*Chaotic Modeling and Simulation (CMSIM) 2: 159–168, 2017*

# Sequences of PRN's produced by circular generator

Sergey Varbanets

Department of Computer Algebra and Discrete Mathematics, Institute of Mathematics, Economics and Mechanics, I.I. Mechnikov Odessa National University, str. Dvoryanskaya, 2, Odessa, 65026, Ukraine
(E-mail: varb@sana.od.ua)

**Abstract.** In the present paper we investigate the family of the sequences of PRN's produced by the generic elements of norm subgroup of multiplicative group of the reduced system of residues modulo $p^m$ of the ring of Gaussian integers. The sequence of that family passes two-dimensional serial test on uniformity and unpredictability.
**Keywords:** norm group, pseudorandom numbers, discrepancy.

## 1 Introduction

The sequence of real numbers $\{a_n\}$, $0 \le a_n < 1$ we call the sequence of pseudorandom numbers (abbreviation, PRN's) if it is produced by deterministic generator and, being a periodical sequence, has the statistical properties such that it looks like to implementation of the sequence of random numbers with independent and uniformly distributed values on $[0, 1)$. More acceptable sequences of PRN's are generated by the congruential recursion

$$y_{n+1} \equiv f(y_n, y_{n-1}, \dots, y_{n-k+1}) \pmod m$$

with some initial values $y_0, y_1, \dots, y_{k-1} \in \{0, 1, \dots, m-1\}$, where $f(u_1, \dots, u_k)$ is integer-valued function over $Z_m^k$.

Because it emerged that linear function $f(u) = au + b$ does not supply requirements of "affinity" to statistical independency (unpredictability) (see, for example, [10]), this motivated the creation of nonlinear congruential pseudorandom sequences having an unpredictability property.

The generator produced by the quadratic function $f(u) = au^2 + bu + c$ satisfies to condition of "practical" unpredictability (see, [6]).

The generator associated with quadratic function $f(c)$ we call parabolical.

In 1989 J. Eichenauer and J. Lehn[4] and H. Niederreiter[13] have studied a recursive sequence generated by the recursive relation

$$x_{n+1} = \begin{cases} ax_n^{-1} + b \; if \; x_n \neq 0, \\ b \qquad\qquad if \; x_n = 0. \end{cases}$$

Received: 15 September 2016 / Accepted: 12 January 2017

ISSN 2241-0503

with some coefficients $a \in F_q^*$, $b \in F_q$.

In the paper [18] there are investigated the analogous of inversive congruential generators, that without any increases of computational complexity of finding the elements of sequence $\{y_n\}$, have got an essential complexity for intruder's to work around the parameters of inversive or linear generator to be recovered.

The requirements to uniform distribution and unpredictability is satisfied the following inversive generator

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m},$$

where $p$ is a prime number, $a, b \in Z$, $y_n^{-1}$ is a multiplicative inverse to $y_n \pmod{p^m}$.

The inversive generator and its generalization was being investigated by many authors (see, [1]-[3], [5]-[8], [15]-[18]).

Starting out from our reasoning, we will call such inversive generator as hyperbolical.

In [19] there have been studied the statistical properties of sequences of PRN's produced by a number generator, which determines by the norm group of the ring of residue classes of modulus $p^m$ of the ring of Gaussian integers. That generator we call circular generator.

In present paper we continue to research the statistical properties of sequences of PRN's produced by the circular generator.

Our main aim here is to elucidate the motivation for constructing circular generator of the sequences of PRN's with some specific properties that be faster of its usage in cryptography. Our exposition focuses on some special measures of "randomness" with respect to which "the good" sequences have been produced by using of norm group $E_m$. A quantive measure of uniformity of distribution of a sequence may be the so-called discrepancy. Originated from a classical problem in Diophantine approximations this concept has found applications in the analysis of PR sequences on uniformity and unpredictability. From the well-known Turan-Erdös-Koksma inequality it is evident that the main tool in estimating discrepancy is the use of bounds on exponential sums over on elements of the sequence of PRN's. This motivates a construction this paper.

Before we proceed further we will fix the notation that will be used throughout this paper.

**Notation**

- Lower case Roman (respectively, Greek) letters usually denote rational (respectively, Gaussian) integers; in particular, $m$, $n$, $k$ are positive integers and $p$ is a rational prime number.
- We also define a *norm* over $Q(i)$ into $Q$ by $N(\alpha) = |\alpha|^2$.
- For the sake of convenience, we denote by $G$ the set of Gaussian integers.
- Let $Z_q$ (or $G_q$) denotes the ring of residue classes modulo $q$, and $Z_q^*$ (or $G_q^*$) denotes the multiplicative group in $Z$ (or $G_q$).
- If $x \in G_q^*$, we write $x^{-1}$ for the multiplicative inverse of $x$ mod $q$, i.e. $x^{-1}$ is an arbitrary Gaussian integer satisfying the condition $x \cdot x^{-1} \equiv 1 \pmod{q}$.

- As usual, $gcd(a, b)$ or $(a, b)$ stand for the greater common divisor of $a$ and $b$ (or, respectively, $\alpha$ and $\beta$ in $G$).
- Through $Z[x]$ (or $G[x]$) we denote the polynomial ring over $Z$ (or $G$). For $a \in Z$ ($\alpha \in G$) stand $\nu_p(a)$ (or $\nu_p(\alpha)$) if $p^{\nu(a)}|a$, $p^{\nu(a)+1} \not| a$.
- The fraction $\frac{a}{b}$, $(b, q) = 1$ of modulus $q$ means as $ab^{-1}$, where $b^{-1}$ is a multiplicative inverse modulo $q$.
- At last, $e_q(x)$ denotes $e^{2\pi i \frac{x}{q}}$.

## 2 Auxiliary results

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

Let $f(x)$ be a periodic function with a period $\tau$. For any $N \in N$, $1 \le N \le \tau$, we denote

$$S_N(f) := \sum_{x=1}^{N} e^{2\pi i f(x)}$$

**Lemma 1.** *The following estimate*

$$|S_N(f)| \le \max_{1 \le n \le \tau} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(f(x) + \frac{nx}{\tau}\right)} \right| \log \tau$$

*holds.*

This statement is well-known lemma about an estimate of uncomplete exponential sum by means of the complete exponential sum (see, [9]).

**Lemma 2.** *Let $p$ be a prime number and let $f(x)$ be a polynomial over $Z$*

$$f(x) = A_1 x + A_2 x^2 + p(A_3 x^3 + \cdots),$$

*and, moreover, let $\nu_p(A_2) = \alpha > 0$, $\nu_p(A_j) \ge \alpha$, $j = 3, 4, \ldots$. Then we have the following estimate*

$$\left| \sum_{x \in Z_{p^m}} e^{2\pi i \frac{f(x)}{p^m}} \right| = \begin{cases} p^{\frac{m+\alpha}{2}} & \text{if } \nu_p(A_1) \ge \alpha, \\ 0 & \text{else,} \end{cases}$$

(see, [16]).

**Lemma 3.** *Let $T \ge N \ge 1$ and $q \ge 2$ be integers, $\mathbf{y_k} \in \{0, 1, \ldots, q-1\}^d$ for $k = 0, 1, \ldots, N-1$; $\mathbf{t_k} = \frac{\mathbf{y_k}}{q} \in [0, 1)^d$. Then*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) \le \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_d(q)} \sum_{h_0 \in \left(-\frac{T}{2}, \frac{T}{2}\right]} \frac{1}{r(\mathbf{h}, q) r(h_0, T)} \times$$

$$\times \left| \sum_{k=0}^{T} e(\mathbf{h} \cdot \mathbf{t_k} + \frac{k h_0}{T}) \right|$$

(see, [12])

**Lemma 4.** *The discrepancy of $N$ arbitrary points $\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}} \in [0,1)^2$ satisfies*

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \dots, \mathbf{t_{N-1}}) \geq \frac{1}{2(\pi+2)|h_1 h_2|N} \left| \sum_{k=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_k}) \right|$$

*for any lattice point $\boldsymbol{h} = (h_1, h_2) \in Z^2$ with $h_1 h_2 \neq 0$.*

(It is the special version of Niederreiter result in [13]).

Let $p$ be a prime rational number, $p \equiv 3 \pmod 4$. Let us denote by $E_m$ the following subgroup of $G^*_{p^m}$

$$E_m := \{x \in G^*_{p^m} : \ N(x) \equiv \pm 1 \pmod{p^m}\}.$$

The subgroup $E_m$ we call the norm group in $G^*_{p^m}$.

**Lemma 5.** *Let $E_m$ be a norm group. Then $E_m$ is a cyclic group, $|E_m| = 2(p+1)p^{m-1}$, and let $u+iv$ be a generating element of $E_m$. Then exist $x_0, y_0 \in Z^*_m$ such that*

$$(u+iv)^{2(p+1)} \equiv 1 + p^2 x_0 + ipy_0, \ \ 2x_0 + y_0^2 \equiv -2p^2 x_0^2 \pmod{p^3}$$

*and we have modulo $p^m$ for any $t = 4, 5, \dots$*

$$\Re((u+iv)^{2(p+1)t}) = A_0 + A_1 t + A_2 t^2 + \cdots$$
$$\Im((u+iv)^{2(p+1)t}) = B_0 + B_1 t + B_2 t^2 + \cdots .$$

*Moreover,*

$$A_0 \equiv 1 \pmod{p^4}, \ B_0 \equiv 0 \pmod{p^4},$$
$$A_1 \equiv p^2 x_0 + \frac{1}{2} p^2 y_0^2 \equiv -\frac{5}{2} x_0^2 p^4 \pmod{p^5},$$
$$B_1 \equiv p y_0 (1 - p^2 x_0) \pmod{p^4},$$
$$A_2 \equiv -\frac{5}{2} x_0^2 p^2 \pmod{p^5},$$
$$B_2 \equiv \frac{5}{3} p^3 x_0 y_0 \pmod{p^4},$$
$$A_j \equiv B_j \equiv 0 \pmod{p^3}, \ j = 3, 4, \dots .$$

*(In greater details see [14])* □

Denote

$$(u+iv)^k = u(k) + iv(k), \ 0 \leq k \leq 2p+1,$$
$$(u+iv)^{2(p+1)t+k} \equiv \sum_{j=0}^{m-1} (A_j(k) + iB_j(k)) \pmod{p^m}.$$

It is clear, that

$$A_j(k) = A_j u(k) - B_j v(k); \ B_j(k) = A_j v(k) + B_j u(k).$$

Thus from Lemma 3 we infer.

**Corollary 1.** *For $k = 0, 1, \ldots, 2p+1$, we have*

$$
\begin{aligned}
&(u(k), p) = (v(k), p) = 1 \ if \ k \not\equiv 0 \pmod{\frac{p+1}{2}};\\
&u(0) = 1,\ v(0) = 0,\ (u(p+1), p) = 1,\ p \| v(p+1);\\
&u(k) \equiv 0 \pmod{p},\ (v(k), p) = 1 \ if \ k = \frac{p+1}{2} \ or \ \frac{3(p+1)}{2};\\
&u(k) = u(-k),\ v(k) = -v(-k).
\end{aligned}
$$

*Hence, for $k \not\equiv 0 \pmod{\frac{p+1}{2}}$ we have*

$$
\begin{aligned}
&A_0(k) \equiv u(k),\ B_0(k) \equiv v(k) \pmod{p},\\
&A_1(k) \equiv -py_0 v(k),\ B_1(k) \equiv py_0 u(k) \pmod{p^3},\\
&A_2(k) = -\frac{5}{2}x_0^2 p^u(k),\ B_2(k) \equiv -\frac{5}{2}x_0^2 p^2 v(k) \pmod{p^4},\\
&A_j(0) = A_j,\ B_j(0) = B_j,\ A_0(p+1) \equiv -1,\ B_0(p+1) \equiv 0 \pmod{p^3},\\
&p^2 \| A_1(p+1),\ p \| B_1(p+1),\ p^2 \| A_2(p+1),\ B_2(p+1) \equiv 0 \pmod{p^3},\\
&p \| A_1(k),\ p^2 \| B_1(k),\ p^2 \| A_2(k),\ B_2(k) \equiv 0 \pmod{p^3} \ if \ k = \frac{p+1}{2} \ or \ \frac{3(p+1)}{2}.
\end{aligned}
$$

□

Consider a finite sequence of $s$-dimensional points $\{x_n\}$, $n = 0, 1, \ldots, N-1$ from $[0,1)^s$,$s$ is a fix positive number. The discrepancy $D_N^{(s)}$ of $\{x_n\}$, $n = 0, 1, \ldots, N-1$ is defined as

$$D_N^{(s)} := \sup_{\Delta} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

where the supremum is taken over all subboxes $\Delta \subseteq [0,1)^s$, $A_N(\Delta)$ is the number of points $x_n$, $n = 0, 1, \ldots, N-1$ that hits the box $\Delta$, $|\Delta|$ is the volume of $\Delta$.

If with grows of $N$ a value $D_N^{(s)}$ tends to zero, we suggest that the sequence is equidistributed in $[0,1)^s$. It is well known that the property of statistical independence of PRN's $x_0, x_1, \ldots, x_{s-1}$ will be hold if and only if $(x_0, x_1, \ldots, x_{s-1})$ is uniformly distributed in $[0,1)^s$. For this reason we say that the sequence of numbers $x_0, x_1, \ldots, x_{N-1}$ from $[0,1)$ is unpredictability if the sequence of $s$-dimensional points $X_n^{(s)}$, $n = 0, 1, \ldots, N-s$, where $X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, is uniformly distributed in $[0,1)^s$ for $s = 1, 2, \ldots, S$, where $S$ is sufficiently barge number. More precisely, in this case one says that the sequence $\{x_n\}$ passes $s$-dimensional serial test on pseudorandomness. In practice sufficiently take $S = 4$.

For integers $d \geq 1$ and $q \geq 2$, let $C_d(q)$ be the set of all nonzero lattice points $\mathbf{h} = (h_1, \ldots, h_d) \in Z^d$ with $-\frac{q}{2} < h_j \leq \frac{q}{2}$ for $1 \leq j \leq d$. Define for

$\mathbf{h} \in C_d(q)$

$$r(h,q) = \begin{cases} 1 & if\ h = 0, \\ q \sin(\pi \frac{|h|}{q})\ if\ h \neq 0, \end{cases}$$

$$r(\mathbf{h},q) = \prod_{j=1}^{d} r(h_j,q)$$

**Lemma 6.** *Let $\{\boldsymbol{y}_n\}$ be the sequence of d-dimensional points in $\{0,1,\dots,q-1\}^d$ with a period $\tau$, and $\boldsymbol{y}_n = \frac{\boldsymbol{Y}_n}{q} \in [0,1)^d$. Then for any $N$, $1 \le N \le \tau$, we have*

$$D_N^{(d)}(\mathbf{y_0},\mathbf{y_1},\dots,\mathbf{y_{N-1}}) \le \frac{d}{q} + \frac{1}{N} \sum_{\mathbf{h}\in C_d(q)} \sum_{h_0 \in \left(-\frac{\tau}{2},\frac{\tau}{2}\right]} \frac{1}{r(\mathbf{h},q) r(h_0,q)} \times$$
$$\times \left| \sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{y_n} + \frac{nh_0}{\tau}) \right|,$$

*where $\boldsymbol{h}\cdot\boldsymbol{y}$ denotes the inner product of $\boldsymbol{h}$ and $\boldsymbol{y}$.*

**Lemma 7.** *Let $X_0, X_1, \dots, X_{N-1} \in [0,1)^d$, $d \ge 1$ with discrepancy $D_N^d$. Then for any nonzero $h = (h_1,\dots,h_d) \in Z^d$ we have*

$$\left| \sum_{n=0}^{N-1} e^{2\pi i \overline{h}\cdot X_n} \right| \le \frac{2}{\pi} \left( \left( \frac{\pi+1}{2} \right)^m - \frac{1}{2^m} \right) N D_N^{(d)} \prod_{j=1}^{d} \max(1, 2|h_j|),$$

*where $m$ is the number of nonzero coordinates of $\overline{h}$.*

(see, [13])

Lastly, we will make use the following sequences produced by a generating element $u+iv$ of the norm group $E_m$.

We select a random number $k \in \{0,1,\dots,2p+1\}$ and consider the sequence $\{(u+iv)^{2(p+1)n+k}\}$, $n = 0,1,\dots,p^{m-1}-1$.

Denote

$$x_n^{(k)} := \Re((u+iv)^{2(p+1)n+k}), \tag{1}$$
$$y_n^{(k)} := \Im((u+iv)^{2(p+1)n+k}). \tag{2}$$

Every sequence $\{x_n^{(k)}\}$ or $\{y_n^{(k)}\}$, $n = 0,1,\dots$, has a period $\tau = p^{m-1}$. From Lemma we obtain the description of elements of these sequences as the polynomials at $n$. Besides, taking into account, that

$$(u+iv)^{2(p+1)} = u_0 + iv_0,\ u_0 = 1 + p^2 x_0,\ v_0 = p y_0,\ (x_0,p) = (y_0,p) = 1$$

and

$$x_n^{(k)} \equiv x_{n-1}^{(k)} u_0 - y_{n-1}^{(k)} v_0 \pmod{p^m}, \tag{3}$$
$$y_n^{(k)} \equiv x_{n-1}^{(k)} v_0 - y_{n-1}^{(k)} u_0 \pmod{p^m} \tag{4}$$

may be achieved the representations of $x_n^{(k)}$, $y_n^{(k)}$ as the polynomials at $x_0$, $y_0$.

By virtue of the congruence $\left(x_n^{(k)}\right)^2 + \left(y_n^{(k)}\right)^2 \equiv (-1)^k \pmod{p^m}$ and recursion (3) we call the sequences (1) and (2) the circular sequences of PRN's and the recursions (3), (4) we call the circular generators.

## 3 Family of sequences of PRN's produced by circular generator

We generate the family of the sequences of congruential PRN's which associated with the sequences $\{x_n(k)\}$ and $\{y_n(k)\}$. Depending on a select $k \in \{0, 1, \dots, 2p+1\}$ we will construct the special sequences of PRN's. The several classes of sequences can be associated with the values of $k$:

(A) $k \not\equiv 0 \pmod{\frac{p+1}{2}}$;
(B) $k = 0$ or $p+1$;
(C) $k = \frac{p+1}{2}$ or $\frac{3(p+1)}{2}$.

Firstly, we consider the class $(A)$. The classes $(B)$ and $(C)$ may be consider by a similar way, but these classes have its specific.

So, let $\{x_n^{(k)}\}$, $\{y_n^{(k)}\}$ be the sequences produce the circular generator with $k \not\equiv 0 \pmod{\frac{p+1}{2}}$. In these cases $(u(k,p)) = (v(k),p) = 1$.

We denote

$$z_n^{(k)} := \frac{x_n^{(k)}}{1 + v_0(k) y_n^{(k)}} \pmod{p^m}, \tag{5}$$

where $v_0(k) = v(k) + p^2 v_1(k)$, $(v_1(k), p) = 1$.

This definition is reasonable by virtue of the fact that

$$1 + v_0(k) y_n^{(k)} \equiv 1 + v_0(k) B_0(k) \equiv 1 + v_0^2(k) \equiv -u^2(k) \pmod{p}$$
$$v_0(k) \sum_{j=1}^{m-1} B_j(k) n^j \equiv 0 \pmod{p}.$$

And hence, denoting $(u(k)^{-1})^2 = u(k)^{-2} \pmod{p^m}$, we have

$$z_n^{(k)} \equiv -(u(k))^{-2}(A_0(k) + A_1(k)n + \cdots)\Bigg(1 + (u(k))^{-2} v_0(k) B_1(k) n +$$
$$+ u^{-2}(k)\left(v_0(k) B_2(k) n^2 + u^{-2}(k) v_0^2(k) B_1(k)\right) n^2 + \cdots\Bigg) \pmod{p^m}.$$

Now, after simple calculations, we get

$$z_n^{(k)} = -(u(k))^{-2} \sum_{j=0}^{M} A_j^{(k)} n^j,$$

where

$$A_1^{(k)} = p u(k)^{-1} y_0 - p y_0 v(k) u(k)^{-2},$$
$$A_2^{(k)} = v_0(k) A_0(k) B_2(k) + u(k)^{-2} v_0(k)^2 A_0(k) B_1^2(k) +$$
$$+ v_0(k) A_1(k) B_1(k) + A_2(k),$$
$$A_j^{(k)} \equiv 0 \pmod{p^3},\ j = 3, 4, \dots.$$

So, we obtain modulo $p^m$

$$z_n^{(k)} \equiv (u(k))^{-1}\left[\text{free term} + p^2 y_0 v_1(k) n + p^2 c_2(k) n^2 + p^3 G(n)\right], \tag{6}$$

where $G(n) \in Z_{p^m}[n]$, and

$$c_2(k) = y_0^2 \cdot (-2x_0u^{-1}(k)v^2(k) - 10x_0^2u^2(k) - 10x_0^2u^{-1}(k)v(k) - u^{-3}(k)v^2(k)).$$

The relation (6) defines the representation of $z_n^{(k)}$ as the polynomial at $n$.

In case of (B) we consider the sequence $\{z_n^{(k)}\}$, $z_n^{(k)} = \frac{x_n^{(k)}}{y_n^{(k)}}$.

Finally, in case of (C) we let

$$z_n^{(k)} = \frac{x_n^{(k)}}{1 + y_n^{(k)}}$$

and similarly to (A) we infer the representation $z_n^{(k)}$ as polynomial at $n$.

This allows us to state and prove the following theorem.

**Theorem 1.** *Let $h_1, h_2, j \in Z$, $(h_1, h_2, p^m) = p^\ell$, $0 \le j \le 2p+1$. The following estimate*

$$|S_j(h_1, h_2)| := \left| \sum_{n=0}^{p^{m-1}-1} e_{p^m}(h_1 z_n^{(k)} + h_2 z_{n+j}^{(k)}) \right| \le p^{\frac{m+\ell}{2}}$$

*holds.*

*Proof.* Without less of generality that $(h_1, h_2, p^m) = 1$, using the relations (6) we can write for $k \not\equiv 0 \pmod{\frac{p+1}{2}}$

$$h_1 z_n^{(k)} + h_2 z_{n+j}^{(k)} \equiv (u(k))^{-2} \left[\text{free term} + p^2((h_1+h_2)y_0v_0(k) + 2{\cdot}h_2c_2(k))n + \right.$$
$$\left. + p^2(h_1+h_2)c_2(k)n^2 + p^3G_1(n)\right] \pmod{p^m}.$$

By the condition $(h_1, h_2, p^m) = 1$, it follows that the congruences

$$(h_1+h_2)y_0v_0(k) + 2{\cdot}h_2c_2(k) \equiv 0 \pmod p$$
$$(h_1+h_2)c_2(k) \equiv 0 \pmod p$$

cannot be realized simultaneously. Thus, by Lemma 2, we infer

$$|S_j(h_1, h_2)| \le \begin{cases} 0 & if\ h_1 + h_2 \equiv 0 \pmod p, \\ p^{\frac{m}{2}} & if\ h_1 + h_2 \not\equiv 0 \pmod p. \end{cases} \tag{7}$$

The same estimate we obtain for the rest values of $k$.

□

**Corollary 2.** *The discrepancy of the sequence $\left\{\frac{X_n^{(s)}}{p^{m-1}}\right\}$, $s = 1, 2$, has the following bound*

$$D_N^{(s)} \le \frac{s}{p^{m-1}} + \frac{2p^{\frac{m-1}{2}}}{N}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^s,\ 0 < N \le \tau, \tag{8}$$

*where $X_n^{(s)} = \left(z_n^{(k)}, \dots, z_{n+s-1}^{(k)}\right)$.*

This assertion follows from Lemma 4 and Theorem 1. Now we prove a lower estimate $D_N^{(2)}$.

**Theorem 2.** *Let $p$ be a prime number, $p \equiv 3 \pmod 4$ and let $z_n^{(k)}$ defined by the relation (5), $k \not\equiv 0 \pmod{\frac{p+1}{2}}$. Then for the sequence $\{w_n^{(k)}\}$, $w_n^{(k)} = \frac{z_n^{(k)}}{p^m}$, $n = 0, 1, \dots, \tau - 1$, we have*

$$D_\tau^{(2)}(W_0^{(k)}, W_1^{(k)}, \dots, W_{\tau-1}^{(k)}) \geq \frac{1}{4(\pi+2)} p^{-\frac{m-1}{2}}, \tag{9}$$

*where $W_n^{(k)} = (w_n^{(k)}, w_{n+1}^{(k)})$, $n = 0, 1, \dots, \tau - 1$.*

*Proof.* We take $h_1 = h_2 = 1$. Then by Theorem 1 with $j = 1$ and Lemma 5, we at one obtain

$$D_\tau^{(2)} \geq \frac{1}{2(\pi+2)} \tau^{-\frac{1}{2}} = \frac{1}{2(\pi+2)} p^{-\frac{m-1}{2}}.$$

□

*Remark 1.* It is straightforward to verify that all that we said in the case the sequence produced of the relation (5) also holds for the sequence produced by the congruence

$$z_n^{(k)} \equiv u_0(k) x_n^{(k)} + v_0(k) y_n^{(k)} \pmod{p^m} \tag{10}$$

with

$$u_0(k) = u(k) + p^2 u_1(k),\ v_0(k) = v(k) + p^2 v_1(k),\ (u_1(k), p) = (v_1(k), p) = 1.$$

Theorem 1 and 2 show that, in general, the upper bound is the best possible up to the logarithmic factor for circular congruential sequence $\{(w_n^{(k)}, w_{n+1}^{(k)})\}$, $n \geq 0$, defined by congruence (5) (or (10)).

*Remark 2.* The relations (3), (4) make it possible to drive a representations $x_n^{(k)}$, $y_n^{(k)}$ and consequently $z_n^{(k)}$ as polynomials at $x_0$, $y_0$. Thus it may be well to construct non-trivial estimates of exponential sums over generating element of the norm group $E_m$.

## References


1. J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. *Internat. Statist. Rev.*, 60, 167–176, 1992.
2. J. Eichenauer-Herrmann. Pseudorandom number generation by nonlinear methods. *Internat. Statist. Rev.*, 63, 247–255, 1995.
3. J. Eichenauer-Herrmann, H. Grothe. A New Inversive Congruential Pseudorandom Number Generator with Power of Two Modulus. *ACM Transactions of Modelling and Computer Simulation*, 2, **1**, 1–11, 1992.
4. J. Eichenauer and J. Lehn. A non-linear congruential pseudorandom number generator. *Statist. Hefte*, 27, 315–326, 1986.

5. J. Eichenauer, J. Lehn and A. Topuzoğlu. A nonlinear congruential pseudorandom number generator with power of two modulus. *Math. Comp.*, 51, 757–759, 1988.
6. J. Eichenauer-Herrmann, E. Herrmann and S. Wegenkittl. A survey of quadratic and inversive congruential pseudorandom numbers, in: Monte Carlo and Quasi-Monte Carlo Methods, 1996, H. Niederreiter et al(eds.), Lecture Notes in Statist. *Springer, New York*, 127, 66–97, 1998.
7. J. Eichenauer-Herrmann and A. Topuzoğlu. On the period of congruential pseudorandom number sequences generated by inversions. *J. Comput. Appl. Math.*, 31, 87–96, 1990.
8. T. Kato, L.-M. Wu, N. Yanagihara. On a nonlinear congruential pseudorandom number generator. *Math. of Comp.*, 65, **213**, 227–233, 1996.
9. N.M. Korobov N.M.. *Trigonometric Sums and Their Applications [in Russian]*. Nauka, Moscow, 1989.
10. D. E. Knuth. *The Art of Computer Programming, Vol. 2:Seminumerical algorithms*. Addison-Wesley, 1998.
11. H. Niederreiter. Nonlinear methods for pseudorandom number and vector generation. *Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems, Springer, Berlin*, 374, 145–153, 1992.
12. H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, Pa., 1992.
13. H. Niederreiter. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers. *Math. of Comput.*, 55, **191**, 277–287, 1990.
14. S.P. Varbanets. The norm Kloosterman sums over $Z[i]$. *Anal. Probab. Mathods Number*, 3, **11**, 225–239, 2006.
15. S. Varbanets. On inversive congruential generator for pseudorandom numbers with prime power modulus. *Annales Univ. Sci. Budapest, Sect. Comp.*, 29, 277–296, 2008.
16. P. Varbanets, S. Varbanets. Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus. *Vorono's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Kyiv, Ukraine, September 22-28, 2008*, 4, **1**, 112–130, 2008.
17. Sergey Varbanets, Exponential sums on the sequences of inversive congruential pseudorandom numbers. *Siauliai Math. Semin.*, 3, **11**, 247–261, 2008.
18. P. Varbanets, S. Varbanets. Generalizations of Inversive Congruential Generator, Analytic and probabilistic methods in number theory. *Proceedings of the* $5^{th}$ *international conference in honour of J. Kubilius, Palanga, Lithuania, September 4–10, 2011, Vilnius: TEV.*, 265–282, 2012.
19. Sergey Varbanets, Circular generator of PRNs. *7th CHAOS Conference Proceedings, 7-10 June 2014, Lisbon, Portugal*, 523–532, 2014.