Annales Univ. Sci. Budapest., Sect. Comp. 29 (2008) 277-296

ON INVERSIVE CONGRUENTIAL GENERATOR FOR PSEUDORANDOM NUMBERS WITH PRIME POWER MODULUS

S. Varbanets (Odessa, Ukraine)

Dedicated to the 70th birthday of Professor Imre Kátai

Abstract. Generalization of the inversive congruential generator of pseudorandom numbers on the prime module is considered and the trigonometrical sums on sequence of pseudorandom numbers are estimated.

1. Introduction

A pseudorandom number generator is an important brick of a stochastic imitation, e.g. the computation of an integral by the Monte-Carlo method or the construction of the cryptographic keys.

A classical standard method of generating uniform pseudorandom numbers in the interval $[0, 1)$ is the linear congruential method, which is given as follows:

For a large modulus M, let $\mathbb{Z}_M$ be the group of residue classes modulus M. A sequence $\{y_n\}$ of integers in $\mathbb{Z}_M$ is generated by the linear recursion:

$$y_{n+1} \equiv ay_n + b \pmod{M}, \quad n = 0, 1, \dots, \tag{1}$$

where $a, b \in \mathbb{Z}_M$. The pseudorandom numbers are obtained by the normalization

$$x_n = \frac{y_n}{M}. \tag{2}$$

This linear congruential generator is widely used, and has been investigated by several authors ([1], [13]). However, there is some drawback owing to the

linearity of the recursion (see [1]). This state affairs provided the motivation for several recent proposals of nonlinear congruential methods in order to overcome the deficiencies of the linear congruential method (see [2], [6], [7], [8], [15]).

A particularly promising nonlinear method is the inversive congruential method where nonlinearity is achieved by employing the operation of multiplicative inversion with respect to a given modulus.

Three types of inversive congruential generators can be distinguished, depending on whether the modulus is a prime (see [2], [3], [4]), an odd prime power (see [9], [11]), or a power of two (see [7], [15], [17]).

In the works of Chou ([4], [5]), Eichenauer and Lehn ([2]), Flahive and Niederreiter ([6]), Niederreiter ([3]) has been studied the problem of when the sequence of pseudorandom numbers (generated by the pseudorandom generator) has the maximal period. Niederreiter and Shparlinski ([11]) considered the special exponential sums on inversive congruential pseudorandom numbers with prime power modulus and obtained nontrivial results concerning the distribution these numbers in part of the period. For surveys of results and applications of inversive congruential numbers see [12]-[14].

In the present paper a new inversive congruential method with prime power modulus is introduced and investigated.

Let $p \geq 3$ be prime and $m \geq 2$ an integer, and let R_m (accordingly, R_m^*) denote the group of residue classes (accordingly, the group of reduced residue classes) modulo p^m. For $a \in R_m^*$, $b, c \in R_m$, $b \equiv c \equiv 0 \pmod{p}$, we consider the maps Ψ_r, $r = 0, 1, 2, \ldots$, $R_m^* \to R_m$ of the form

$$\Psi_{r+1}(\omega) = \frac{a}{\Psi_r(\omega)} + b + c\omega, \quad \Psi_0(\omega) = \omega \tag{3}$$

(here and in the following, it will be convenient to write $\frac{u}{v}$ for the expression uv^{-1} in a multiplicative abelian group R_m^*).

The condition $b \equiv c \equiv 0 \pmod{p}$ guarantees that $(\Psi_r(\omega), p) = 1$ if $(a, p) = (\omega, p) = 1$.

The recursion (3) generalizes the inversive congruential generator with prime power modulus (see [9], [11], [17]). But now for $c \not\equiv 0 \pmod{p^m}$ we obtain that $\Psi_{k+1}(\omega) \neq \Psi_1(\Psi_k(\omega))$ as in [11]. Therefore the method of proof of estimate of the discrepancy for the sequence $\{\frac{\omega_n}{p^m}\}$ is different.

Notations. We denote $e_{p^m}(x) = e^{2\pi i \frac{x}{p^m}}$; ω^{-1} means that $\omega\omega^{-1} \equiv 1 \pmod{p^m}$ for $(\omega, p) = 1$; $\nu_p(n)$ means $p^{\nu_p(n)} \| n$.

2. Preliminaries

For $k \in \mathbb{Z}$, $k \geq 0$, we consider a map Ψ_k, given by (3).

Lemma 1. *For any integer k, $k \geq 0$, we have*

$$\Psi_k(\omega) = \frac{A_0^{(k)} + A_1^{(k)}\omega + \cdots + A_{k+1}^{(k)}\omega^{k+1}}{B_0^{(k)} + B_1^{(k)}\omega + \cdots + B_k^{(k)}\omega^k}, \tag{4}$$

moreover,

$$\begin{aligned} &\left(A_0^{(k)}, p\right) = \left(B_1^{(k)}, p\right) = 1, \ A_i^{(k)} \equiv B_j^{(k)} \equiv 0 \,(mod\ p), \\ &\qquad i = 1, 2, \ldots, k+1, \ j = 0, 2, 3, \ldots, k, \ if\ k\ is\ odd\ integer; \\ &\left(A_1^{(k)}, p\right) = \left(B_0^{(k)}, p\right), \ A_i^{(k)} \equiv B_j^{(k)} \equiv 0 \,(mod\ p), \\ &\qquad i = 0, 2, 3, \ldots, k+1, \ j = 1, 2, \ldots, k, \ if\ k\ is\ even\ integer. \end{aligned} \tag{5}$$

Furthermore, for $k = 0, 1, 2, \ldots$

(6)

$$\begin{cases} A_0^{(k+2)} = (a+b^2)A_0^{(k)} + abB_0^{(k)}, \\ A_1^{(k+2)} = 2bcA_0^{(k)} + (a+b^2)A_1^{(k)} + acB_0^{(k)} + abB_1^{(k)}, \\ A_i^{(k+2)} = c^2A_{i-2}^{(k)} + 2bcA_{i-1}^{(k)} + (a+b^2)A_i^{(k)} + acB_{i-1}^{(k)} + abB_i^{(k)}, \\ i = 2, 3, \ldots, k+1; \\ \\ A_{k+2}^{(k+2)} = 2bcA_{k+1}^{(k)} + c^2A_{k+1}^{(k)}, \\ A_{k+3}^{(k+2)} = c^2A_{k+1}^{(k)}, \\ B_0^{(k+2)} = aB_0^{(k)} + bA_0^{(k)}, \\ B_j^{(k+2)} = aB_j^{(k)} + bA_j^{(k)} + cA_{j-1}^{(k)}, \ j = 1, 2, \ldots, k; \\ B_{k+1}^{(k+2)} = bA_{k+1}^{(k)} + cA_k^{(k)}, \\ B_{k+2}^{k+2} = cA_{k+1}^{(k)}, \\ A_0^{(0)} = 0, \ B_0^{(0)} = 1, \ A_1^{(0)} = 1, \ B_1^{(0)} = 0, \ A_i^{(0)} = B_i^{(0)}, \ i > 1; \\ \\ A_0^{(1)} = a, \ B_0^{(1)} = 0, \ A_1^{(1)} = b, \ B_1^{(1)} = 1, \ A_2^{(1)} = c, \ B_2^{(1)} = 0, \\ A_i^{(1)} = B_i^{(1)} = 0, \ i > 2; \\ \\ A_0^{(2)} = ab, \ A_1^{(2)} = (a + ac + b^2), \ A_2^{(2)} = 2bc, \ A_3^{(2)} = c^2, \ B_0^{(2)} = a, \ B_1^{(2)} = b, \\ B_2^{(2)} = c, \ A_i = B_i = 0, \ i > 3, \ j > 2. \end{cases}$$

Proof. The formula (4) and the relations (6) can be shown by induction on k from (3). And then (5) follows from (6).

Lemma 2. *Let $A_i^{(k)}$, $B_i^{(k)}$ be those as in Lemma 1 and let $bc \equiv 0\,(mod\ p^m)$, $\nu_p(b) \le \nu_p(c)$. Then we have*

$$\begin{aligned}\Psi_{2k}(\omega) =& \frac{A_0^{(2k)} + A_1^{(2k)}\omega}{B_0^{(2k)} + B_1^{(2k)}\omega + B_2^{(2k)}\omega^2},\\ \Psi_{2k+1}(\omega) =& \frac{C_0^{(2k+1)} + C_1^{(2k+1)}\omega + C_2^{(2k+1)}\omega^2}{D_0^{(2k+1)} + D_1^{(2k+1)}\omega},\end{aligned} \tag{7}$$

where

$$\begin{aligned}A_0^{(2k)} =& ka^k b + \overline{A}_0^{(2k)} b^3,\ \ A_1^{(2k)} = a^k + k\overline{A}_1^{(2k)} b^2;\\ B_0^{(2k)} =& a^k + \overline{B}_0^{(2k)} b^2,\ \ B_1^{(2k)} = ka^{k-1}b + \overline{B}_1^{(2k)} b^3,\ \ B_2^{(2k)} = ka^{k-1}c;\\ C_0^{(2k+1)} =& a^{k+1}b + \overline{C}_0^{(2k+1)} b^2,\ \ C_1^{(2k+1)} = (k+1)a^k b + \overline{C}_1^{(2k+1)} b^3,\\ C_2^{(2k+1)} =& (k+1)a^k c;\\ D_0^{(2k+1)} =& ka^k b + \overline{D}_0^{(2k+1)} b^3,\ \ D_1^{(2k+1)} = a^k + ka^k c + \overline{D}_1^{(2k+1)} b^2.\end{aligned} \tag{8}$$

Proof. We denote

$$A = \begin{pmatrix} a+b^2 & ab \\ b & a \end{pmatrix},\quad B = \begin{pmatrix} 0 & ac \\ c & 0 \end{pmatrix}. \tag{9}$$

Since $bc \equiv 0\,(\mathrm{mod}\ p^m)$ and $\nu_p(b) \le \nu_p(c)$, we have $c^2 \equiv 0\,(\mathrm{mod}\ p^m)$. Thus by Lemma 1 we infer after short computations

$$\begin{pmatrix} A_0^{(2k+2)} \\ B_0^{(2k+2)} \end{pmatrix} = A^{k+1} \begin{pmatrix} A_0^{(0)} \\ B_0^{(0)} \end{pmatrix} = A^{k+1} \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{10}$$

$$\begin{pmatrix} A_1^{(2k+2)} \\ B_1^{(2k+2)} \end{pmatrix} = A \begin{pmatrix} A_1^{(2k)} \\ B_1^{(2k)} \end{pmatrix} + B \begin{pmatrix} A_0^{(2k-2)} \\ B_0^{(2k-2)} \end{pmatrix} = \tag{11}$$

$$= A^k \begin{pmatrix} A_1^{(2)} \\ B_1^{(2)} \end{pmatrix} + ka^{k-1}c \begin{pmatrix} A_0^{(1)} \\ B_0^{(1)} \end{pmatrix} = A^k \begin{pmatrix} a+ac+b^2 \\ b \end{pmatrix} + ka^{k-1}c \begin{pmatrix} a \\ 0 \end{pmatrix}.$$

From (9) we can produce

$$A = a(E + A_1),\ E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A_1 = \begin{pmatrix} a_1 b & b \\ a_1 & 0 \end{pmatrix},\ a_1 \equiv ba^{-1} \pmod{p^m},$$

$$A^k \equiv a^k \left(E + kA_1 + \cdots + \begin{pmatrix} k \\ M \end{pmatrix} A_1^M \right) \pmod{p^m}, \tag{12}$$

$$A_1^j \equiv 0 \pmod{p^{\mu(j-1)}},$$

where $\mu = \nu_p(b)$, $M = \left[\frac{m}{\mu}\right]$.

Now from (3), (10)-(12) the assertion of Lemma 2 easily follows.

Remark. In general case, let $b^\ell c \equiv 0 \pmod{p^m}$, $b^{\ell-1}c \not\equiv 0 \pmod{p^m}$, $\ell \geq 2$ $\nu_p(b) = \mu \leq \nu_p(c)$. Then we obtain similarly

$$\Psi_{2k}(\omega) = \frac{A_0^{(2k)} + A_1^{(2k)}\omega + \cdots + A_\ell^{2k}\omega^\ell}{B_0^{(2k)} + B_1^{(2k)}\omega + \cdots + B_{\ell+1}^{(2k)}\omega^\ell},$$

$$\begin{pmatrix} A_i^{(2k+2)} \\ B_i^{(2k+2)} \end{pmatrix} = A^{k+1-i} \begin{pmatrix} A_i^{(2i)} \\ B_i^{(2i)} \end{pmatrix} + B_k \begin{pmatrix} A_{i-1}^{(2i-2)} \\ B_{i-1}^{(2i-2)} \end{pmatrix} + C_k \begin{pmatrix} A_{i-2}^{(2i-4)} \\ B_{i-2}^{(2i-4)} \end{pmatrix},\ a \leq i \leq \ell,$$

where the matrices B_k, C_k satisfy $B_k \equiv C_k \pmod{p^\mu}$.

Lemma 3. *For every $k = 1, 2, \ldots$, the map $\Psi_k(\omega)$ is a permutation of R_m^*.*

Proof. For $c \equiv 0 \pmod{p^m}$ the assertion of lemma is clear. Let $\nu_p(c) < m$. From $b \equiv c \equiv 0 \pmod{p}$ it follows $(\Psi_k(\omega), p) = 1$ for every $\omega \in R_m^*$. Further, let $k = 1$. From the congruence

$$a\omega_1^{-1} + b + c\omega_1 \equiv a\omega_2^{-1} + b + c\omega_2 \pmod{p^m}$$

it follows that $a\omega_1^{-1} \equiv a\omega_2^{-1}$ and, hence, $\omega_1 \equiv \omega_2 \pmod{p}$. Set $\omega_2 = \omega_1 + p\delta_1$. Then $\omega_2^{-1} \equiv \omega_1^{-1}(1 - p\delta_1\omega_1^{-1}) \pmod{p^2}$ (here $\omega_1^{-1}\omega_1 \equiv 1 \pmod{p^m}$). Therefore

$$a\omega_1^{-1} + b + c\omega_1 \equiv a(\omega_1^{-1} - p\delta_1\omega_1^{-2}) + b + c(\omega_1 + p\delta_1) \pmod{p^2} \Rightarrow$$

$$\Rightarrow p\delta_1\omega_1^{-2} \equiv 0 \pmod{p^2} \Rightarrow \delta_1 = p\delta_2 \Rightarrow \omega_2 = \omega_1 + p^2\delta_2 \Rightarrow$$

$$\Rightarrow \omega_2^{-1} \equiv \omega_1^{-1} - p^2\delta_2\omega_1^{-2} \pmod{p^3}.$$

Now from the congruence

$$a\omega_1^{-1}+b+c\omega_1\equiv a(\omega_1^{-1}-p^2\delta_2\omega_1^{-2})+b+c(\omega_1+p^2\delta_2)\pmod{p^3}$$

we obtain $\omega_2=\omega_1+p^3\delta_3$ similarly. Through m steps we obtain $\omega_2\equiv$ $\equiv\omega_1\pmod{p^m}$, i.e. for k=1 the assertion of lemma proved.

Suppose that for $k-1$ we have

$$\Psi_{k-1}(\omega_1)\equiv\Psi_{k-1}(\omega_2)\pmod{p^m}\Leftrightarrow\omega_1\equiv\omega_2\pmod{p^m}.$$

Consider the congruence

$$\frac{a}{\Psi_{k-1}(\omega_1)}+b+c\omega_1\equiv\frac{a}{\Psi_{k-1}(\omega_2)}+b+c\omega_2\pmod{p^m}.$$

If $\omega_1\equiv\omega_2\pmod{p^{m-\nu_p(c)}}$ then we have

$$\Psi_{k-1}(\omega_1)\equiv\Psi_{k-1}(\omega_2)\pmod{p^m}\Rightarrow\omega_1\equiv\omega_2\pmod{p^m}.$$

Suppose that $\omega_1\not\equiv\omega_2\pmod{p^{m-\nu_p(c)}}$. But we have from

$$\begin{aligned}
&\frac{a}{\Psi_{k-1}(\omega_1)}+b+c\omega_1\equiv\frac{a}{\Psi_{k-1}(\omega_2)}+b+c\omega_2\pmod{p^{\nu_p(c)}}\Rightarrow\\
&\frac{a}{\Psi_{k-1}(\omega_1)}\equiv\frac{a}{\Psi_{k-1}(\omega_2)}\pmod{p^{\nu_p(c)}}\Rightarrow\omega_1\equiv\omega_2\pmod{p^{\nu_p(c)}}\Rightarrow\\
&\frac{a}{\Psi_{k-1}(\omega_1)}+b+c\omega_1\equiv\frac{a}{\Psi_{k-1}(\omega_2)}+b+c\omega_2\pmod{p^{2\nu_p(c)}}\Rightarrow\\
&\Rightarrow\omega_1\equiv\omega_2\pmod{p^{2\nu_p(c)}}.
\end{aligned}$$

Through $\left[\frac{m}{\nu_p(c)}\right]$ steps we obtain the contradiction with supposition $\omega_1\not\equiv$ $\not\equiv\omega_2\pmod{p^{m-\nu_p(c)}}$. The proof of Lemma 3 is complete.

Lemma 4. *Let $Au+pBu^2+p^2(du^3+\cdots)$ be a polynomial with integer coefficients, $(B,p)=1$. Then*

$$\left|\sum_{u\in R_m}e_{p^m}(Au+pBu^2+p^2(du^3+\cdots))\right|\ll\begin{cases}0 & \text{if } (A,p)=1,\\ p^{\frac{m+1}{2}} & \text{if } (A,p)=p.\end{cases}$$

Proof. This assertion can be obtained by a substitution

$$u=v+p^{\left[\frac{m}{2}\right]}z,\ u=0,1,\dots,p^{m-\left[\frac{m}{2}\right]}-1,$$

and by the estimation of the Gaussian sum.

Lemma 5. *Let $f(\omega) = B\omega + C\omega^2 + p(D\omega^3 + \cdots)$ be polynomial over $\mathbb{Z}$, and let $(C, p) = 1$. Then for any $A \in \mathbb{Z}$ we have*

$$T = \left| \sum_{\omega \in R_m^*} e_{p^m}(A\omega + f(\omega^{-1})) \right| \leq 4p^{\frac{m}{2}}.$$

Proof. We put $\omega^{-1} = u + p^{m-1}z$, $\omega \equiv u^{-1} - p^{m-1}u^{-2}z \pmod{p^m}$, $\omega^{-2} = u^2 + 2p^{m-1}uz$. Hence, we infer

$$A\omega + f(\omega^{-1}) \equiv$$

$$\equiv (Au^{-1} + Bu + Cu^2 + p(Du^3 + \cdots)) + p^{m-1}(-u^{-2}A + B + 2Cu)z \pmod{p^m}.$$

Therefore by Lemma 4

$$T = \left| \sum_{u \in R_{m-1}^*} e_{p^m}(Au^{-1} + Bu + Cu^2 + p(Du^3 + \ldots)) \cdot \right.$$

$$\left. \cdot \sum_{z \in R_1} e_p((-Au^{-2} + B + 2Cu)z) \right| \leq$$

$$\leq p \left| \sum_{\substack{u_0 \in R_1^* \\ Au_0^{-1} - Bu_0 - 2Cu_0^2 \equiv 0 \pmod{p}}} e_{p^m}(Au_0^{-1} + Bu_0 + Cu_0^2 + p(Du^3 + \cdots)) \times \right.$$

$$\left. \times \sum_{v \in R_{m-2}} e_{p^{m-2}}(A_1 v + A_2 v^2 + p(A_3 v^3 + \cdots)) \right| \leq 4p^{\frac{m}{2}},$$

(here, $A_1 = \frac{-Au_0^{-1} + B + 2Cu_0}{p} \in \mathbb{Z}$, $A_2 = C$, $A_j \in \mathbb{Z}$, $j = 3, 4, \ldots$).

Consider the sequence ω_n, $n = 0, 1, 2, \ldots$, defined by the recurrence relation

$$\omega_n = \frac{a}{\omega_{n-1}} + b + c\omega, \qquad \omega_0 = \omega \in R_m^*, \tag{13}$$

i.e. $\omega_n = \Psi_n(\omega)$.

From Lemmas 1 and 3 it follows that this sequence is purely periodic with least period length $\tau \le p^{m-1}(p-1)$, τ is even integer. In the case $c \equiv 0 \pmod{p^m}$ W.-S. Chou [5] investigated dependence τ on a, b, ω. Below we shall study τ as function of a, b, c and ω.

For positive integer h we put

$$\sigma_{k,\ell}(h, p^m) = \sigma_{k,\ell} := \sum_{\omega \in R_m^*} e_{p^m}(h(\Psi_k(\omega) - \Psi_\ell(\omega))). \tag{14}$$

Lemma 6. *Let k, ℓ are non-negative integers of different parity and let $h \in \mathbb{Z}$, $(h, p^m) = p^\delta$, $\delta < m$. Then we have*

$$|\sigma_{k,\ell}| \le 2p^{\frac{m+\delta}{2}} \tag{15}$$

Proof. Without loss of generality we can account that $(h, p^m) = 1$ and $k = 2k_1$, $\ell = 2\ell_1 + 1$. From Lemma 1 we easy infer

$$\Psi_{2k_1}(\omega) = \frac{k_1 a^{k_1} b + (a^{k_1} + p^\mu A_1)\omega + p^\mu(A_1\omega^2 + pA_3\omega^3 + \cdots)}{(a^{k_1} + p^\mu B_0) + (ka^{k_1} b + p^\mu B_2)\omega + p^\mu(B_2\omega^2 + \cdots)},$$

$$\Psi_{2\ell_1+1}(\omega) = \tag{16}$$

$$= [(a^{\ell_1+1} + C_0 p^\mu) + ((\ell_1+1)a^\ell b + c_1 p^{\mu+\nu_p(b)})\omega + ((\ell+1)a^\ell c + p^{\nu_p(c)+\nu_p(b)} C_2)\omega^2 + \cdots]$$

$$\cdot[(\ell_1 a^{\ell_1} b + D_0 b^3) + (a^{\ell_1} + p^{\min(\nu_p(c), 2\nu_p(b))} D_1)\omega + p^{\nu_p(b)+\nu_p(c)}(D_2\omega^2 + \cdots)]^{-1},$$

where $\mu = \min(\nu_p(b), \nu_p(c))$.

We multiply the numerator and denominator of $\Psi_{2k_1}(\omega)$ on $(a^{k_1} + p^\mu B_0)^{-1} \pmod{p^m}$, and similarly multiply numerator and denominator of $\Psi_{2\ell_1+1}(\omega)$ on $((a^{\ell_1} + p^{\min(\nu_p(c), 2\nu_p(b))})\omega)^{-1} \pmod{p^m}$. Since

$$(1 + p(A\omega + \cdots))^{-1} \equiv 1 - p(A\omega + \cdots) + p^2(A\omega + \cdots)^2 + \cdots \pmod{p^m},$$

$$(1 + pB\omega^{-1} + pB'\omega + \cdots)^{-1} \equiv$$

$$\equiv 1 - p(B\omega^{-1} + B'\omega + \cdots) + p^2(B\omega^{-1} + B'\omega + \cdots)^2 + \cdots \pmod{p^m}$$

we obtain, after short computations

$$\Psi_{2k_1}(\omega) - \Psi_{2\ell_1+1}(\omega) \equiv E_0 + E_1\omega + E_{-1}\omega^{-1} + p^\mu G(\omega, \omega^{-1}) \pmod{p^m}, \tag{17}$$

where $E_1 \equiv 1 \pmod{p^\mu}$, $E_{-1} \equiv a \pmod{p^\mu}$, $G(x, y)$ is a polynomial on x, y.

We denote $E(\omega) = \Psi_{2k_1}(\omega) - \Psi_{2\ell_1+1}(\omega)$. Put $\omega = u + p^{m-1}z$, $u \in R^*_{m-1}$, $z = 0, 1, \ldots, p-1$. Then

$$\omega^j \equiv u^j + jp^{m-1}u^{j-1}z, \quad \omega^{-j} \equiv u^{-j} - jp^{m-1}u^{-j-1}z \pmod{p^m}.$$

Hence, we have after simple computations

$$\sigma_{k,\ell} = \sum_{u \in R^*_{m-1}} \sum_{z=0}^{p-1} e_{p^m}\left(E_1 u + E_{-1}u^{-1} + p^\mu(E'_2 u^2 + E'_{-2}u^{-2} + \cdots) + \right.$$

$$\left. + p^{m-1}(E_1 - E_{-1}u^{-2})z\right) = \tag{18}$$

$$= p \sum_{\substack{u \in R^*_{m-1} \\ u^2 \equiv E_1^{-1}E_{-1} \pmod{p}}} e_{p^m}(E_1 u + E_{-1}u^{-1} + p^\mu(E'_2 u^2 + E'_{-2}u^{-2} + \cdots)).$$

Let u_1, u_2 be two solutions of the congruence

$$u_i^2 \equiv E_{-1}E_1^{-1} \pmod{p^{m-1}}, \ i = 1, 2.$$

Put $u = u_i + pv$, $v \in R_{m-2}$. Then we obtain

$$\sigma_{k,\ell} = p \sum_{i=1}^{2} \sum_{v \in R_{m-2}} e^{2\pi i h \frac{F_1^{(i)}(v) + F_2^{(i)}(v)}{p^{m-2}}}, \tag{19}$$

where

$$F_1^{(i)} = \frac{E_1 - E_{-1}u_i^{-2}}{p} + 2(-E_1 u_i + E_{-1}u_i^{-3}) \pmod{p^{m-2}},$$

$$F_2^{(i)}(v) = E_2 v^2 + p(E_3 v^3 + \cdots), \ E_2 \equiv E_{-1} \pmod{p}, \ (E_2, p) = 1.$$

By virtue of Lemma 4 the inner sum on v in equation (19) estimates as $p^{\frac{m-2}{2}}$. Hence, $|\sigma_{k,\ell}| \le 2p^{\frac{m}{2}}$.

Corollary. *The least period of the sequence $\Psi_k(\omega)$ cannot be an odd integer.*

Lemma 7. *Let k, ℓ be non-negative integers of identical parity, $h \in \mathbb{Z}$, $\nu_p(h, p^m) = \delta$, $\nu_p(k-b) = \kappa$ and let $bc \equiv 0 \,(mod\ p^m)$, $1 \le \nu_p(b) \le \nu_p(c) < m$. Then*

$$|\sigma_{k,\ell}(h)| \le \begin{cases} p^m & \text{if} \quad m - \delta - \kappa - \mu \le 0, \\ 2p^{\frac{m+\delta+\kappa+\mu}{2}} & \text{if} \quad m - \delta - \kappa - \mu > 0, \end{cases}$$

where $\nu_p(b)=\mu$.

Proof. First we suppose that $b^2\equiv 0 \pmod{p^m}$. Since b and c satisfy the condition $bc\equiv 0 \pmod{p^m}$, we have by Lemma 1 for $k=2,3,\dots$

$$\begin{aligned}\Psi_{2k}(\omega)&=\frac{ka^kb+(a^k+ka^kc)\omega}{a^k+ka^{k-1}b\omega+ka^{k-1}c\omega^2},\\ \Psi_{2k+1}(\omega)&=\frac{a^{k+1}+(k+1)a^kb+(k+1)a^kc\omega^2}{ka^kb+(a^k+ka^kc)\omega}.\end{aligned}\tag{20}$$

Hence,

$$\Psi_{2k}(\omega)-\Psi_{2\ell}(\omega)=\frac{E_0+E_1\omega+E_2\omega^2+E_3\omega^3}{F_0+F_1\omega+F_2\omega^2},\tag{21}$$

where

$$\begin{aligned}E_0&=(k-\ell)a^{k+\ell}b,\\ E_1&=(k-\ell)a^{k+\ell}c,\\ E_2&=(k-\ell)a^{k+\ell-1}b,\\ E_3&=-(k-\ell)a^{k+\ell-1}c,\\ F_0&=a^{k+\ell},\ F_1=(k+\ell)a^{k+\ell-1}b,\ F_2=(k+\ell)a^{k+\ell-1}c.\end{aligned}\tag{22}$$

Similarly, we infer

$$\Psi_{2k+1}(\omega)-\Psi_{2\ell+1}(\omega)=\frac{E'_0+E'_1\omega+E'_2\omega^2+E'_3\omega^3}{F'_0+F'_1\omega+F'_2\omega^2},\tag{23}$$

where

$$\begin{cases}E'_0=(k-\ell)a^{k+\ell-1}b,\ E'_1=-(k-\ell)a^{k+\ell-1}c,\\ E'_2=(k-\ell)a^{k+\ell}b,\ E'_3=(k-\ell)a^{k+\ell}c,\\ F'_0=0,\ F'_1=(k+\ell)a^{k+\ell}b,\ F'_2=a^{k+\ell}(1+(k+\ell)c).\end{cases}\tag{24}$$

Now, by analogy with proof of Lemma 6, we have modulo p^m

$$\begin{cases}\Psi_{2k}(\omega)-\Psi_{2\ell}(\omega)\equiv(k-\ell)(b+c\omega+a^{-1}b\omega^2-a^{-1}c\omega^3),\\ \Psi_{2k+1}(\omega)-\Psi_{2\ell+1}(\omega)\equiv\\ \equiv(k-\ell)(\omega^{-2}(1-(k+\ell)c)(a^{-1}b-a^{-1}c\omega+b\omega^2+c\omega^3)\cdot\\ \qquad\cdot(1-(k+\ell)b\omega^{-1}))\equiv\\ \equiv(k-\ell)(c\omega+b-a^{-1}c\omega^{-1}+a^{-1}b\omega^{-2}).\end{cases}\tag{25}$$

In general case $b \equiv c \equiv 0 \pmod p$, $bc \equiv 0 \pmod{p^m}$, $b^2 \not\equiv 0 \pmod{p^m}$, we have for $k = 2, 3, \ldots$

(26)
$$\Psi_{2k}(\omega) = \frac{(ka^k b + A_k a^k b^3) + (a^k + ka^k c + B_k a^{k-1} b^2)\omega}{(a^k + C_k a^{k-1} b^2) + (ka^{k-1} b + D_k a^{k-1} b^3)\omega + ka^{k-1} c\omega^2},$$

$$\Psi_{2k+1}(\omega) = \frac{(a^{k+1} + C_k a^k b^2) + ((k+1)a^k b + D_{k+1} a^{k-1} b^3)\omega + (k+1)a^k c\omega^2}{(ka^k b + A_k a^k b^3) + (a^k + ka^k c + B_k a^{k-1} b^2)\omega},$$

where

$$A_k = \frac{k(k+1)(k+2)}{12} - 1 + p^{2\mu} F_A(k), \qquad B_k = \frac{k(k+1)}{2} + p^{2\mu} F_B(k),$$

(27)
$$C_k = \frac{(k-1)k}{2} + p^{2\mu} F_C(k), \qquad D_k = \frac{k(k^2-1)}{6} + p^{2\mu} F_D(k),$$

$$F_A(k),\ F_B(k),\ F_C(k),\ F_D(k) \in \mathbb{Z}[k].$$

Thus, as in (25) we derive

$$\Psi_{2k}(\omega) - \Psi_{2\ell}(\omega) \equiv (k-\ell)[f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3 + p^{2\mu}\omega^4 G_0(\omega)] \pmod{p^m},$$

(28)
$$\Psi_{2k+1}(\omega) - \Psi_{2\ell+1}(\omega) \equiv$$

$$\equiv (k-\ell)[e_1\omega + e_0 + e_{-1}\omega^{-1} + e_{-2}\omega^{-2} + p^{2\mu}\omega^{-3} G_1(\omega^{-1})] \pmod{p^m},$$

where

$$f_0 \equiv b,\ f_1 \equiv c,\ f_2 \equiv a^{-1}b,\ f_3 \equiv -a^{-1}c \pmod{p^{2\mu}},$$
$$e_1 \equiv c,\ e_0 \equiv b,\ e_{-1} \equiv -a^{-1}c,\ e_{-2} \equiv a^{-1}b \pmod{p^{2\mu}},$$
$$G_0(\omega),\ G_1(\omega) \in \mathbb{Z}[\omega].$$

Denote $\nu_p(c) = \nu$, $m_0 = m - \mu - \delta - \kappa$, $c_0 = cp^{-\nu}$, $b_0 = bp^{-\mu}$, $h + 0 = hp^{-\delta}$. If $\mu < \nu$ then from (25) or (28), by using Lemmas 4 and 5 obtain for k, ℓ even numbers we obtain

$$|\sigma_{k,\ell}(h)| \le p^{\delta+\kappa+\mu} \left| \sum_{\omega \in R^*_{m_1}} e_{p^{m_0}} \left(h_0(c_0 p^{\nu-\mu}\omega + a^{-1}b_0\omega^2 + pG_0(\omega))\right) \right| \le$$

$$\leq \begin{cases} p^{\frac{m+\delta+\kappa+\mu}{2}} & \text{if } \delta+\kappa+\mu < m, \\ p^m & \text{if } \delta+\kappa+\mu \geq m, \end{cases} \tag{29}$$

and if k, ℓ are odd numbers, then

$$|\sigma_{k,\ell}(h)| \leq$$

$$\leq p^{\delta+\kappa+\mu} \left| \sum_{\omega \in R^*_{m_0}} e_{p^{m_0}} \left(h_0(c_0 p^{\nu-\mu}\omega - a^{-1}c_0 p^{\nu-\mu} + a^{-1}b_0\omega^{-2} + pG(\omega^{-1}))\right)\right| \leq$$

$$\leq \begin{cases} 2p^{\frac{m+\delta+\kappa+\mu}{2}} & \text{if } \delta+\kappa+\mu < m, \\ p^m & \text{if } \delta+\kappa+\mu \geq m. \end{cases} \tag{30}$$

Applying Lemmas 4 and 5 we obtain the assertion of lemma.

Remark. The estimate of $|\sigma_{k,\ell}|$ remains correct in a general case $b \equiv c \equiv \equiv 0 \pmod p$, $b \not\equiv 0 \pmod{p^m}$. In this case the representations for $\Psi_k(\omega)$ become cumbersome.

Lemma 8. *Let $b \equiv c \equiv 0 \,(mod\ p)$, $bc \equiv 0 \,(mod\ p^m)$ and let τ be a least period length of the sequence $\Psi_k(\omega)$, $k = 0, 1, 2, \ldots$, modulo p^m. Then $\tau = 2p^{m-\mu_0}$, where $\mu_0 = \min(\mu, \nu)$, if $ab + ac\omega + b\omega^2 - c\omega^3 \not\equiv 0 \,(mod\ p^{\mu_0+1})$.*

Proof. If $ab + ac\omega + b\omega^2 - c\omega^3 \equiv 0 \pmod{p^{\mu_0+1}}$ then the sequence $\{\psi_k(\omega)\}$ has the maximal period length among all inversive congruential pseudorandom generators (3) with modulus p^m. Moreover, $\tau = 2p^{m-\mu_0}$, where $\mu_0 = \min(\mu, \nu)$.

This assertion follows from (22)-(28) and the condition

$$\omega_{2k} - \omega_{2\ell} \equiv 0 \pmod{p^n}.$$

Here we take into account that

$$B_k - B_\ell,\ D_kB_\ell - D_\ell B_k,\ A_k - A_\ell,\ A_kC_\ell - A_\ell C_k,\ \ell C_k - kC_\ell,\ C_k - C_\ell$$

divide on $k - \ell$. Since a least period length τ is even integer, we have $\tau = 2p^{m-\mu_0}$, where $\mu_0 = \min(\nu_p(b), \nu_p(c))$.

3. The estimates for exponential sums

Let h, N be integers, $(h, p^m) = p^\delta$, $0 \le \delta < m$, and let τ be a least period length of the sequence $\Psi_k(\omega)$, $k = 0, 1, 2, \ldots$ (see (3)). We denote

$$S_N(h,\omega) := \sum_{k=0}^{N-1} e_{p^m}(h\Psi_k(\omega)) \quad (\omega \in R_m^*). \tag{31}$$

We shall construct the estimates for $S_N(h,\omega)$. From (4), after short computations, we obtain

$$\begin{cases} \Psi_{2k}(\omega) = \omega + (b(1-a^{-1}\omega) + c\omega + b^2 g_1(\omega))k + \\ \qquad + (a^{-2}\omega^2 b^2 + b^4 g_2(\omega)k^2 + b^3(g_3\omega)k^3 + \cdots) \pmod{p^m}, \\ \Psi_{2k+1}(\omega) = (a\omega^{-1} + b + c\omega + b^3 f_0(\omega, \omega^{-1})) + \\ \qquad + \left[\omega^{-2}((\omega - a)b - a\omega c + b^2 f_1(\omega))\right] k + \\ \qquad + (a^{-2}\omega^2 b^2 + b^3 f_2(\omega))k^2 + b^3(f_3(\omega)k^3 + \cdots) \pmod{p^m}, \end{cases} \tag{32}$$

where $g_i(\omega)$, $f_0(\omega, \omega^{-1})$, $f_j(\omega)$ are polynomials over $\mathbb{Z}$. $\Psi_{2k}(\omega)$ and $\Psi_{2k+1}(\omega)$, as polynomials on k, have the coefficients at k^2 dividing on $p^{2\mu}$ exactly, where $\mu = \nu_p(b)$.

Theorem 1. *Let $N = \tau$, $\alpha = \nu_p((a-\omega)b + ac)$, $(a,p) = 1$, $b \equiv c \equiv 0 \,(mod\ p^m)$. Then the following estimate*

$$|S_\tau(h,\omega)| := \left|\sum_{k=0}^{\tau-1} e_{p^m}\left(h\Psi_k(\omega)\right)\right| \le \begin{cases} 0 & \text{if } \alpha < 2\mu,\ m - \delta - \mu > \alpha, \\ 2p^{m-\mu} & \text{if } m - \mu - \alpha \le 0 \\ & \text{or } m - \delta - \mu > 0 \\ & \text{and } \alpha \ge 2\mu,\ m - \delta - 2\mu \le 0, \\ 2p^{\frac{m+\delta}{2}} & \text{if } \alpha \ge 2\mu,\ m - \delta - 2\mu > 0 \end{cases} \tag{33}$$

holds.

Proof. First let $2\mu \ge m$. Then from (32) we have

$$\Psi_{2k}(\omega) = A_0(\omega) + A_1(\omega)k,$$
$$\Psi_{2k+1}(\omega) = B_0(\omega) + B_1(\omega)k,$$

where

$$A_0(\omega) = \omega,$$

$$A_1(\omega)=b(1-a^{-1}\omega)+c\omega=p^{\mu}[b_0(1-a^{-1}\omega)+cp^{-\mu}\omega]=p^{\mu}A_1^{(0)}(\omega),$$

$$B_0(\omega)=a\omega^{-1}+b+c\omega, B_1(\omega)=\omega^{-2}((\omega-a)b-a\omega c)=p^{\mu}B_1^{(0)}(\omega).$$

Since $\tau=2p^{m-\mu}$, we obtain

$$|S_\tau(h,\omega)|\le\left|\sum_{k=0}^{p^{m-\mu}-1}e^{2\pi i\frac{A_0(\omega)h}{p^m}}e^{2\pi i\frac{A_1^{(0)}(\omega)h}{p^{m-\mu}}k}\right|+\left|\sum_{k=0}^{p^{m-\mu}-1}e^{2\pi i\frac{B_0(\omega)h}{p^m}}e^{2\pi i\frac{B_1^{(0)}(\omega)h}{p^{m-\mu}}k}\right|=$$

$$(34)\qquad=\begin{cases}2p^{m-\mu} & \text{if } \delta\ge m-\mu,\\ 0 & \text{if } \delta<m-\mu,\ \nu_p((\omega-a)b_0-a\omega cp^{-\mu})<m-\mu-\delta,\\ 2p^{m-\mu} & \text{if } \delta<m-\mu,\ \nu_p((\omega-a)b_0-a\omega cp^{-\mu})\ge m-\mu-\delta.\end{cases}$$

Now let $2\mu<m$. The relation (32) gives

$$(35)\qquad\begin{aligned}\Psi_{2k}(\omega)&=\widetilde{A}_0(\omega)+p^{\mu}\widetilde{A}_1(\omega)k+p^{2\mu}\widetilde{A}_2(\omega)k^2+p^{3\mu}F_0(k),\\ \Psi_{2k+1}(\omega)&=\widetilde{B}_0(\omega)+p^{\mu}\widetilde{B}_1(\omega)k+p^{2\mu}\widetilde{B}_2(\omega)k^2+p^{3\mu}F_1(k),\end{aligned}$$

where

$$\begin{aligned}\widetilde{A}_1(\omega)&\equiv b_0(1-a^{-1}\omega)+cp^{-\mu}\omega \pmod{p^{\mu}},\\ \widetilde{B}_1(\omega)&\equiv\omega^{-2}((\omega-a)b_0-acp^{-\mu}\omega) \pmod{p^{\mu}},\\ \widetilde{A}_2&\equiv\widetilde{B}_2\equiv a^{-2}\omega^2b_0^2p^{\mu} \pmod{p^{2\mu}},\\ F_0(k),\ F_1(k)&\in\mathbb{Z}[k].\end{aligned}$$

So that we have

$$(36)\qquad\begin{aligned}|S_\tau(h,\omega)|\le&p^{\delta}\left|\sum_{k=0}^{p^{m_1}-1}e_{p^{m_1}}\left(\left(\widetilde{A}_1(\omega)k+\widetilde{A}_2(\omega)k^2+p^{2\mu}F_0(k)\right)h_0\right)\right|+\\ &+p^{\delta}\left|\sum_{k=0}^{p^{m_1}-1}e_{p^{m_1}}\left(\left(\widetilde{B}_1(\omega)k+\widetilde{B}_2(\omega)k^2+p^{2\mu}F_1(k)\right)h_0\right)\right|,\end{aligned}$$

where $m_1=m-\mu-\delta$.

The last sums in (36) we can estimate by Lemma 4. Consequently,

(37)
$$|S_\tau(h,\omega)| \le \begin{cases} 2p^{m-\mu} & \text{if } \alpha \ge 2\mu,\ m-\delta-2\mu \le 0 \text{ or } \alpha < 2\mu,\ \alpha \ge m-\mu-\delta, \\ 0 & \text{if } \alpha < 2\mu,\ \alpha < m-\mu-\delta, \\ 2p^{\frac{m+\delta}{2}} & \text{if } \alpha \ge 2\mu,\ m-\delta-2\mu > 0, \end{cases}$$

where $\alpha = \nu_p((a-\omega)b+ac)$.

Moreover, it is obvious that for $m-\mu-\delta \le 0$ we have $|S_\tau(h,\omega)| = 2p^{m-\mu}$. This completes the proof Theorem 1.

Theorem 2. *Let a, b, c, α and μ be those in Theorem 1. Then for N, $1 \le N < \tau$, we have*

(38)
$$|S_N(h,\omega)| \le \begin{cases} N & \text{always,} \\ 2p^{\frac{m+\delta+\mu}{2}}\left(\frac{N}{\tau}+\frac{\log\tau}{p^\delta}\right) & \text{if } m-\delta-2\mu > 0. \end{cases}$$

Proof. We shall estimate $S_N(h,\omega)$ using an estimate of uncomplete sums through an estimate of complete sum. We have

$$|S_N(h,\omega)| = \left|\sum_{\ell=0}^{N-1}\frac{1}{\tau}\sum_{k=0}^{\tau-1}\sum_{x=0}^{\tau-1} e_{p^m}(h\Psi_k(\omega))\cdot e_\tau(x(k-\ell))\right| \le$$

(39)
$$\le \frac{N}{\tau}\left|\sum_{k=0}^{\tau-1} e_{p^m}(h\Psi_k(\omega))\right| + \sum_{x=1}^{\tau-1}\frac{1}{\min(x,\tau-x)}\left|\sum_{k=0}^{\tau-1} e^{2\pi i(\frac{h\Psi_k(\omega)}{p^m}+\frac{kx}{\tau})}\right| \le$$

$$\le \frac{N}{\tau}|S_\tau(h,\omega)| + \sum_{x=1}^{\tau-1}\frac{1}{\min(x,\tau-x)}\left|\sum_{j=0}^{1}\sum_{k=0}^{\tau-1} e^{2\pi i\frac{\Phi_j(k)}{p^{m-\mu}}}\right|,$$

where

(40)
$$\begin{aligned} &\Phi_j(k) = A_1^{(j)}k + A_2^{(j)}k^2 + A_3^{(j)}k^3 + \cdots,\ \ j = 0,1; \\ &A_1^{(0)} \equiv h(b_0(1-a^{-1}\omega)+cp^{-\mu}\omega) - \kappa \pmod{p^{\mu+\delta}}, \\ &A_1^{(1)} \equiv h\omega^{-2}(b_0(\omega-a)-ac\omega p^{-\mu}) - \kappa \pmod{p^{\mu+\delta}}, \\ &A_2^{(j)} \equiv -a^{-2}b_0^2p^{\mu+\delta},\ \ A_i^{(j)} \equiv 0 \pmod{p^{2\mu+\delta}},\ i = 3,4,\dots\ . \end{aligned}$$

From (40) and Lemma 4 we conclude that the sums

$$\sum_{k=0}^{\tau-1} e^{2\pi i \frac{\Phi_j(k)}{p^{m-\mu}}} \qquad (j=0,1)$$

allow nontrivial estimate only in the case

$$h\omega^{-2}(b_0(\omega-a)-ac\omega p^{-\mu}) \equiv \kappa \pmod{p^{2\mu+\delta}}. \tag{41}$$

It is possible only if

$$\kappa \equiv 0 \pmod{p^{\delta}}. \tag{42}$$

Therefore, from (39)-(41), Lemma 5 and Theorem 1 we derive for $m \le \delta+\mu$

$$|S_N(h,\omega)| = N, \tag{43}$$

and for $m > \delta+\mu$

$$|S_N(h,\omega)| \le \frac{N}{\tau}|S_\tau(h,\omega) + 4\sum_{x=1}^{\frac{N}{2}} \frac{1}{xp^{\delta}} p^{\frac{m+\delta+\mu}{2}}|. \tag{44}$$

The proof of Theorem 2 is complete.

Theorem 3. *For almost all $\omega \in R_m^*$ and every N, $1 \le N \le \tau$, we have*

$$S_N(h,\omega) \le 3Np^{-\frac{m-\delta-\mu}{4}}.$$

Proof. Consider the sum

$$\overline{S}_N = \frac{1}{\phi(p^m)} \sum_{\omega \in R_m^*} S_N(h,\omega). \tag{45}$$

By the Cauchy-Schwarz inequality we obtain

(46)

$$|\overline{S}_N|^2 \le \frac{1}{\phi(p^m)} \sum_{\omega\in R_m^*} |S_N(h,\omega)|^2 = \frac{1}{\phi(p^m)} \sum_{k,\ell=0}^{N-1} \sum_{\omega\in R_m^*} e^{2\pi i \frac{h(\Psi_k(\omega)-\Psi_\ell(\omega))}{p^m}} \le$$

$$\le \frac{1}{\phi(p^m)} \sum_{t=0}^{m} \sum_{\substack{k,\ell=0 \\ k\equiv \ell \pmod{p^t} \\ k,\ell\le N}}^{N-1} |\sigma_{k,\ell}(h)|.$$

Hence, by Lemma 6 we have
(47)

$$|\overline{S}_N|^2 \le \frac{1}{\phi(p^m)} \left(\sum_{\kappa=0}^{m_2-1} p^{\frac{m+\delta+\mu+\kappa}{2}} \sum_{\substack{k,\ell \le N \\ k \equiv \ell \pmod{p^\kappa}}} 1 + \sum_{\kappa=m_2}^{m} p^m \sum_{\substack{k,\ell \\ k \equiv \ell \pmod{p^\kappa}}} 1 \right) \le$$

$$\le \frac{N^2}{\phi(p^m)} \left(\sum_{\kappa \le m_2-1} p^{\frac{m+\delta+\mu-\kappa}{2}} + \sum_{\kappa=m_2}^{m} p^{m-\kappa} \right) \le 4\frac{N^2}{p^m} \left(p^{\frac{m+\delta+\mu}{2}} + p^{\delta+\mu} \right).$$

From this we obtain for any $N \le \tau$

$$|\overline{S}_N| \le 2N \left(p^{-\frac{m-\delta-\mu}{4}} + p^{-\frac{m-\delta-\mu}{2}} \right) \le 3Np^{-\frac{m-\delta-\mu}{4}}. \tag{48}$$

This implies immediately Theorem 3.

4. The discrepancy bound

In this section we study the pseudorandom numbers x_n, which are obtained by the normalization

$$x_n = \frac{\omega_n}{p^n}, \quad n = 0, 1, \ldots,$$

where a sequence ω_n of integers in R_m^* is generated by the nonlinear recursion

$$\omega_{n+1} = a\omega_n^{-1} + b + c\omega_0, \ \omega_0 = \omega \in R_m^*, \quad n = 0, 1, 2, \ldots,$$

$$(a, p) = 1, \ b \equiv c \equiv 0 \pmod{p}, \ bc \equiv 0 \pmod{p^m}.$$

For a sequence of N points ($1 \le N \le \tau$),

$$x_0, x_1, \ldots, x_{N-1}$$

we denote by $D_N(\omega)$ its discrepancy which is defined by

$$D_N(\omega) = \sup_{\Delta \subset I} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

where $A_N(\Delta)$ is the number of elements of $x_0, x_1, \ldots, x_{N-1}$, which hit the interval Δ, $|\Delta|$ is the length of Δ, and the supremum is extended over subintervals $\Delta \subset I$, $I = [0, 1)$. The discrepancy can be considered as

a characterization of uniform distribution of the pseudorandomness of the sequence $\omega_0, \omega_1, \dots, \omega_{N-1}$. We shall say that $D_N(\omega)$ is the discrepancy of inversive congruential pseudorandom numbers with modulus p^m.

Theorem 4. *Let $p \geq 3$ be a prime number and $m \geq 2$ an integer, and let $a, b, c \in \mathbb{Z}$, $(a, p) = 1$, $b \equiv c \equiv 0 \,(mod\ p)$, $bc \equiv 0 \,(mod\ p^m)$, $1 \leq \nu_p(b) \leq \nu_p(c) < m$. The following estimate*

$$D_N(\omega) \leq \frac{18}{\pi} p^{\frac{m}{2}} N^{-1} \log p^m + 5p^{-(m-2\mu)} \log p^m \tag{49}$$

holds for any $\omega \in R_m^*$ and $m > 2\mu$.

Proof. For any integer $H > 1$ the Erdős-Turán inequality ([18], p.214) gives

$$D_N(\omega) \leq \frac{1}{H+1} + \frac{2}{N} \sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1} \right) |S_N(h, \omega)| \quad \text{for} \quad \omega \in R_m^*, \tag{50}$$

where $S_N(h, \omega)$ is defined in (31).

If $m - 2\mu > 0$, we obtain, by Theorem 2, for $H \leq \tau$

$$\sum_{h=1}^{H} \frac{1}{h} |S_N(h, \omega)| \leq$$

$$\leq \sum_{\delta=0}^{m-2\mu-1} 2p^{\frac{m+\delta}{2}} \left(\frac{N}{\tau} + \frac{\log \tau}{p^\delta} \right) \sum_{\substack{h=1 \\ (h, p^m) = p^\delta}}^{H} \frac{1}{h} + N \sum_{\delta=m-2\mu}^{m-1} \sum_{\substack{h=1 \\ p^\delta \,||\, h}}^{H} \frac{1}{h} \leq$$

$$\leq 2p^{\frac{m}{2}} \left(1 - \frac{1}{\sqrt{3}} \right)^{-1} \left(\frac{N}{\tau} + \log \tau \right) \log H + 2Np^{-m+2\mu} \log H \leq \tag{51}$$

$$\leq 8p^{\frac{m}{2}} \log^2 \tau + 2N \frac{p^\mu}{\tau} \log \tau;$$

$$\sum_{h=1}^{H} |S_N(h, \omega)| \leq \left(8p^{\frac{m}{2}} \log \tau + 2\frac{N}{\tau} p^\mu \right) \cdot H. \tag{52}$$

We put $H = \tau$. So that we have for $m - 2\mu > 0$

$$D_N(\omega) \leq$$

$$\leq \frac{18}{\pi} p^{\frac{m}{2}} N^{-1} \log^2 \tau + 5p^{\mu} \tau^{-1} \log \tau \leq \frac{18}{\pi} p^{\frac{m}{2}} N^{-1} \log^2 p^m + 5p^{-(m-2\mu)} \log p^m.$$

For $c = 0$ this result is better than the estimate of $D_N(\omega)$ in [11].

Theorem 5. *For almost all $\omega \in R_m^*$ and every $N \leq \tau$ we have*

$$D_N(\omega) \leq 19 N^{-\frac{1}{4}} \log \tau. \tag{53}$$

Proof. In (50) set $H = p^{\frac{m-\mu}{4}}$ and apply Theorem 3. Then we easily infer

$$D_N(\omega) \leq \frac{1}{H+1} + 6 \sum_{\delta=0}^{\frac{m-\mu}{4}} p^{-\frac{m-\mu}{4}} \sum_{h=1}^{H/p^{\delta}} \left(\frac{1}{\pi h p^{\delta}} + \frac{1}{H+1} \right) p^{\frac{\delta}{4}} \leq$$

$$\leq 19 p^{-\frac{m-\mu}{4}} \log p^{m-\mu} \leq 19 N^{-\frac{1}{4}} \log \tau.$$

References

[1] **Knuth D.E.,** *The art of computer programming II. Seminumerical algorithms,* Addison-Wesley, 1998.

[2] **Eichenauer J. and Lehn J.,** A non-linear congruential pseudorandom number generator, *Statist. Hefte,* **27** (1986), 315-326.

[3] **Niederreiter H.,** *Finite fields and their applications,* Contributions to General Algebra **7**, Vienna, 1990, Teubner, Stuttgart, 1991.

[4] **Chou W.-S.,** On inversive maximal period polynomials over finite fields, *Appl. Algebra Engrg. Comm. Comput.,* **6** (1995), 245-250.

[5] **Chou W.-S.,** The period lengths of inversive congruential recursions, *Acta Arith.,* **73** (4)(1995), 325-341.

[6] **Flahive M. and Niederreiter H.,** On inversive congruential generators for pseudorandom numbers, *Finite fields, coding theory and advances in communications and computing,* eds. G.L. Mullen and P.J.-S. Shine, Marcel Dekker, New York, 1992, 75-80.

[7] **Eichenauer J., Lehn J. and Topuzoğlu A.,** A nonlinear congruential pseudorandom number generator with power of two modulus, *Math. Comp.,* **51** (1988), 757-759.

[8] **Eichenauer-Herrmann J.,** Construction of inversive congruential pseudoramdom number generators with maximal period length, *J. Comput. Appl. Math.,* **40** (1992), 345-349.

[9] **Eichenauer-Herrmann J. and Topuzoğlu A.,** On the period of congruential pseudorandom number sequences generated by inversions, ibid. **31** (1990), 87-96.

[10] **Huber K.,** On the period length of generalized inversive pseudorandom generators, *Appl. Algebra Engrg. Comm. Comput.,* **5** (1994), 255-260.

[11] **Niederreiter H. and Shparlinski I.,** Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus, *Acta Arith.,* **90** (1) (2000), 89-98.

[12] **Eichenauer-Herrmann J., Herrmann E. and Wegenkittl S.,** A survey of quadratic and inversive congruential pseudorandom numbers, *Monte Carlo and quasi-Monte Carlo methods, 1996,* eds. H. Niederreiter et al., Lecture Notes in Statist. **127**, Springer Verlag, New York, 1998, 66-97.

[13] **Niederreiter H.,** *Random number generation and quasi-Monte Carlo methods,* SIAM, Philadelphia, 1992.

[14] **Niederreiter H.,** New developments in uniform pseudorandom number and vector generation, *Monte Carlo and quasi-Monte Carlo methods in scientific computing,* eds. H. Niederreiter and P.J.-S. Shine, Lecture Notes in Statist. **106**, Springer Verlag, New York, 1995, 87-120.

[15] **Kato T., Wu L.-M. and Yanagihara N.,** On a nonlinear congruential pseudorandom number generator, *Math. Comput.,* **65 (213)** (1996), 227-233.

[16] **Niederreiter H.,** Remarks on nonlinear congruential pseudorandom numbers, *Metrika,* **35** (1988), 321-328.

[17] **Eichenauer-Herrmann J. and and Grothe H.,** A new inversive congruential pseudorandom number generator with power of two modulus, *ACM Transactions of Modeling and Computer Simulation,* **2** (1)(1992), 1-11.

[18] **Vaaler J.D.,** Some extremal functions in Fourier analysis, *Bull. Amer. Math. Soc. (N.S.),* **12** (1985), 183-216.

S.P. Varbanets
Department of Computer Algebra and Discrete Mathematics
Odessa National University
Dvoryanskaya str. 2
65026 Odessa, Ukraine
varb@sana.od.ua