X_r]$$

for $n \geq r - 1$ with some initial values $u_0, \ldots, u_{r-1}$.

To study this pseudorandom number generator, we define the sequence of polynomials $f_k(\mathbf{X}) \in \mathbb{Z}_M[\mathbf{X}]$, with $\mathbf{X} = X_1, \ldots,\ X_r$ by the recurrence relation

$$f_k(\mathbf{X}) \equiv f_{k-1}(g_1(\mathbf{X}), \ldots, g_r(\mathbf{X})) \pmod{M}, \qquad k \geq 1 \quad (2)$$

where $f_0(\mathbf{X}) = f(\mathbf{X})$.

It is obvious that (1) becomes periodic with some period $t \leq M^r$. Throughout this paper we assume that this sequence is *purely periodic*, i.e. $u_n = u_{n+t}$ beginning with $n = 0$, otherwise we consider a shift of the original sequence.

⋆ Domingo Gomez is partially supported by the Spanish Ministry of Education and Science grant MTM20067088.

M. Bras-Amorós and T. Høholdt (Eds.): AAECC 2009, LNCS 5527, pp. 195–203, 2009.

Although the distribution of nonlinear congruential generators has been studied extensively, see [5,6,9] for instance, much less is known for its higher orders analogue. A result for a class of polynomials for prime moduli was established in [7], where this was later extended to a larger family of polynomials in [8]. In this paper we show a generalization of this result to a larger class of pseudorandom number generators.

1.1 Notation and First Results

This section begins with some notation. It will be assumed that $N,\ A_i,\ B_i$ and b_i represent integer positive numbers and $\mathbf{0}$ is the r-dimensional 0 vector. The elements of $\mathbb{Z}_M$ will be identified with the integers $\{0, \ldots,\ M-1\}$. For this reason, we can define $\mathbf{e}_M(z) = \exp(2\pi i z/M)$ for any element $z \in \mathbb{Z}_M$.

For a polynomial f, G is the gcd of the coefficients of nonconstant monomials with M.

We will denote $f^{(p)}(\mathbf{X}) \equiv f(\mathbf{X}) \pmod p$ of total degree d' for a polynomial f with integer coefficients and total degree d. Finally, we define $\deg_{X_r} f$, the degree of the coefficient X_r of the polynomial f, to be $\deg_{X_r}$ modulo every prime factor p of M.

Lemma 1. *Given a polynomial in the ring $\mathbb{Z}_M[\mathbf{X}]$,*

$$f(\mathbf{X}) \equiv \sum_{i_1=0}^{d_1} \ldots \sum_{i_r=0}^{d_r} b_{i_1,\ldots,i_r} X_1^{i_1} \ldots X_r^{i_r} \pmod M$$

with $\deg_{X_r} f \geq 1$, total degree d, then exist polynomials $h_1(X_r), \ldots,\ h_{r-1}(X_r)$ of degree less than $d(\lceil \log d \rceil + 1)$ such that

$$g^{(p)}(X_r) = f^{(p)}(a_1 + h_1^{(p)}(X_r), \ldots, a_{r-1} + h_{r-1}^{(p)}(X_r), X_r) \tag{3}$$

is a nonconstant polynomial for any $p|M$, $p \not| G$ and any values $a_1, \ldots, a_{r-1} \in \mathbb{Z}_M$.

Proof. Let $p|M$ be a prime number not dividing G and $D = \lceil \log d \rceil + 1$. By the definition of G, we note that $f^{(p)}(\mathbf{X})$ is not a constant polynomial and it can be expressed as $f^{(p)}(\mathbf{X}) = h(X_1, \ldots,\ X_{r-1}) X_r^{d'} + f'(\mathbf{X})$ where $f'(\mathbf{X})$ is a polynomial of degree stricly less than d' in X_r. If $d' = 0$ then $f^{(p)}(\mathbf{X}) = h(X_1, \ldots,\ X_{r-1})$, but in any case h is a not a constant polynomial.

Let $\mathbb{F}$ be an extension field of degree D over $\mathbb{Z}_p$. By the cardinality of $\mathbb{F}$, there exist $\xi_1, \ldots,\ \xi_{r-1} \in \mathbb{F}$ such as $h(\xi_1, \ldots,\ \xi_{r-1}) \neq 0$.

It is easy to check that

$$f^{(p)}(X_1 + \xi_1 X_r, \ldots, X_{r-1} + \xi_{r-1} X_r,\ X_r) = h(\xi_1, \ldots,\ \xi_{r-1}) X_r^{d''} + f''(\mathbf{X}) \tag{4}$$

where $d \geq d'' > 0$ and $f''(\mathbf{X})$ is a polynomial with total degree less than $d'' - 1$ in X_r. Let $\mathbf{E}$ be a extension field of degree $d+1$ over $\mathbb{F}$ and let θ be a defining element of $\mathbf{E}$ over both $\mathbb{Z}_p$ and $\mathbf{E}$, i.e. $\mathbf{E} \equiv \mathbb{Z}_p(\theta) \equiv \mathbb{F}(\theta)$.

The evaluation of the polynomial in (4)

$$f^{(p)}(a_1 + \xi_1\theta, \ldots, a_{r-1} + \xi_{r-1}\theta,\ \theta) \neq 0, \qquad a_1, \ldots,\ a_{r-1} \in \mathbb{Z}_p \tag{5}$$

because the degree of the minimal polynomial of θ over $\mathbb{F}$ is $d+1$.

For $i = 1, \ldots, r-1$, each element $\xi_i\theta$ can be expressed as $h_i^{(p)}(\theta)$, where $h_i^{(p)}(X_r) \in \mathbb{Z}_p[X_r]$. Applying the Chinese Remainder Theorem to the different polynomials $h_i^{(p)}(X_r)$ for each prime $p|M$, we find the corresponding $h_i(X_r)$. By construction, $f^{(p)}(a_1 + h_1^{(p)}(X_r), \ldots, a_{r-1} + h_{r-1}^{(p)}(X_r),\ X_r)$ is not the zero polynomial by (5) for any integer values $a_1, \ldots,\ a_{r-1}$.

Now, we proceed to define a family of polynomials depending on $g_1(\mathbf{X}),\ldots,g_r(\mathbf{X})$ which will be the main subject of the article.

Let $\mathbb{K}$ be a field. We denote by $\mathcal{T}$ as the set of polynomials, f, such that $\sum_{j=0}^{s-1} a_j\,(f_{k+j}(\mathbf{X}) - f_{l+j}(\mathbf{X}))$ is nonconstant, where $f_i(\mathbf{X})$ are defined by (2) and $a_j \in \mathbb{K}$, with at least one $a_j \neq 0$ and $k \neq l$.

Here is a sufficient condition for a certain polynomial to be in class $\mathcal{T}$. To prove the result, we need some background.

We start defining a homomorphism of polynomial rings $\phi : \mathbb{K}[X_1, \ldots,\ X_r] \to \mathbb{K}[X_1, \ldots,\ X_r]$ with $\phi(X_i) = g_i(\mathbf{X})$.

Polynomials $g_1(\mathbf{X}), \ldots,\ g_r(\mathbf{X})$ are said to be algebraically independent if the application ϕ is injective. ϕ^k denotes the composition of the function ϕ k times with ϕ^0 being the identity map.

Lemma 2. *Let $f(\mathbf{X})$ be a polynomial in $\mathbb{K}[\mathbf{X}]$ and $g_1(\mathbf{X}), \ldots,\ g_r(\mathbf{X})$ be algebraically independent and $\mathbb{F}$ be an extension field of $\mathbb{K}$. Suppose that there exists $(b_1, \ldots,\ b_r)$, $(c_1, \ldots,\ c_r) \in \mathbb{F}^r$ two different zeros of the polynomials $g_1(\mathbf{X}), \ldots,\ g_r(\mathbf{X})$ with $f(c_1, \ldots,\ c_r) \neq f(b_1, \ldots,\ b_r)$, then $f \in \mathcal{T}$.*

Proof. Suppose that $k > l$, and exist $a_0, \ldots,\ a_{s-1} \in \mathbb{K}$ with $a_0 \neq 0$ satisfying; $\sum_{j=0}^{s-1} a_j\,(f_{k+j}(\mathbf{X}) - f_{l+j}(\mathbf{X})) = K$, where $K \in \mathbb{K}$.

Then

$$\sum_{j=0}^{s-1} a_j\,(f_{k+j}(\mathbf{X}) - f_{l+j}(\mathbf{X})) = \phi^{k-1}\left(\textstyle\sum_{j=0}^{s-1} a_j\,(f_{1+j}(\mathbf{X}) - f_{1-k+l+j}(\mathbf{X}))\right)$$

and this implies $K = \sum_{j=0}^{s-1} a_j\,((f_{1+j}(\mathbf{X})) - (f_{1-k+l+j}(\mathbf{X})))$ because ϕ is an injective map.

By equation (2), we notice that for $k \neq 0$, we have that $f_k(b_1, \ldots,\ b_r) = f_{k-1}(0, \ldots, 0) = f_k(c_1, \ldots,\ c_r)$, so substituting in the equation both points and subtracting the result, we get that $a_0 = 0$.

The last remark in this section is that conditions in this criterion can be tested using Groebner basis.

1.2 Exponential Sums and Previous Results

We start by listing some previous bounds on exponential sums which will be used to establish our main results.

The first Lemma is the well-known Hua-Loo Keng bound in a form which is a relaxation of the main result of [11] (see also Section 3 of [3] and Lemma 2.2 in [6]), followed by its multidimensional version.

Lemma 3. *For any polynomial* $f(X) = b_d X^d + \ldots + b_1 X + b_0 \in \mathbb{Z}_M[X]$ *of degree* $d \geq 1$*, there is a constant* $c_0 > 0$ *where the bound*

$$\left| \sum_{x \in \mathbb{Z}_M} \mathbf{e}_M(f(x)) \right| < e^{c_0 d} M^{1-1/d} G^{1/d}$$

holds, where $G = \gcd(b_d, \ldots, b_1, M)$.

Lemma 4. *Let* $f(\mathbf{X})$*, with total degree* $d \geq 2$ *and degree greater than one in* X_r*, be a polynomial with integer coefficients, with* $G = 1$*. Then the bound*

$$\left| \sum_{x_1,\ldots,x_r \in \mathbb{Z}_M} \mathbf{e}_M(f(x_1, \ldots, x_r)) \right| \leq e^{c_0 d^2 (\log d + 1)} M^{r - 1/(d^2(\log d+1))}$$

holds, where c_0 *is some positive constant.*

Proof. We recall the univariate case that appears as Lemma 3. Then let

$$g(\mathbf{X}) = f(X_1 + h_1(X_r), X_2 + h_2(X_r), \ldots, X_r)$$

where $h_i(X_r)$ are the polynomials defined in Equation (3). It is easy to see that

$$\left| \sum \mathbf{e}_M(f(x_1, x_2 \ldots, x_r)) \right| = \left| \sum \mathbf{e}_M(g(x_1, x_2 \ldots, x_r)) \right|.$$

where the summations are taken over $x_1, x_2 \ldots, x_r \in \mathbb{Z}_M$ since $(x_1, \ldots, x_r) \to (x_1 + h_1(x_r), x_2 + h_2(x_r), \ldots, x_r)$ merely permutates the points. By Lemma 1, for any selection $x_1, \ldots, x_{r-1}$ this polynomial is not constant modulo p and the gcd of the coefficients of g and M are coprime. Hence, applying Lemma 3, we have

$$\begin{aligned} &\left| \sum_{x_1,x_2\ldots,x_r \in \mathbb{Z}_M} \mathbf{e}_M(g(x_1, x_2 \ldots, x_r)) \right| \\ &\qquad \leq \sum_{x_1,\ldots,x_{r-1} \in \mathbb{Z}_M} \left| \sum_{x_r \in \mathbb{Z}_M} \mathbf{e}_M(g(x_1, x_2 \ldots, x_r)) \right| \\ &\qquad \leq e^{c_0 d^2 (\log d+1)} M^{r - 1/d^2(\log d+1)}. \end{aligned}$$

We obtain the last step by noting that the degree of g in X_r can be bounded by $d^2(\log d + 1)$ and so we are done.

This now allows us to state and prove the following Lemma.

Lemma 5. *Let $f(\mathbf{X})$ be a polynomial with integer coefficients with $\deg_{X_r} f \geq 1$ and total degree d. Recalling the definition of G,*

$$\left| \sum_{x_1 \ldots, x_r \in \mathbb{Z}_M} \mathbf{e}_M(f(x_1, \ldots, x_r)) \right| \leq e^{c_0 d^2 (\log d + 1)} M^r (G/M)^{1/d^2(\log d+1)}$$

Proof. We let

$$f_G(x_1, \ldots, x_r) = (f(x_1, \ldots, x_r) - f(\mathbf{0}))/G$$

and $m = M/G$.
Then,

$$\left| \sum_{x_1, \ldots, x_r \in \mathbb{Z}_M} \mathbf{e}_M(f(x_1, \ldots, x_r)) \right| = \left| \sum_{x_1, \ldots, x_r \in \mathbb{Z}_M} \mathbf{e}_M(f(x_1, \ldots, x_r) - f(\mathbf{0})) \right|$$

$$= G^r \left| \sum_{x_1, \ldots, x_r \in \mathbb{Z}_m} \mathbf{e}_m\left(f_G(x_1, \ldots, x_r)\right) \right|$$

Now $f_G(x_1, \ldots, x_r)$ satisfies the conditions in Lemma 4, so:

$$G^r \left| \sum_{x_1, \ldots, x_r \in \mathbb{Z}_m} \mathbf{e}_m(f_G(x_1, \ldots, x_r)) \right| \leq G^r e^{c_0 d^2 (\log d + 1)} (m)^{r - 1/d^2(\log d+1)}$$

and so the result follows.

Lastly, we will make use of the following lemma, which is essentially the multi-dimensional version of Lemma 2.3 of [6].

Lemma 6. *Let $f(\mathbf{X}) \in \mathbb{Z}_M[\mathbf{X}]$ be a polynomial such that $f^{(p)} \in \mathcal{T}$ for every $p|M$ and let*

$$\sum_{j=0}^{s-1} a_j \left(f_{k+j}(\mathbf{X}) - f_{l+j}(\mathbf{X})\right) = \sum_{i_1=0}^{d_1} \cdots \sum_{i_r=0}^{d_r} b_{i_1, \ldots, i_r} X_1^{i_1} \ldots X_r^{i_r},$$

where $k \neq l$. Recalling the definition of G, the following equality $G = \gcd(a_0, \ldots, a_{s-1}, M)$ holds.

Proof. We put $A_j = a_j/G$ and $m = M/G$, $j = 0, \ldots, s-1$. In particular,

$$\gcd(A_0, \ldots, A_{s-1}, m) = 1. \tag{6}$$

It is enough to show that the polynomial

$$H(\mathbf{X}) = \sum_{j=0}^{s-1} A_j \left(f_{k+j}(\mathbf{X}) - f_{l+j}(\mathbf{X})\right)$$

is nonconstant modulo any prime $p|m$, for $k \neq l$.

By definition, we have

$$H^{(p)}(\mathbf{X}) \equiv \sum_{j=0}^{s-1} A_j \left(f_{k+j}^{(p)}(\mathbf{X}) - f_{l+j}^{(p)}(\mathbf{X}) \right) \pmod{p}$$

and $H^{(p)}(\mathbf{X})$ can not be a constant polynomial, since $f^{(p)} \in \mathcal{T}$ and so we are done.

1.3 Discrepancy

For a sequence of N points

$$\Gamma = (\gamma_{0,n}, \ldots, \gamma_{s-1,n})_{n=0}^{N-1} \tag{7}$$

of the half-open interval $[0,1)^s$, denote by Δ_Γ its discrepancy, that is,

$$\Delta_\Gamma = \sup_{B \subseteq [0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

$$B = [\alpha_0, \beta_0) \times \ldots \times [\alpha_{s-1}, \beta_{s-1}) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes.

For an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max_{i=0,\ldots,s-1} |a_i|, \qquad r(\mathbf{a}) = \prod_{i=0}^{s-1} \max\{|a_i|, 1\}. \tag{8}$$

We need the *Erdös–Turán–Koksma inequality* (see Theorem 1.21 of [4]) for the discrepancy of a sequence of points of the s-dimensional unit cube, which we present in the following form.

Lemma 7. *There exists a constant $C_s > 0$ depending only on the dimension s such that, for any integer $L \geq 1$, for the discrepancy of a sequence of points (7) the bound*

$$\Delta_\Gamma < C_s \left(\frac{1}{L} + \frac{1}{N} \sum_{0 < |\mathbf{a}| \leq L} \frac{1}{r(\mathbf{a})} \left| \sum_{n=0}^{N-1} \exp\left(2\pi i \sum_{j=0}^{s-1} a_j \gamma_{j,n} \right) \right| \right)$$

holds, where $|\mathbf{a}|$, $r(\mathbf{a})$ are defined by (8) and the sum is taken over all integer vectors

$$\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$$

with $0 < |\mathbf{a}| \leq L$.

The currently best value of C_s is given in [2].

2 Discrepancy Bound

Let the sequence (u_n) generated by (1) be purely periodic with an arbitrary period t. For an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ we introduce the exponential sum

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j u_{n+j} \right).$$

Theorem 1. *Let the sequence (u_n), given by (1) with a polynomial $f^{(p)}(\mathbf{X}) \in \mathcal{T}$, for every prime divisor p of M, with total degree d and $\deg_{X_r} f \geq 1$, be purely periodic with period t and $t \geq N \geq 1$. The bound*

$$\max_{\gcd(a_0,\ldots,a_{s-1},M)=G} |S_{\mathbf{a}}(N)| = O\left(N^{1/2} M^{r/2} (\log\log(M/G))^{-1/2}\right)$$

holds, where $G = \gcd(a_0, \ldots, a_{s-1}, M)$ and the implied constant depends only on s and d.

Proof. The proof follows a strategy first seen in [9].
Select any $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ with $\gcd(a_0, \ldots, a_{s-1}, M) = G$.

It is obvious that for any integer $k \geq 0$ we have

$$\left| S_{\mathbf{a}}(N) - \sum_{n=0}^{N-1} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j u_{n+k+j} \right) \right| \leq 2k.$$

Therefore, for any integer $K \geq 1$,

$$K|S_{\mathbf{a}}(N)| \leq W + K^2,$$

where

$$W = \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j u_{n+k+j} \right) \right| \leq \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j u_{n+k+j} \right) \right|.$$

Accordingly, letting $\mathbf{x} = x_1, \ldots, x_r$, we obtain

$$\begin{aligned} W^2 &\leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j f_{k+j}\left(u_n, \ldots, u_{n-r+1}\right) \right) \right|^2 \\ &\leq N \sum_{\mathbf{x} \in \mathbb{Z}_M^r} \left| \sum_{k=0}^{K-1} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j f_{k+j}\left(\mathbf{x}\right) \right) \right|^2 \\ &= N \sum_{k=0}^{K-1} \sum_{l=0}^{K-1} \sum_{\mathbf{x} \in \mathbb{Z}_M^r} \mathbf{e}_M \left(\sum_{j=0}^{s-1} a_j \left(f_{k+j}\left(\mathbf{x}\right) - f_{l+j}\left(\mathbf{x}\right) \right) \right). \end{aligned}$$

If $k = l$, then the inner sum is trivially equal to M^r. There are K such sums. Otherwise the polynomial $\sum_{j=0}^{s-1} a_j \left(f_{k+j}\left(\mathbf{X}\right) - f_{l+j}\left(\mathbf{X}\right)\right)$ is nonconstant since $f^{(p)} \in \mathcal{T}$. Hence we can apply Lemma 5 and Lemma 6 (so that we only need consider $a_j, j = 0, \ldots, s-1$, instead of the coefficients of f) to the inner sum, obtaining the upper bound

$$e^{c_0 d^{3(K+s-2)}} M^{r-1/d^{3(K+s-2)}} G^{1/d^{3(K+s-2)}}$$

for at most K^2 sums and positive constant c_0 and noting that
$d^2(\log d + 1) < d^3$.
Hence,

$$W^2 \leq KNM^r + K^2 N e^{c_0 d^{3(K+s-2)}} M^{r-1/d^{3(K+s-2)}} G^{1/d^{3(K+s-2)}}.$$

Now, without too much loss of generality we may assume $(d+1)^{3(K+s-2)} \geq 2$. Next we put $K = \lceil \log\log(M/G)/(3c\log(d+1)) \rceil$, for some $c > 2$ to guarantee that the first term dominates and the result follows.

Next, let $D_s(N)$ denote the discrepancy of the points given by

$$\left(\frac{u_n}{M}, \ldots, \frac{u_{n+s-1}}{M}\right), \qquad n = 0, \ldots, N-1,$$

in the s-dimensional unit cube $[0,1)^s$.

Theorem 2. *If the sequence (u_n), given by (1) with a polynomial $f^{(p)}(\mathbf{X}) \in \mathcal{T}$, for every prime divisor p of M, with total degree d and $\deg_{X_r} f \geq 1$ is purely periodic with period t with $t \geq N \geq 1$, then the bound*

$$D_s(N) = O\left(N^{-1/2} M^{r/2} (\log\log\log M)^s / (\log\log M)^{1/2}\right)$$

holds, where the implied constant depends only on s and d.

Proof. The statement follows from Lemma 7, taken with

$$L = \left\lceil N^{1/2} M^{-r/2} (\log\log M)^{1/2} \right\rceil$$

and the bound of Theorem 1, where all occurring $G = \gcd(a_0, \ldots, a_{s-1}, M)$ are at most L.

References

1. Arkhipov, G.I., Chubarikov, V.N., Karatsuba, A.A.: Trigonometric Sums in Number Theory and Analysis, de Gruyter Expositions in Mathematics, Berlin, vol. 39 (2004)
2. Cochrane, T.: Trigonometric approximation and uniform distribution modulo 1. Proc. Amer. Math. Soc. 103, 695–702 (1988)
3. Cochrane, T., Zheng, Z.Y.: A Survey on Pure and Mixed Exponential Sums Modulo Prime Numbers. Proc. Illinois Millenial Conf. on Number Theory 1, 271–300 (2002)

4. Drmota, M., Tichy, R.F.: Sequences, discrepancies and applications. Springer, Berlin (1997)
5. El-Mahassni, E.D., Shparlinski, I.E., Winterhof, A.: Distribution of nonlinear congruential pseudorandom numbers for almost squarefree integers. Monatsh. Math. 148, 297–307 (2006)
6. El-Mahassni, E.D., Winterhof, A.: On the distribution of nonlinear congruential pseudorandom numbers in residue rings. Intern. J. Number Th. 2(1), 163–168 (2006)
7. Griffin, F., Niederreiter, H., Shparlinski, I.: On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders. In: Fossorier, M.P.C., Imai, H., Lin, S., Poli, A. (eds.) AAECC 1999. LNCS, vol. 1719, pp. 87–93. Springer, Heidelberg (1999)
8. Gutierrez, J., Gomez-Perez, D.: Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. In: Bozta, S., Sphparlinski, I. (eds.) AAECC 2001. LNCS, vol. 2227, pp. 192–199. Springer, Heidelberg (2001)
9. Niederreiter, H., Shparlinski, I.E.: On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. Finite Fields and Their Appl. 5, 246–253 (1999)
10. Niederreiter, H., Shparlinski, I.E.: Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arith. 92, 89–98 (2000)
11. Stečkin, S.B.: An estimate of a complete rational exponential sum. Trudy Mat. Inst. Steklov. 143, 188–207 (1977) (in Russian)