ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 1, Pages 3–13
ISSN 1930-1235: (2010)

EXPONENTIAL SUMS FOR NONLINEAR RECURRING SEQUENCES IN RESIDUE RINGS

EDWIN EL-MAHASSNI

ABSTRACT. We prove some new bounds on exponential sums for nonlinear recurring sequences over residue rings. In addition, we also show similar novel results when the modulus is almost squarefree, thereby improving the results in El-Mahassni, Shparlinski, and Winterhof [11] and El-Mahassni and Winterhof [13] This is done by using a technique employed by Niederreiter and Winterhof [26] and through the generalisation of a Lemma found in [11] and [13]. Lastly, applications to the distribution of nonlinear congruential pseudorandom numbers are also given.

1. Introduction

For an integer $M \geq 2$, we let $f(X) \in \mathbb{Z}_M[X]$ be a polynomial of degree $d \geq 2$ over the residue ring $\mathbb{Z}_M$ modulo M , defined by a recurrence relation of the form

$$u_{n+1} \equiv f(u_n) \pmod{M}, \quad 0 \leq u_n \leq M-1, \qquad n = 0, 1, \dots \tag{1}$$

with some initial value $u_0 = v$. It is obvious that the sequence (1) eventually becomes periodic with some period $t \leq M$.

We define the sequence of polynomials $f_k(X)$, by the recurrence relation

$$f_k(X) = f(f_{k-1}(X)), \qquad k = 1, 2, \dots , \tag{2}$$

where $f_0(X) = X$. It is clear that if $\deg f = d \geq 2$ then $\deg f_k \leq d^k$ and that $u_{n+k} \equiv f_k(u_n) \pmod{M}$.

Throughout this paper we assume that this sequence is *purely periodic*, that is, $u_n = u_{n+t}$ beginning with $n = 0$, otherwise we consider a shift of the original sequence.

We define $\mathbf{e}_M(x) = \exp(2\pi i x/M)$ and consider the incomplete exponential sums

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

where $\mathbf{a} = (a_0, \dots, a_{s-1}) \not\equiv 0 \pmod{M}$. Now, throughout the rest of the paper we assume that f is of degree at least 2 modulo every prime divisor of M.

Key words and phrases. Pseudorandom numbers; nonlinear congruential method; discrepancy; exponential sums.

The author is very grateful to Igor Shparlinski for helpful comments and suggestions.

2000 Mathematics Subject Classification. Primary: 11K45, 11L07, 65C10.

We now go on to recall some previous bounds which we will improve upon. First, we assume that $G = \gcd(a_0, \ldots, a_{s-1}, M) < M/2$. We start by noting that from [13], for an arbitrary modulus M, the bound

$$\max_{\gcd(a_0,\ldots,a_{s-1},M)=G} S_{\mathbf{a}}(M,N) = O\left(N^{1/2}\frac{M^{1/2}}{(\log\log(M/G))^{1/2}}\right) \tag{3}$$

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

Then, in [11], an improvement on this bound was proven when the modulus is almost squarefree. This was defined to be when

$$\omega(M) \le 2\log\log M \quad \text{and} \quad \rho(M) \ge \frac{M}{(\log\log M)^2}, \tag{4}$$

where $\omega(M)$ denotes the number of distinct prime divisors of M and $\rho(M)$ is the largest squarefree divisor of M. In those cases, for any $\varepsilon \ge 0$, the bound

$$\max_{\gcd(a_0,\ldots,a_{s-1},M)\le M^{1-\varepsilon}} S_{\mathbf{a}}(M,N) = O\left(N^{1/2}M^{1/2}\frac{(\log\log M)^{1/2}}{(\log M)^{1/2}}\right) \tag{5}$$

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

Further, in [11], it has also been proven that if the constraints of (4) are satisfied, for every sufficiently large integer Q, the bound given by (5) holds for all positive integers $M \le Q$ except $o(Q)$ of them.

The rest of the paper is structured as follows. In Section 2, we list some previously established results which we use to prove our main bound. In Section 3, using a similar technique to that in [26], we modify the methods in [11] and [13] to provide new bounds for $S_{\mathbf{a}}(M,N)$. We will show that we can obtain improvements for the bounds in (3) and (5) when $N \ge M/\log M$ and by placing some restrictions on the size of p_1, the smallest prime divisor of M. In Section 4, we apply the exponential sum bound to analyse the distribution of *nonlinear congruential pseudorandom numbers* $u_n/M, n \ge 0$, in the unit interval in terms of a discrepancy bound. We refer to [22, Chapter 8], [24] and [1] for further background on nonlinear congruential pseudorandom numbers.

2. Preliminaries

We now recall some results which will aid us in proving our main results. For a sequence of N points

$$\Gamma = (\gamma_{1,n}, \ldots, \gamma_{s,n})_{n=1}^{N} \tag{6}$$

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

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes. For an integer vector $\mathbf{a} = (a_0, \dots, a_{s-1}) \in \mathbb{Z}^s$ we put

$$(7) \qquad |\mathbf{a}| = \max_{i=0,\dots,s-1} |a_i| \qquad \text{and} \qquad r(\mathbf{a}) = \prod_{i=0}^{s-1} \max\{|a_i|, 1\}.$$

We also need the *Erdös–Turán–Koksma inequality* (see [5, Theorem 1.21]) for the discrepancy of a sequence of points of the s-dimensional unit cube, which we present in the following form.

Lemma 1. *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* (6) *the bound*

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

holds, where $|\mathbf{a}|$ and $r(\mathbf{a})$ are defined by (7) *and the sum is taken over all integer vectors*

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

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

The currently best value of C_s is given in [3].

We also make use of the Hua Loo Keng bound in a form which is a relaxation of the main result of [27] (see also Section 3 of [2]).

Lemma 2. *For any polynomial $F(X) = B_D X^D + \dots + B_1 X + B_0 \in \mathbb{Z}_M[X]$ of degree $D \geq 1$, there is a constant $c_0 > 0$ so that the bound*

$$\left| \sum_{x=1}^{M} \mathbf{e}_M \left(F(x) \right) \right| < e^{c_0 D} M^{1-1/D} G^{1/D}$$

holds, where $G = \gcd(B_D, \dots, B_1, M)$.

Note that the currently best known constant is $c_0 = 1.74$ see [4].

We now list the following lemmas. The first is listed in a slightly weaker form than found in [11, Lemma 4], whilst the second is an extension of [13, Lemma 3] respectively.

Lemma 3. *Let $F(X) = \sum_{i=0}^{D} B_i X^i \in \mathbb{Z}_M[X]$ be of degree D. Then*

$$\left| \sum_{x=0}^{M-1} \mathbf{e}_M(F(x)) \right| \leq (D-1)^{\omega(M)} M \Delta^{1/2} \rho(M)^{-1/2},$$

where $\Delta = \gcd(B_1, ..., B_D, M)$.

Lemma 4. *Let $f(X) \in \mathbb{Z}_M[X]$ be a polynomial of degree at least 2 modulo every prime divisor of M, with p_1 being the least prime divisor of M, and let*

$$\sum_{j=0}^{s-1} a_j \left(\left(f_{k_1+j}(X) + \dots + f_{k_r+j}(X) \right) - \left(f_{k_{r+1}+j}(X) + \dots f_{k_{2r}+j}(X) \right) \right)$$
$$= B_D X^D + \dots + B_1 X + B_0.$$

Then, if $\{k_1, \ldots, k_r\} \neq \{k_{r+1}, \ldots, k_{2r}\}$ *as multisets, for any* $p_1 > r \geq 1$*, we have*

$$\gcd(B_D, \ldots, B_1, M) = \gcd(a_0, \ldots, a_{s-1}, M).$$

Proof. We put $A_j = a_j/G$, $j = 0, \ldots, s-1$ and $m = M/G$, where $G = \gcd(a_0, \ldots, a_{s-1}, M)$. In particular,

$$\gcd(A_0, \ldots, A_{s-1}, m) = 1. \tag{8}$$

It is enough to show that the polynomial

$$H(X) = \sum_{j=0}^{s-1} A_j \left(\left(f_{k_1+j}(X) + \ldots + f_{k_r+j}(X) \right) - \left(f_{k_{r+1}+j}(X) + \ldots + f_{k_{2r}+j}(X) \right) \right)$$

is not a constant polynomial modulo p for any prime $p|m$.

We take $f^{(p)}$ to be the reduction of f modulo p. By our assumption, $\deg f^{(p)} = d_p \geq 2$. Denoting by $f_k^{(p)}$ the kth iteration of $f^{(p)}$ defined similarly to (2) and by $H^{(p)}(X)$ as $H(X) \mod p$. Thus,

$$H^{(p)}(X) = \sum_{t=1}^{r} \sum_{j=0}^{s-1} A_j \left(f_{k_t+j}^{(p)}(X) - f_{k_{r+t}+j}^{(p)}(X) \right) \pmod p.$$

Let h be the largest $j = 1, \ldots, s$ with $\gcd(A_j, p) = 1$ (we see from (8) that such h exists). Then for $\{k_1, \ldots, k_r\} \neq \{k_{r+1}, \ldots, k_{2r}\}$ as multisets, where $r < p_1$, the polynomial $H(X)$ is of degree exactly $d_p^{k+h} \geq 1$ modulo p, where k is the largest k_i which appears in one of the two sets more often than in the other one, such that $k_i \neq k_{i+r}$, for some $1 \leq i \leq t$, which finishes the proof. □

The following statement proceeds immediately from the classical result of Hardy-Ramanujan on the typical order of $\omega(M)$, see [18, Theorem 431], [28, Section 3.4, Theorem 4], and used also in [11, Lemma 6].

Lemma 5. *For every sufficiently large* Q*, the bound* $\omega(M) \leq 2 \log\log M$ *holds for all positive integers* $M \leq Q$ *except* $o(Q)$ *of them.*

Lastly, we also use the next result which was proved in [11, Lemma 7].

Lemma 6. *For any integer* $Y \geq 1$ *the bound* $\rho(M) > M/Y$ *holds for all positive integers* $M \leq Q$ *except* $O(Q/Y^{1/2})$*.*

3. Bounds of Exponential Sums

In this section, through the use of the Hölder inequality as employed in [26], we improve bounds (3) and (5) respectively, by refining the method of bounding exponential sums that were applied in [11] and [13].

Theorem 7. *Let the sequence* (u_n)*, given by* (1) *with a polynomial* $f(X) \in \mathbb{Z}_M[X]$*, of total degree* d*, be purely periodic modulo* M *with period* t*. Assume that for every* *prime divisor p of M, we have $p \geq 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \geq N \geq M/\log\log M$, then the bound*

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

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

Proof. We first prove that, for any integer $2\log\log\log M > r \geq 1$, and $\gcd(a_0,\ldots,a_{s-1},M) = G$, we have

$$S_{\mathbf{a}}(M,N) = O\Bigg(Nr^{1/2}(M/N)^{1/(2r)} \times \left(\min\left\{\lfloor \log\log(M/G)/3\log d\rfloor, \left\lfloor rc_1 e^{(\log(M/G))^{1/3}/r}\right\rfloor\right\}\right)^{-1/2}\Bigg)$$

for $T \geq N \geq M/\log\log M$ and some positive constant c_1. It is obvious that for any integer $k \geq 0$ we have

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

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

$$K|S_{\mathbf{a}}(M,N)| \leq W + K(K-1), \tag{9}$$

where

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

By the Hölder inequality, and using

$$F_k(X) = \sum_{j=0}^{s-1} a_j f_{k+j}(X),$$

we obtain

$$\begin{aligned} W^{2r} &\leq N^{2r-1}\sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(u_n)\right)\right|^{2r} \\ &\leq N^{2r-1}\sum_{x\in\mathbb{Z}_M}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(x)\right)\right|^{2r} \\ &\leq N^{2r-1}\sum_{k_1,\ldots,k_{2r}=0}^{K-1}\left|\sum_{x\in\mathbb{Z}_M}\mathbf{e}_M\left(F_{k_1,\ldots,k_{2r}}(x)\right)\right|, \end{aligned}$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$.

If $\{k_1,\ldots,k_r\} = \{k_{r+1},\ldots,k_{2r}\}$ as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to M. There are at most $r!K^r \leq r^rK^r$ such sums. Otherwise, we can apply Lemma 2 together with Lemma 4, to get the upper bound $e^{c_0 d^{K+s-2}} M^{1-1/d^{K+s-2}} G^{1/d^{K+s-2}}$ for at most K^{2r}. Hence,

$$W^{2r} \leq r^rK^rN^{2r-1}M + e^{c_0 d^{K+s-2}} M^{1-1/d^{K+s-2}} G^{1/d^{K+s-2}} K^{2r}N^{2r-1} \tag{10}$$

Choose

$$K = \min\left\{ \left\lfloor \frac{\log\log(M/G)}{3\log d} \right\rfloor, \left\lfloor rc_1 e^{(\log(M/G))^{1/3}/r} \right\rfloor \right\},$$

for some positive constant c_1. Note that we get $\left\lfloor \frac{\log\log(M/G)}{3\log d} \right\rfloor$, when $r = 1$ and using this value for $e^{c_0 d^{K+s-2}}$ we then obtain $\left\lfloor rc_1 e^{(\log(M/G))^{1/3}/r} \right\rfloor$ for arbitrary r.

Then it is easy to see that the first term in the right-hand side of (10) dominates the second one in terms of the order of magnitude in M, and we get the first equation of the proof from (9) and (10) after simple calculations.

Finally, we choose

$$r = \lceil \log(2M/N) \rceil .$$

Note that $1 \leq r < 2\log\log\log M$, since $N \geq M/\log\log M$. Thus, for all suitable large M, we have

$$c_1 r e^{(\log(M/G))^{1/3}/r} \geq \log\log(M/G).$$

To see this is true, we note that this is equivalent to proving

$$\log r + \log c_1 + \frac{(\log(M/G))^{1/3}}{r} \geq \log\log\log(M/G).$$

If $\log r \geq \log\log\log(M/G)$ then we are done, else we have $r < \log\log(M/G)$. In this case, we simply need to show that for all large enough M

$$\frac{(\log(M/G))^{1/3}}{(\log\log(M/G))} \geq \log\log(M/G).$$

But, taking logarithms from both sides we can then indeed see that

$$\log\log(M/G) \geq 4\log\log\log(M/G)).$$

If we then note that $r^{1/2}(M/N)^{1/2r} < \log(2M/N)$, the theorem then follows from the first equation of the proof. □

This next bound is an improvement for the exponential sum of nonlinear congruential generators with an "almost squarefree" modulus.

Theorem 8. *Let an integer $M \geq 1$ be such that*

$$\omega(M) \leq 2\log\log M \qquad \textit{and} \qquad \rho(M) \geq \frac{M}{(\log\log M)^2},$$

where $\omega(M)$ denotes the number of distinct prime divisors of M and $\rho(M)$ is the largest squarefree divisor of M.

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \geq 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \geq N \geq M/\log\log M$, then, for any $\varepsilon > 0$, the bound

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

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

Proof. Put $w = \omega(M)$ and $R = \rho(M)$. We first prove that, for any integer $2\log\log\log M > r \geq 1$, and $\gcd(a_0, \ldots, a_{s-1}, M) \leq M^{1-\varepsilon}$, we have

$$S_{\mathbf{a}}(M,N) =$$

$$O\Bigg(Nr^{1/2}(M/N)^{1/(2r)}\bigg(\min\Big\{\lfloor\varepsilon\log M/(5\log d\log\log M)\rfloor\,, \left\lfloor r\left(M^{\varepsilon/10}/\left(\log\log M\right)\right)^{1/r}\right\rfloor\Big\}\bigg)^{-1/2}\Bigg),$$

for $M/\log\log M \leq t \leq M$. It is obvious that for any integer $k \geq 0$ we have

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

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

$$K|S_{\mathbf{a}}(M,N)| \leq W + K(K-1), \tag{11}$$

where

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

By the Hölder inequality, and using

$$F_k(X) = \sum_{j=0}^{s-1}a_j f_{k+j}(X),$$

we obtain

$$\begin{aligned} W^{2r} &\leq N^{2r-1}\sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(u_n)\right)\right|^{2r} \\ &\leq N^{2r-1}\sum_{x\in\mathbb{Z}_M}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(x)\right)\right|^{2r} \\ &\leq N^{2r-1}\sum_{k_1,\ldots,k_{2r}=0}^{K-1}\left|\sum_{x\in\mathbb{Z}_M}\mathbf{e}_M\left(F_{k_1,\ldots,k_{2r}}(x)\right)\right|, \end{aligned}$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$

If $\{k_1, \ldots, k_r\} = \{k_{r+1}, \ldots, k_{2r}\}$ as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to M. There are at most $r!K^r \leq r^r K^r$ such sums. Otherwise, we can apply Lemma 3, together with Lemma 4 to the inner sum, to get the upper bound $d^{(K+s-2)w}M^{(3-\varepsilon)/2}R^{-1/2}$ for at most K^{2r}. Hence,

$$W^{2r} \leq r^r K^r N^{2r-1}M + d^{2(K+s-2)\log\log M}K^{2r}N^{2r-1}M^{1-\varepsilon/2}\log\log M \tag{12}$$

Choose

$$K = \min\left\{\left\lfloor\frac{\varepsilon\log M}{5\log d\log\log M}\right\rfloor, \left\lfloor r\left(M^{\varepsilon/10}/\log\log M\right)^{1/r}\right\rfloor\right\}.$$

Note that we get $\left\lfloor \frac{\varepsilon \log M}{5 \log d \log\log M} \right\rfloor$ when $r = 1$ and using this value for $d^{2(K+s-2)\log\log M}$ we then obtain $\left\lfloor r \left(M^{\varepsilon/10}/\log\log M\right)^{1/r} \right\rfloor$ for arbitrary r.

Then it is easy to see that the first term in the right-hand side of (12) dominates the second one in terms of the order of magnitude in M, and we get the first equation of the proof from (11) and (12) after simple calculations.

Finally, we choose

$$r = \lceil \log(2M/N) \rceil.$$

Note that $r < 2\log\log\log M$ since $N \geq M/\log\log M$. Clearly, for our choice of r and all large enough M, we have

$$\begin{aligned} r\left(M^{\varepsilon/10}/\log\log M\right)^{1/r} &> \log\left(M^{\varepsilon/10}/\log\log M\right)/2\log\log\log M \\ &> \log M^{\varepsilon}/5\log d \log\log M, \end{aligned}$$

for any $\varepsilon > 0$. If we then note that $r^{1/2}(M/N)^{1/2r} < \log(2M/N)$, the theorem then follows from the first equation of the proof. □

Recalling Lemmas 5 and 6 we obtain:

Corollary 9. *For every sufficiently large Q, the following statement holds for all positive integers $M \leq Q$ except $o(Q)$ of them:*

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \geq 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \geq N \geq M/\log\log M$, then, for any $\varepsilon > 0$, the bound

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

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

We now present some new discrepancy bounds using our new results for the exponential sums for the nonlinear congruential generator. The first bound applies to arbitrary moduli, whilst the latter is for almost squarefree moduli.

Let $D_s(M,N)$ denote the discrepancy of the points

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

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

Theorem 10. *If the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \geq 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \geq N \geq M/\log\log M$, then, the bound*

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

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

Proof. The statement follows from Lemma 1, taken with

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

and the bound of Theorem 7, as

$$\gcd(a_0, \ldots, a_{s-1}, M) \le L \le 2\,(\log\log M)^{1/2} \le (\log M)^{1/2} \le M^{1/2}$$

where for any nonzero vector $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{Z}^s$ with $|\mathbf{a}| \le L$ and sufficiently large M. □

Theorem 11. *Let an integer $M \ge 1$ be such that*

$$\omega(M) \le 2\log\log M \qquad \textit{and} \qquad \rho(M) \ge \frac{M}{(\log\log M)^2}.$$

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \ge 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \ge N \ge M/\log\log M$, then, for any $\varepsilon > 0$, the bound

$$D_s(M,N) = O\left(\left(\frac{(\log(2M/N)}{\log M} \right)^{1/2} (\log\log M)^{s+1/2} \right)$$

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

Proof. The statement follows from Lemma 1 taken with

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

and the bound of Theorem 8, as

$$\gcd(a_0, \ldots, a_{s-1}, M) \le L \le 2\,(\log M)^{1/2} \le M^{1/2}$$

for any nonzero vector $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{Z}^s$ with $|\mathbf{a}| \le L$ and sufficiently large M. □

Recalling Lemmas 5 and 6 we obtain:

Corollary 12. *For every sufficiently large Q, the following statement holds for all positive integers $M \le Q$ except $o(Q)$ of them:*

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \ge 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \ge N \ge M/\log\log M$, then, for any $\varepsilon > 0$, the bound

$$D_s(M,N) = O\left(\left(\frac{(\log(2M/N)}{\log M} \right)^{1/2} (\log\log M)^{s+1/2} \right)$$

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

4. Discussion

We remark that for Theorems 7 and 8 results covering all possible N would be desirable. We also note that for the counter-dependent generators, the Holdër inequality was also applied to the prime modulus case [12]. However, we believe that through a similar variant of Lemma 4, improvements on the bounds for the arbitrary modulus case [10] and for the higher order cases (both prime and arbitrary modulus [9, 17]) could also be obtained. We finally note that this technique does not improve the bound of permutation polynomials modulo almost a squarefree integer (see [11, Section 4]).

References

[1] S. Blackburn and I. Shparlinski, Character Sums and Nonlinear Recurring Sequences, Discrete Mathematics, 2006, 306, 1126-1131.

[2] T. Cochrane and Z. Y. Zheng, A Survey on Pure and Mixed Exponential Sums Modulo Prime Powers, Proc. Illinois Millennial Conf. on Number Theory, 2002, 1, 271-300.

[3] T. Cochrane, Trigonometric Approximations and Uniform Distribution Modulo 1, Proc. Amer. Math. Soc., 1988, 103, 695—703.

[4] P. Ding and M. G. Qi, Further Estimates of Complete Trigonometric Sums, J. Tsinghua Univ., 1989, 29, 74–85.

[5] M. Drmota and R. Tichy, Sequences, Discrepancies and Applications, Springer-Verlag, Berlin, 1997.

[6] E. El-Mahassni and I. E. Shparlinski, On the Distribution of the Elliptic Curve Power Generator, Proc. 8th. Conf. Finite Fields and Their Appl, Contemp. Math. (2007), 2008, 461, 111–118.

[7] On the Distribution of the Power Generator Modulo a Prime Power for Parts of the Period, Bol. Soc. Mat. Mex., 2008, 13 (1), 1.

[8] E. El-Mahassni, On the Distribution of the Power Generator Over a Residue Ring for Parts of the Period, Rev. Mat. Compl., 2008, 21 (2), 319-325.

[9] E. El-Mahassni and D. Gomez, On the Distribution of the Counter-Dependent Nonlinear Congruential Generator in Residue Rings, Int. J. Num. Th., 2008, 4 (6), 1009–1018.

[10] E. El-Mahassni and D. Gomez, On the Distribution of Nonlinear Congruential Pseudorandom Numbers of Higher Orders in Residue Rings, AAECC, Lecture Notes in Computer Science, 2009, 5527, 195-203.

[11] E. D. El-Mahassni and I. E. Shparlinski and A. Winterhof, Distribution of Nonlinear Congruential Pseudorandom Numbers for Almost Squarefree Integers, Monatsh. Math., 2006, 148, 297–307.

[12] E. D. El-Mahassni and A. Winterhof, On the Distribution and Linear Complexity of Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators, JP Journal of Algebra and Number Theory, 2006, 6(2), 411–423.

[13] E. D. El-Mahassni and A. Winterhof, On the Distribution of Nonlinear Congruential Pseudorandom Numbers in Residue Rings, Intern. J. Number Th., 2006, 2(1), 163–168.

[14] J. B. Friedlander, J. Hansen and I. E. Shparlinski, On Character Sums with Exponential Functions, Mathematika, 2000, 47, 75–85.

[15] J. B. Friedlander and I. E. Shparlinski , On the Distribution of the Power Generator, Math. Comp., 2001, 70, 1575–1589.

[16] Domingo Gomez and Jaime Gutierrez and Igor E. Shparlinski, Exponential sums with Dickson polynomials, Finite Fields and Their Applications, 2006, 12, 16–25.

[17] F. Griffin and H. Niederreiter and I. E. Shparlinski, On the Distribution of Nonlinear Recursive Congruential Pseudorandom Numbers of Higher Orders, AAECC, Lecture Notes in Computer Science , 1999, 1719, 87-93.

[18] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, 1979.

[19] R. Lidl and H. Niederreiter, Finite Fields and Applications, Cambridge, 1997.

[20] T. Lange and I. E. Shparlinski, Certain Exponential Sums and Random Walks on Elliptic Curves, Canada J. Math, 2005, 57, 338–350.

[21] H. Niederreiter, Design and Analysis of Nonlinear Pseudorandom Number Generators, Monte Carlo Simulation, 2001, A. A. Balkema Publishers, Rotterdam, 3–9.

[22] H. Niederreiter, Random Number Generation and Quasi–Monte Carlo Methods, Siam Press, 1992.

[23] H. Niederreiter and I. E. Shparlinski, On the Distribution and Lattice Structure of Nonlinear Congruential Pseudorandom Numbers, Finite Fields and Their Appl., 1999, 5, 246–253.

[24] H. Niederreiter and I. E. Shparlinski, Recent Advances in the Theory of Nonlinear Pseudorandom Number Generators, Proc. Conf. on Monte Carlo and Quasi Monte Carlo Methods, 2000, 2002, 86–102.

[25] H. Niederreiter and I. E. Shparlinski, Dynamical Systems Generated by Rational Functions, Lect. Notes in Comp. Sci., 2003, 2643,Springer-Verlag, Berlin, 6–17.

[26] H. Niederreiter and A. Winterhof, Exponential Sums for Nonlinear Recurring Sequences, Finite Fields and Their Appl., 2008, 14(1), 59–64.

[27] S. B. Stečkin, An Estimate of a Complete Rational Exponential Sum, Trudy Mat. Inst. Steklov., 1977, 143, 188–207 (in Russian).

[28] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, University Press, 1995, Cambridge, UK.

Department of Computing, Macquarie University, North Ryde, NSW 2109, Australia

E-mail address: `edwinelm@ics.mq.edu.au`