Annales Univ. Sci. Budapest., Sect. Comp. 32 (2010) 151-176

ON INVERSIVE CONGRUENTIAL GENERATOR WITH A VARIABLE SHIFT FOR PSEUDORANDOM NUMBERS WITH PRIME POWER MODULUS

P. Varbanets and S. Varbanets

(Odessa, Ukraine)

Abstract. The inversive congruential method for generating uniform pseudorandom numbers is a particularly attractive alternative to linear congruential generators which have many undesirable regularities. In the present paper, a new inversive congruential generator with a variable shift and prime-power modulus is introduced. Exponential sums on inversive congruential pseudorandom numbers are estimated.

1. Introduction

Nonlinear methods of generating uniform pseudorandom numbers in the interval $[0, 1)$ have been introduced and studied during the last twenty years. The development of this attractive field of research is described in the survey articles ([2, 8, 11, 21, 22, 27, 28, 30, 31, 32]) and in Niederreiter's monograph [29]. A particularly promising approach is the inversive congruential method. The generated sequences of pseudorandom numbers have nice equidistribution and statistical independence (unpredictability) properties ([3, 4, 6, 24, 25]). Four types of inversive congruential generators can be distinguished, depending on whether the modulus is a prime ([1, 11, 27]), an odd prime power ([33, 37, 38]), a power of two ([10, 12, 15]) or a product of distinct prime numbers ([5, 7, 9, 10, 17, 19, 20]).

Mathematics Subject Classification: Primary 11L07; Secondary 45B67, 11T23, 11T71, 11K45.

In the works of Chou ([1]), Eichenauer and Lehn ([11]), Eichenauer and Topuzoğlu ([14]), Niederreiter ([26]) have been studied the problem of when the sequence of pseudorandom numbers (generated by the pseudorandom generator) has the maximal period. Niederreiter and Shparlinski ([33]) considered the special exponential sums on inversive congruential pseudorandom numbers with prime power modulus and obtained nontrivial results concerning the distribution of these numbers in part of the period. For surveys of results and applications of inversive congruential numbers see [17], [29], [35].

In the case of an odd prime-power modulus the inversive congruential generator is defined in the following way:

Let p be a prime, $p \geq 3$, m be a natural number, $m \geq 2$. For given $a, b \in \mathbb{Z}$, $(a,p) = 1$, $b \equiv 0 \pmod p$, we take an initial value $\omega_0 = \omega \in \mathbb{Z}$, $(\omega, p) = 1$, and then the recurrence relation

$$\omega_{n+1} \equiv a\omega_n^{-1} + b \pmod{p^m} \tag{1.1}$$

generates a sequence $\omega_0, \omega_1, \ldots$, which we call the inversive congruential sequence modulo p^m.

It is clear that the numbers $\frac{\omega_0}{p^m}, \frac{\omega_1}{p^m}, \ldots$ belong to the interval $[0,1)$ and form a sequence of inversive congruential pseudorandom numbers with modulus p^m.

Such method of pseudorandom number generation was introduced in [14]. In practice, one works with a large power p^m of a small prime p. Surveys of results of inversive congruential pseudorandom numbers see in [13], [18], [20], [27], [29].

For the investigation of equidistribution and statistical independence of the sequence $\left\{\frac{\omega_k}{p^m}\right\}$, $k \geq 0$, we shall apply upper and lower bounds for the exponential sums

$$S^{(d)}(h_1, \ldots, h_d) = \sum_{k=0}^{N-1} e_{p^m}(h_1\omega_k + \cdots + h_d\omega_{k+d-1}) \ \ (d = 1, 2, \ldots), \tag{1.2}$$

where $N \leq \tau$, τ is a least period length of the sequence $\omega_0, \omega_1, \ldots$ considered modulo p^m, $(h_1, \ldots, h_d) \in \mathbb{Z}^d$, $(h_1, \ldots, h_d) \neq 0 \in \mathbb{Z}^d$. The sums $S^d(h_1, \ldots, h_d)$ are considered in [21, 25, 33, 36, 37, 38].

The present paper deals with some generalization of the inversive congruential sequence from (1.1) in such sense that we substitute a fixed shift b in (1.1) by a variable shift $b_{k+1} = b + (k+1)c\omega$.

The organization of our paper is as follows. In the second and third sections the auxiliary results are stated and the behavior of inversive congruential sequences is discussed. Here also we construct two representations of ω_k: as the polynomial on k and as the polynomial on ω, and obtain condition for maximal value of a least period length of the generated sequence ω_k. The main results of the present paper are established in the fourth and fifth sections, in which upper bounds are obtained for the exponential sums of type (1.2) and upper and lower bounds found for the discrepancy of the sequence of the points $\frac{\omega_k}{p^m} \in [0,1)$ and the points $\left(\frac{\omega_k}{p^m}, \frac{\omega_{k+1}}{p^m}\right) \in [0,1)^2$ accordingly.

Notations. The letter p denotes a prime number, $p \geq 3$. For $m \in \mathbb{N}$ the notation R_m (accordingly, R_m^*) denotes the complete(accordingly, reduced) system of residues modulo p^m. We write $\gcd(a,b) = (a,b)$ to note the greatest common divisor of a and b. For $z \in \mathbb{Z}$, $(z,p) = 1$ let z^{-1} be the multiplicative inverse of a modulo p^m. We write $\nu_p(A) = \alpha$ if $p^\alpha | A$, $p^{\alpha+1} \not| A$. For real t and natural q, the abbreviation $e_q(t) = e^{2\pi i \frac{t}{q}}$ is used and $\mathfrak{u} \cdot \mathfrak{v}$ stands for the standard inner product $\mathfrak{u}, \mathfrak{v} \in \mathbb{R}^d$.

2. Auxiliary results

We need the following three simple statements.

Lemma 1. *Let $q > 1$ be a natural number, $a \in \mathbb{Z}$. Then*

$$\sum_{x=0}^{q-1} e^{2\pi i \frac{ax}{q}} = \begin{cases} q & \text{if} \quad q|a, \\ 0 & \text{if} \quad q \not| a. \end{cases}$$

Lemma 2. *Let $p > 3$ be a prime, $m \in \mathbb{N}$, $m \geq 2$ and let $f(x) = A_1 x + A_2 x^2 + p(A_3 x^3 + \cdots)$ be a polynomial over $\mathbb{Z}$, moreover, $(A_1, A_2, p) = 1$. Then*

$$\left| \sum_{x \in R_m} e^{2\pi i \frac{f(x)}{p^m}} \right| = \begin{cases} 0 & \text{if} \quad (A_1,p) = 1, \ p|A_2, \\ p^{\frac{m}{2}} & \text{if} \quad (A_2,p) = 1. \end{cases}$$

These lemmas are well-known.

Lemma 3. *Let $f(x) = A_1x + A_2x^2 + p(A_3x^3 + \cdots)$ and $g(x) = B_1x + +p(B_2x^2 + \cdots)$ be polynomials over $\mathbb{Z}$, and let $\nu_p(A_2) = \nu > 0$, $\nu_p(A_j) \geq \nu$, $j = 3, 4, \ldots$; $(B_1, p) = 1$. Then for $\nu \leq m$, $m \geq 2$, the following estimates*

$$\left|\sum_{x\in R_m} e^{2\pi i\frac{f(x)}{p^m}}\right| = \begin{cases} p^{\frac{m+\nu}{2}} & \text{if } \nu_p(A_1) \geq \nu, \\ 0 & \text{else,} \end{cases} \tag{2.1}$$

$$\left|\sum_{x\in R_m^*} e^{2\pi i\frac{f(x)+g(x^{-1})}{p^m}}\right| \leq 4p^{\frac{m}{2}} \tag{2.2}$$

hold.

Proof. The relation (2.1) is a corollary of Lemma 2. In order to prove (2.2) we put $x = y + p^{m-1}z$, $y = 1, \ldots, p^{m-1}$, $(y, p) = 1$, $z = 0, 1, \ldots, p-1$. Bearing in mind that

$$\begin{aligned} x^j &\equiv y^j + jp^{m-1}y^{j-1}z \pmod{p^m}, \\ x^{-j} &\equiv y^{-j} - jp^{m-1}y^{-j-1}z \pmod{p^m}, \quad j = 1, 2, 3, \ldots \end{aligned}$$

we get

$$f(x) + g(x^{-1}) \equiv f(y) + f'(y)p^{m-1}z + g(y^{-1}) - B_1p^{m-1}y^{-2}z \pmod{p^m}.$$

Hence, applying Lemma 1 we obtain

$$\left|\sum_{x\in R_m^*} e^{2\pi i\frac{f(x)+g(x^{-1})}{p^m}}\right| = p\left|\sum_{y\in R_{m-1}^*} e^{2\pi i\frac{f(y)+g(y^{-1})}{p^m}}\right| \leq$$

$$\begin{cases} p\left\{\left|\sum\limits_{y\in R_{m-2}^*} e^{2\pi i\frac{f_1(y)+g_1(y^{-1})}{p^{m-2}}}\right| + \left|\sum\limits_{y\in R_{m-2}^*} e^{2\pi i\frac{f_2(y)+g_2(y^{-1})}{p^{m-2}}}\right|\right\} & \text{in the case (A),} \\ p\left|\sum\limits_{y\in R_{m-2}^*} e^{2\pi i\frac{f_3(y)+g_3(y^{-1})}{p^{m-2}}}\right| & \text{in the case (B),} \\ 0 & \text{in the case (C),} \end{cases}$$

where

(A) the congruence $A_1 - B_1y^{-2} \equiv 0 \pmod{p}$ has two solutions,
(B) the congruence $A_1 - B_1y^{-2} \equiv 0 \pmod{p}$ has one solution,
(C) the congruence $A_1 - B_1y^{-2} \equiv 0 \pmod{p}$ has no solutions.

Now, by induction on m and by the estimate of the Kloosterman sum we obtain the assertion (2.2).

3. Preparations

Let us consider the transformation Ψ_k defined on R_m^*:

$$\Psi_{k+1}(\omega) = \frac{a}{\Psi_k(\omega)} + b + (k+1)c \pmod{p^m},\ k = 0, 1, 2, \ldots, \tag{3.1}$$

where p is a prime number, $m \in \mathbb{N}$, $m \geq 3$; $a, b, c \in \mathbb{Z}$, $(a, p) = 1$, $b \equiv c \equiv$ $\equiv 0 \pmod{p}$, $\nu_p(b) < \nu_p(c)$, $\omega \in R_m^*$, $\Psi_0(\omega) = \omega$.

In subsequent we shall write $\Psi_k(\omega) = \omega_k$, $\omega_0 = \omega$ is the initial value. The sequence $\{\omega_k\}$ defined by (3.1) can be considered as the generalization of the inversive congruential sequence $\{u_k\}$, was studied by H. Niederreiter and I. Shparlinski in [33]:

$$u_{k+1} = \frac{a}{u_k} + b \pmod{p^m},\ u_0 \in R_m^*. \tag{3.2}$$

The parameter b is called naturally a shift of inversive congruential number generator, which does not depend on k. But in our case ω_k has a variable shift $b + (k+1)c\omega$. We shall say that $\{\omega_k\}$ defined by (3.1) is the inversive congruential sequence with variable shift. In order to show that the sequence ω_k is defined by the parameters a, b, c, ω we shall denote it as $\Omega(\omega, a, b, c; p^m)$. In this section we shall obtain two representations for $\omega_k \in \Omega(\omega, a, b, c; p^m)$:

the representation of ω_k *as a polynomial on* k *modulo* p^m, $\omega_k \equiv f_\omega(k)$,

the representation of ω_k *as a polynomial on* ω *and* ω^{-1} *modulo* p^m, $\omega_k \equiv$ $\equiv F_k(\omega, \omega^{-1})$.

Lemma 4. *Let* Ψ_k *be the transformation defined by (3.1) and let* $c^r \equiv$ $\equiv 0 \pmod{p^m}$, $r > 1$. *Then for* $k = 0, 1, 2, \ldots$

(i) the transformation is a permutation of R_m^*,

$$(ii) \qquad \Psi_k(\omega) := \omega_k \equiv \frac{A_0^{(k)} + A_1^{(k)}\omega + \cdots + A_r^{(k)}\omega^r}{B_0^{(k)} + B_1^{(k)}\omega + \cdots + B_r^{(k)}\omega^r} \pmod{p^m},$$

where for $r=2$ the following congruences $mod\ p^m$ hold:

$$\text{(3.3)}\qquad \begin{cases} \Psi_{2k}(\omega)=\frac{A_0^{(2k)}+A_1^{(2k)}\omega}{B_0^{(2k)}+B_1^{(2k)}\omega+B_2^{(2k)}\omega^2}, \\ \Psi_{2k+1}(\omega)=\frac{C_0^{(2k+1)}+C_1^{(2k+1)}\omega+C_2^{(2k+1)}\omega^2}{D_0^{(2k+1)}+D_1^{(2k+1)}\omega}, \end{cases}$$

$$\text{(3.4)}\qquad \begin{cases} A_0^{(2k)}=ka^kb+\overline{A}_0^{(2k)}b^3,\ \ A_1^{(2k)}=a^k+k\overline{A}_1^{(2k)}b^2; \\ B_0^{(2k)}=a^k+\overline{B}_0^{(2k)}b^2,\ \ B_1^{(2k)}=ka^{k-1}b+\overline{B}_1^{(2k)}b^3, \\ B_2^{(2k)}=ka^{k-1}c; \\ C_0^{(2k+1)}=a^{k+1}b+\overline{C}_0^{(2k+1)}b^2, \\ C_1^{(2k+1)}=(k+1)a^kb+\overline{C}_1^{(2k+1)}b^3, \\ C_2^{(2k+1)}=(k+1)a^kc; \\ D_0^{(2k+1)}=ka^kb+\overline{D}_0^{(2k+1)}b^3, \\ D_1^{(2k+1)}=a^k+ka^kc+\overline{D}_1^{(2k+1)}b^2. \end{cases}$$

$$\text{(3.5)}\qquad \begin{cases} A_{2\ell-1}^{(2k)}\equiv 0\pmod{c^\ell},\quad A_{2\ell}^{(2k)}\equiv 0\pmod{bc^\ell}, \\ B_{2\ell-1}^{(2k)}\equiv 0\pmod{bc^{\ell-1}},\quad B_{2\ell}^{(2k)}\equiv 0\pmod{c^\ell}, \\ A_{2\ell-1}^{(2k+1)}\equiv 0\pmod{bc^{\ell-1}},\quad A_{2\ell}^{(2k+1)}\equiv 0\pmod{c^\ell}, \\ B_\ell^{(2k+1)}=A_\ell^{(2k)},\ \ell=1,2,\dots \end{cases}$$

Proof. The assertion (i) is obvious and, hence, the sequence $\Omega(\omega_0,a,b,c;p^m)$ is purely periodic with some period $\tau\le\phi(p^m)$. Further, one can show by induction on n that $A_r^{(k)}\equiv B_r^{(k)}\equiv 0\pmod{c}$.

For the sake of clarity and simplicity, we shall assume that $r=2$. And now, taking into account that $c^2\equiv 0\pmod{p^m}$, we can obtain (ii), by using induction on k.

In order to prove the congruences (3.3)-(3.5) we consider the matrices

$$\text{(3.6)}\qquad \begin{aligned} A&=\begin{pmatrix} a+b^2 & ab \\ b & a \end{pmatrix}, \qquad A_1=\begin{pmatrix} a^{-1}b^2 & b \\ a^{-1}b & 0 \end{pmatrix}, \\ B&=\begin{pmatrix} 2bc & ac \\ c & 0 \end{pmatrix}, \qquad C=\begin{pmatrix} bc & 0 \\ c & 0 \end{pmatrix}. \end{aligned}$$

We have

$$
\begin{aligned}
&A = a(E + A_1), \quad A_1^s \equiv 0 \pmod{p^{\nu^s}},\\
&E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad s = 1, 2, \ldots; \quad \nu = \nu_p(b).
\end{aligned} \tag{3.7}
$$

Moreover,

$$
A^k \equiv a^k \left(E + kA_1 + \frac{k(k-1)}{2} A_1^2 + \cdots\right) \pmod{p^m}. \tag{3.8}
$$

Calculating $\Psi_{k+1}(\omega)$, $\Psi_{k+2}(\omega)$ from the expression for $\Psi_k(\omega)$ we obtain the relations

$$
\begin{cases}
A_0^{(k+2)} = (a + b^2) A_0^{(k)} + abB_0^{(k)}, \\
A_\ell^{(k+2)} = (a + b^2) A_\ell^{(k)} + abB_\ell^{(k)} + \\
\qquad\qquad + ac(k+2) B_{\ell-1}^{(k)} + bc(2k+3) A_{\ell-1}^{(k)}, \quad 1 \le \ell \le r,
\end{cases} \tag{3.9}
$$

$$
\begin{cases}
B_0^{(k+2)} = aB_0^{(k)} + bA_0^{(k)}, \\
B_\ell^{(k+1)} = aB_\ell^{(k)} + bA_\ell^{(k)} + c(k+1) A_{\ell-1}^{(k)}, \quad 1 \le \ell \le r.
\end{cases}
$$

Straightforward calculations show that

$$
\begin{gathered}
A_0^{(0)} = 0, \quad B_0^{(0)} = 1, \quad A_1^{(0)} = 1, \quad B_1^{(0)} = 0, \quad A_2^{(0)} = B_2^{(0)} = 0, \\
A_0^{(1)} = a, \quad B_0^{(1)} = 0, \quad A_1^{(1)} = b, \quad B_1^{(1)} = 1, \quad A_2^{(1)} = c, \quad B_2^{(1)} = 0.
\end{gathered}
$$

Let $k = 2k_1 + t$, where

$$
t = \begin{cases} 0 & \text{if } k \text{ is even}, \\ 1 & \text{if } k \text{ is odd}. \end{cases}
$$

Thus from (3.9),(3.10) and (3.6)-(3.8) we obtain for even k:

$$
\begin{pmatrix} A_0^{(k)} \\ B_0^{(k)} \end{pmatrix} \equiv A^{k_1} \begin{pmatrix} A_0^{(t)} \\ B_0^{(t)} \end{pmatrix},
$$

$$\begin{aligned}\begin{pmatrix} A_1^{(k)} \\ B_1^{(k)} \end{pmatrix} \equiv & A^{k_1} \begin{pmatrix} A_1^{(0)} \\ B_1^{(0)} \end{pmatrix} + \\ & + \left[\sum_{j=0}^{k_1-1} (k-2j) A^j B A^{k_1-j-1} - \sum_{j=0}^{k_1-1} A^j C A^{k_1-j-1} \right] \begin{pmatrix} A_0^{\ell} \\ B_0^{\ell} \end{pmatrix} \equiv \\ \equiv & \left(a^{k_1} \left(E + k_1 A_1 + \frac{k_1(k_1-1)}{2} A_1^2 + \cdots \right) \right) \begin{pmatrix} A_1^{(0)} \\ B_1^{(0)} \end{pmatrix} + \\ & + \left[2 \sum_{j=0}^{k_1-1} (k_1-j) a^{k_1-1} \left(E + jA_1 + \frac{j(j-1)}{2} A_1^2 + \cdots \right) BA' - \right. \\ & - \sum_{j=0}^{k_1-1} a^{k_1-1} \left(E + jA_1 + \frac{j(j-1)}{2} A_1^2 + \cdots \right) CA'' + \\ & \left. + a^{k_1-1} b^3 ck D_1(k) \right] \begin{pmatrix} A_0^{(0)} \\ B_0^{(0)} \end{pmatrix}, \end{aligned}$$

where

$$\begin{aligned} A' &= \left(E + (k_1 - j - 1) A_1 + \frac{(k_1-j-1)(k_1-j-2)}{2} A_1^2 + \cdots \right), \\ A'' &= \left(E + (k_1 - j - 1) A_1 + \frac{(k_1-j-1)(k_1-j-2)}{2} A_1^2 + \cdots \right). \end{aligned}$$

Analogously,

$$\begin{aligned}\begin{pmatrix} A_2^{(k)} \\ B_2^{(k)} \end{pmatrix} \equiv & A^{k_1} \begin{pmatrix} A_2^{(0)} \\ B_2^{(0)} \end{pmatrix} + \\ & + \left[2a^{k_1-1} \sum_{j=0}^{k_1-1} (k_1-j) \left(E + jA_1 + \cdots \right) BA' - \right. \\ & - a^{k_1-1} \sum_{j=0}^{k_1-1} \left(E + jA_1 + \cdots \right) CA'' + \\ & \left. + a^{k_1-1} b^3 ck D_2(k) \right] \begin{pmatrix} A_1^{(0)} \\ B_1^{(0)} \end{pmatrix}, \end{aligned}$$

where $D_1(k), D_2(k) \in \mathfrak{M}_2\left(\mathbb{Z}_{p^m}[k]\right)$.

From this for $k = 2k_1$ we at once obtain the formulas (3.3)-(3.4) in formulation of lemma. The formulas (3.5) follow from the representation $\Psi_{k+1}(\omega)$: $\Psi_{k+1}(\omega)$ through $\Psi_k(\omega)$ bearing in mind the formulas (3.3)-(3.4).

Lemma 5. *Let p be a prime, $p \geq 5$, and let $m \in \mathbb{N}$, $m \geq 3$; $a, b, c \in \mathbb{Z}$, $\gcd(a, p) = 1$, $b \equiv c \equiv 0 \pmod{p}$, $\nu = \nu_p(b)$, $\mu = \nu_p(c)$, $\nu < \mu$, and let $\{\omega_k\}$ be the sequence from (1). Then for any $y_0 \in R_n^*$ and $k = 0, 1, 2, \ldots$ we have*

$$\begin{aligned}\omega_{2k} =&(kb - 2^{-1}k(k^2-1)a^{-1}b^3 + G_0(k))+\\ &+ (1 + k(k+1)a^{-1}c + G_1(k))\omega+\\ &+ (-ka^{-1}b - (k^3c + k^2(k+1)a^{-1})bc+\\ &+ (2^{-1}3k^3 - 2k^2 + 2^{-1}k)a^{-2}b^3 + G_2(k))\omega^2+\\ &+ (k^2a^{-2}b^2 - k^2a^{-1}c + G_3(k))\omega^3 + G_4(k,\omega)\omega^4;\end{aligned}$$

$$\begin{aligned}\omega_{2k+1} =&((k+1)b - k^2a^{-1}c + k(k-1)a^{-1}b^3 + H_0(k))+\\ &+ ((2k+)c + H_1(k))\omega + (a - k^2c - 2k^2b^2 + H_{-1}(k))\omega^{-1}+\\ &+ (-kab + 2^{-1}3k^2(k+1)b^3 + 4^{-1}k^2(k^2-1)a^{-1}b^3+\\ &+ H_{-2}(k))\omega^{-2} + \omega^{-3}H_3(k, \omega^{-1}),\end{aligned}$$

where

$$G_i(k) \in \mathbb{Z}[k],\ G_i(0) = 0,\ G_i(k) \equiv 0 \pmod{p^{\min(2\nu+\mu, 4\nu)}},\ i = 0, 1, 2, 3;$$
$$H_i(k) \in \mathbb{Z}[k],\ H_i(0) = 0,\ H_i(k) \equiv 0 \pmod{p^{\min(2\nu+\mu, 4\nu)}},\ i = -2, \pm 1, 0;$$

$G_4(k, u)$, $H_3(k, u)$ are polynomials on k, u, moreover,

$$G_4(0, u) = H_3(0, u) = 0,\ G_4(k, u) \equiv H_3(k, u) \pmod{p^{\min(2\nu+\mu, 4\nu)}}.$$

Proof. An application of Lemma 4 and straightforward computations give the assertion of lemma at once.

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

$$\begin{aligned}\omega_{2k} =&\omega + k(b(1 - a^{-1}\omega^2) + 2a^{-1}b^3(a + \omega^2) + a^{-1}c\omega + C_1(\omega))+\\ &+ k^2(-a^{-1}b^2\omega + a^{-1}c\omega(1 - \omega^2) + C_2(\omega)) + k^3C_3(k, \omega),\end{aligned}$$

$$\begin{aligned}\omega_{2k+1} =&(b + c\omega + a\omega^{-1}) + k(b(1 - a\omega^{-2}) + 2c\omega + D_1(\omega, \omega^{-1}))+\\ &+ k^2(c(a^{-1} - \omega^{-1}) + D_2(\omega, \omega^{-1})) + k^3D_3(k, \omega, \omega^{-1}),\end{aligned}$$

where $C_1(\omega) \equiv C_2(\omega) \equiv C_3(k,\omega) \equiv 0 \pmod{p^{\min(\nu+\mu,3\nu)}}$, $D_1(\omega,\omega^{-1}) \equiv \equiv D_2(\omega,\omega^{-1}) \equiv D_3(k,\omega,\omega^{-1}) \equiv 0 \pmod{p^{\min(\nu+\mu,3\nu)}}$ *for every* $\omega,\omega^{-1} \in R_m^*$, $k \in \mathbb{Z}$.

Corollary 2. *Let* τ *be the period length of* $\Omega(\omega,a,b,c;p^m)$ *and* $\nu_p(b)=\nu$, $\nu_p(c)=\mu>\nu$.

(A) If $a \not\equiv \omega^2 \pmod{p}$, *then* $\tau = 2p^{m-\nu}$,

(B) If $\nu_p(a-\omega^2)=\delta<\min(3\nu,\mu)$, *then* $\tau = 2p^{m-\nu-\delta}$.

(C) In other cases: $\tau \le 2p^{m-\nu-\min(3\nu,\mu)}$.

4. Exponential sums on the inversive congruential sequence

Well-known that we can make the conclusion on a character of distribution of arbitrary sequence $\{x_n\}$, $x_n \in [0,1)$ by an estimation of the exponential sum

$$\sum_{n=0}^{N-1} e^{2\pi i m x_n} \qquad (N \to \infty), \tag{4.1}$$

where m is any non-zero integer.

For the periodic sequence x_n, $x_n \in [0,1)$ is usually studied the exponential sum over part of the period (i.e. $N<\tau$). R.G. Stoneham [36], H. Niederreiter [21] investigated the exponential sum over part of the period τ for the linear congruential sequences $\{x_n\}$, where $x_n = \frac{y_n}{m}$ and y_n are generated by the linear congruential recursion

$$x_{n+1} \equiv a x_n + b \pmod{m}, \tag{4.2}$$

where $a,b,m,x_0 \in \mathbb{Z}$, $a \ge 1$, $m>1$, $b,x_0 \ge 0$, $(a,m)=1$.

Similarly, H. Niederreiter and I. Shparlinski [33, 34] studied the sum (4.1) for the inversive congruential sequences with fixed shift.

These results permitted to make the conclusion that the congruential sequences $\left\{\frac{\omega_k}{p^m}\right\}$, $k \ge 0$, are pseudorandom sequences (see D. Knuth [16]).

The sequences of pseudorandom numbers have various applications in the numerical analysis and the cryptography. But for cryptographic purposes the requirement of statistical independence (unpredictability) of elements of the sequence is very important. The testing on unpredictability also can be realize

by the estimates of special exponential sums over the elements of the given sequence.

In this section we obtain the estimates of certain exponential sums over the inversive congruential sequence with a variable shift which was defined in (3.1).

For $h_1, h_2 \in \mathbb{Z}$ we denote

$$\sigma_{k,\ell}(h_1,h_2) := \sum_{\omega \in R_m^*} e_{p^m}(h_1\omega_k + h_2\omega_\ell). \tag{4.3}$$

Here we consider ω_k, ω_ℓ as a function at ω generated by (3.1).

Theorem 1. *Let* $(h_1, h_2, p^m) = p^s, s \le m$, $h_1 = h_1^0 p^s$, $h_2 = h_2^0 p^s$, $(h_1^0, h_2^0, p) = 1$, $(h_1 + h_2, p^m) = t \ge s$, $(h_1^0 k + h_2^0 \ell, p^{m-s}) = \kappa$. *The following estimates*

$$|\sigma_{k,\ell}(h_1,h_2)| \le \begin{cases} 0 & \text{if} \quad t \ne \kappa+\nu,\ \min(t, \kappa+\nu) < m-s-\nu, \\ 2^{\frac{m}{2}} p^{\frac{m+\nu+s+t}{2}} & \text{if} \quad t = \kappa+\nu \text{ and } m-\nu-s-t > 0, \\ \phi(p^m) & \text{if} \quad \min(t, \kappa+\nu) \ge m-s-\nu. \end{cases}$$

hold, where $\phi(m)$ *is Euler's function.*

Proof. First, let k, ℓ be non-negative integers of different parity, for example, $k := 2k$, $\ell := 2\ell + 1$. By Lemma 5 we obtain

$$\begin{aligned} h_1\omega_{2k} + h_2\omega_{2\ell+1} =& p^s \left[\left(A_0 + A_1\omega + A_2\omega^2 + A_3\omega^3 + b^3\omega^4 H(\omega)\right) + \right. \\ &\left. + \left(A_{-1}\omega^{-1} + A_{-2}\omega^{-2} + A_{-3}\omega^{-3} + b^3\omega^{-4}G(\omega^{-1})\right)\right] = \\ =& p^s F(\omega, \omega^{-1}), \end{aligned} \tag{4.5}$$

where

$$\begin{aligned} A_1 &\equiv h_1^0 \pmod{p^\nu}, \qquad A_2 \equiv -kba^{-1}h_1^0 \pmod{p^{\nu+1}}, \\ A_{-1} &\equiv ah_2^0 \pmod{p^\nu}, \quad A_{-2} \equiv h_2^0 a\ell b \pmod{p^{\nu+1}}, \\ A_3 &\equiv A_{-3} \equiv 0 \pmod{p^{\nu+1}}. \end{aligned} \tag{4.6}$$

We put $\omega = u + p^{m-1-s}z$, $u \in R_{m-s-1}^*$, $z \in R_1$. Then we have

$$\begin{aligned} \omega^{-1} &\equiv u^{-1} - p^{m-1}u^{-2}z \pmod{p^m}, \\ \omega^j &\equiv u^j + jp^{m-1}u^{j-1}z \pmod{p^m}, \\ \omega^{-j} &\equiv u^{-j} - jp^{m-1}u^{-j-1}z \pmod{p^m}. \end{aligned}$$

Therefore we can write

$$p^{-s}\left(h_1\omega_{2k}+h_2\omega_{2\ell+1}\right)\equiv \tag{4.7}$$

$$\equiv \left(F\left(u,u^{-1}\right)+\left(h_1^0-h_2^0au^{-2}\right)p^{m-s-1}z\right)\pmod{p^{m-s}}.$$

Hence, from (4.3), (4.7) and Lemma 1 we get

$$|\sigma_{k,\ell}(h_1,h_2)|=p^{s+1}\left|\sum_{\substack{u\in R^*_{m-s-1}\\ h_1^0u^2\equiv h_2^0a\pmod p}} e_{p^{m-s}}\left(F\left(u,u^{-1}\right)\right)\right|\le \tag{4.8}$$

$$\le 2p^{s+1}\left|\sum_{e\in R^*_{m-s-2}} e_{p^{m-s-2}}\left(F_1\left(u,u^{-1}\right)\right)\right|,$$

where $F_1(u,u^{-1})$ is a polynomial of the same type as $F(u,u^{-1})$.

Continuing we obtain the assertion of the Lemma 3 for $k\not\equiv\ell\pmod 2$.

Now, let k and ℓ be integers of identical parity. Then for $k:=2k$, $\ell:=2\ell$, we have modulo p^{m-s}

$$p^{-s}(h_1\omega_{2k}+h_2\omega_{2\ell})\equiv B_0+B_1\omega+B_2\omega^2+B_3\omega^3+\omega^4B_4(\omega):=F(\omega), \tag{4.9}$$

where

$$B_1=h_1^0+h_2^0+pB_1',$$
$$B_2=a^{-1}b(h_1^0k+h_2^0\ell)+p^{2\nu}B_2',$$
$$B_3=(a^{-2}b^2-a^{-1}c)(h_1^0k^2+h_2^0\ell^2)+p^{3\nu}B_3',$$
$$B_4=(\omega)=p^{2\nu+\mu}B_4'(\omega),$$

moreover the coefficients of $B_4'(\omega)$ (as a polynomial on ω) contain multipliers of type $h_1k^j+h_2\ell^j$, $i\ge 0$, and B_1', B_2', B_3' consist out of the summand of type $c\cdot\left(h_1k^j+h_2\ell^j\right)$, $c\in\mathbb{Z}$.

It will be observed that $h_1^0k^j+h_2^0\ell^j\equiv 0\pmod{p^t}$, $j=2,3,\dots,$ if $\nu_p(h_1^0+$ $+h_2^0)=\nu_p(h_1^0k+h_2^0\ell)=t$. (Indeed, we have

$$h_1^0k^j+h_2^0\ell^j=(h_1^0k^{j-1}+h_2^0\ell^{j-1})(k+\ell)-k\ell(h_1k^{j-2}+h_2^0\ell^{j-2}),$$

and then we apply an induction over j).

Now, as above we infer

$$p^{-s}\left(h_1\omega_{2k}+h_2\omega_{2\ell}\right)\equiv F(u)+p^{m-s-1}z(B_1+2B_2u)\pmod{p^{m-s}}.$$

Hence, by Lemma 1 and Lemma 3 we obtain easily

$$|\sigma_{2k,2\ell}(h_1,h_2)| \le \begin{cases} 0 & \text{if } t \ne \kappa+\nu,\ \min(t,\kappa+\nu) < m-s-\nu, \\ 2p^{\frac{m+\nu+s+t}{2}} & \text{if } t=\kappa+\nu \text{ and } m-\nu-s-t>0, \\ \phi(p^m) & \text{if } \min(t,\kappa+\nu) \ge m-s-\nu. \end{cases}$$

For $k \equiv \ell \equiv 1 \pmod 2$ we have the analogous estimates.

Let h be integer, $(h,p^m)=p^s$, $0 \le s < n$, and let τ be a least period length of the sequence $\{\omega_k\}$, $k=0,1,2,\ldots$, defined in (3.1). For $1 \le N \le \tau$ we denote

$$S_N(h,\omega) = \sum_{k=0}^{N-1} e_{p^m}(h\omega_k). \tag{4.10}$$

We shall obtain the bound for $S_N(h,\omega)$. By Corollary from Theorem 7 we can write

$$\begin{aligned} \omega_{2k} &= \omega + A_1(\omega)k + A_2(\omega)k^2 + A_3(\omega,k)k^3 := F(k), \\ \omega_{2k+1} &= (a\omega^{-1}+b+c\omega) + B_1(\omega)k + B_2(\omega)k^2 + B_3(\omega,k)k^3 := G(k), \end{aligned} \tag{4.11}$$

where

$$\begin{aligned} A_1(\omega) &\equiv b(1-a^{-1}\omega^2) \pmod{p^\beta}, \\ A_2(\omega) &\equiv -a^{-1}b^2\omega + ac\omega(1-\omega^2) \pmod{p^\beta}, \\ A_3(\omega,k) &\equiv 0 \pmod{p^\gamma}, \\ B_1(\omega) &\equiv b(1-a\omega^{-2}) + 2c\omega - c\omega^{-1} \pmod{p^\beta}, \\ B_2(\omega) &\equiv c(\omega-\omega^{-1}) \pmod{p^\gamma}, \\ B_3(\omega,k) &\equiv 0 \pmod{p^\gamma}, \\ \beta &= \min(3\nu,\mu),\ \gamma = \min(3\nu,\nu+\mu). \end{aligned}$$

We recall that $(a,p)=1$, $b=b_0p^\nu$, $c=c_0p^\mu$, $h=h_0p^s$, $(b_0,p)=(c_0,p)=(h_0,p)=1$.

Theorem 2. *Let the inversive congruential sequence $\{\omega_k\}$ has the maximal period τ, $\tau=2p^{m-\nu}$ and let $2\nu<\mu$. Then the following bound*

$$|S_\tau(h,\omega)| = \left|\sum_{k=0}^{\tau-1} e_{p^m}(h\omega_k)\right| \le \begin{cases} 0 & \text{if } \nu+s<n, \\ \tau & \text{if } \nu+s \ge n, \end{cases} \tag{4.12}$$

holds.

Proof. By Corollary 2 from Lemma 5 we conclude that $(a-\omega^2,p)=(1-a\omega^{-2},p)=1$. Then from (4.11) we easily obtain

$$
\begin{aligned}
|S_\tau(h,\omega)| &= \left|\sum_{\substack{k_1=0\\ k=2k_1}}^{p^{m-\nu}-1} + \sum_{\substack{k_1=0\\ k=2k_1+1}}^{p^{m-\nu}-1}\right| \le \\
&\le \left|\sum_{k_1=0}^{p^{m-\nu}-1} e_{p^m}(hF(k_1))\right| + \left|\sum_{k_1=0}^{p^{m-\nu}-1} e_{p^m}(hG(k_1))\right| = \\
&= 2p^s \begin{cases} 0 & \text{if } \nu+s<n \\ p^{m-\nu-s} & \text{if } \nu+s\ge n \end{cases} = \begin{cases} 0 & \text{if } \nu+s<m, \\ \tau & \text{if } \nu+s\ge m. \end{cases}
\end{aligned} \tag{4.13}
$$

Theorem 3. *Let $\{\omega_k\}$ be the sequence generated by the recurrent formula (3.1) and let $0<\nu_p(a-\omega^2)<\min(3\nu,\mu)$, $2\nu<\mu$. Then the sequence $\{\omega_k\}$ has a least period $\tau<2p^{m-\nu}$, and the following bound*

$$
|S_\tau(h,\omega)| \le \begin{cases} 0 & \text{if } 0<\nu_p(a-\omega^2)<\nu, \\ & \text{and } \nu_p(a-\omega^2)<n-\nu-s, \\ \tau & \text{if } 0<\nu_p(a-\omega^2)<\nu, \\ & \text{and } \nu_p(a-\omega^2)\ge n-\nu-s, \\ 4p^{\frac{n+s+2\nu}{2}} & \text{if } \nu_p(a-\omega^2)\ge\nu \text{ and } 2\nu+s<n, \\ \tau & \text{if } \nu_p(a-\omega^2)\ge\nu \text{ and } 2\nu+s\ge n \end{cases} \tag{4.14}
$$

holds.

Proof. The proof of this assertion can be obtained similarly as Theorem 2 by Lemma 3.

Corollary. *Let $\{\omega_k\}$ be the sequence generator by recurrent formula (3.1) with a least period length τ and let $0\le\nu_p(a-\omega^2)<\nu$, $2\nu<\mu$, $\nu_p(h)=s$. Then for $0<N\le\tau$ we have*

$$
|S_N(h,\omega)| \le \begin{cases} N & \text{always}, \\ 2p^{\frac{m+s+\nu}{2}}\left(\frac{N}{\tau}+\frac{\log\tau}{p}\right) & \text{if } \nu+s<m. \end{cases}
$$

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

$$
\begin{aligned}
|S_N(h,\omega)| &= \left|\sum_{\ell=0}^{N-1}\frac{1}{\tau}\sum_{k=0}^{\tau-1}\sum_{x=0}^{\tau-1} e_{p^m}(h\omega_k)e_\tau(x(k-\ell))\right| \le \\
&\le \frac{N}{\tau}\left|\sum_{k=0}^{\tau-1} e_{p^m}(h\omega_k)\right| + \sum_{x=1}^{\tau-1}\frac{1}{\min(x,\tau-x)}\left|\sum_{x=0}^{\tau-1} e^{2\pi i\left(\frac{h\omega_k}{p^m}+\frac{kx}{\tau}\right)}\right| \le \\
&\le \frac{N}{\tau}|S_N(h,\omega)| + \sum_{x=1}^{\tau-1}\frac{1}{\min(x,\tau-x)}\left|\sum_{j=0}^{1}\sum_{k=0}^{\tau-1} e^{2\pi i\frac{\Phi_j(k)}{p^{m-\nu}}}\right|,
\end{aligned}
\tag{4.15}
$$

where

$$
\begin{aligned}
&\Phi_j(k) = A_1^{(j)}k + A_2^{(j)}k^2 + \cdots,\ j=0,1;\ h = h_0p^s,\ (h_0,p)=1;\\
&A_1^{(0)}(x) \equiv hb_0(1-a^{-1}\omega^2) - d_1^{(0)}x \pmod{p^{\nu+s}},\\
&A_1^{(1)}(x) \equiv hb_0(1-a\omega^{-2}) - d_1^{(1)}x \pmod{p^{\nu+s}},\\
&A_2^{(j)} \equiv (-1)^{j+1}h_0a^{-2}b_0^2\omega^3p^{\nu+s} \pmod{p^{2\nu+s}},\ j=0,1;\\
&A_i^j \equiv 0 \pmod{p^{2\nu+s}},\ i=3,4,\ldots;\ j=0,1.
\end{aligned}
\tag{4.16}
$$

From (4.16) and Lemma 3 we conclude that the sums

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

allow nontrivial estimate only in the case when

$$
A_1^{(0)}(x) \equiv 0\,(p^\nu) \quad \text{or} \quad A_1^{(1)}(x) \equiv 0 \pmod{p^\nu}. \tag{4.17}
$$

It may occur only if $x \equiv 0 \pmod{p^s}$. Therefore, from (4.15)-(4.17), Lemma 3 and Theorems 1-2 we derive

$$
\begin{aligned}
&|S_N(h,\omega)| = N \ \text{ if } \ m \le \nu+s;\\
&|S_N(h,\omega)| \le \frac{N}{\tau}|S_\tau(h,\omega)| + 4\sum_{x=1}^{\frac{1}{2}N}\frac{1}{xp^s}p^{\frac{m+\nu+s}{2}} \ \text{ if } \ \nu+s<m.
\end{aligned}
$$

This completes the proof of corollary.

In the following theorem we obtain an upper bound for the average value of the sum $S_N(h,\omega)$ of the initial value $\omega \in R_m^*$.

Theorem 4. *Let a,b,c be parameters of the inversive congruential sequence (3.1) which satisfy the conditions*

$$(a,p)=1,\ 0>\nu=\nu_p(b),\ 2\nu<\mu=\nu_p(c).$$

Then the average value of the $S_N(h,\omega)$ over $\omega \in R_m^*$ satisfies

$$\overline{S}_N(h)=\frac{1}{\phi(p^m)}\sum_{\omega\in R_m^*}|S_N(h,\omega)|\le 3Np^{-\frac{-m-s-\nu}{4}}.$$

Proof. By the Cauchy-Schwarz inequality we obtain

$$\begin{aligned}|\overline{S}_N(h)|^2 &\le \frac{1}{\phi(p^m)}\sum_{\omega\in R_m^*}|S_N(h,\omega)|^2=\\ &=\frac{1}{\phi(p^m)}\sum_{k,\ell=0}^{N-1}\sum_{\omega\in R_m^*}e_{p^m}(h(\omega_k-\omega_\ell))\le\\ &\le\frac{1}{\phi(p^m)}\sum_{r=0}^{m}\sum_{\substack{k,\ell=0\\ k\equiv\ell(mod\ p^r)}}^{N-1}|\sigma_{k,\ell}(h)|.\end{aligned}$$

Hence, by Theorem 1 we have (with $h_1=1$,$h_2=-1$)

$$|\overline{S}_N|^2\le$$

$$\le\frac{1}{\phi(p^m)}\left(\sum_{t=0}^{m-\nu-s-1}p^{\frac{m+\nu+s+t}{2}}\sum_{\substack{k,\ell\le N\\ k\equiv\ell(mod\ p^t)}}1+\sum_{t=m-\nu-s}^{m}p^m\sum_{\substack{k,\ell\le N\\ k\equiv\ell(mod\ p^t)}}1\right)\le$$

$$\le\frac{N^2}{\phi(p^m)}\left(\sum_{t=m-\nu-s-1}p^{\frac{m+\nu+s-t}{2}}+\sum_{t=m-\nu-s}^{m}p^{m-t}\right)\le 4\frac{N^2}{p^m}\left(p^{\frac{m+s+\nu}{2}}+p^{\nu+s}\right).$$

From this we obtain for any $N\le 2p^{m-\nu}$

$$\overline{S}_N(h)\le 2N\left(p^{-\frac{m-s-\nu}{4}}+p^{-\frac{m-s-\nu}{2}}\right)\le 3Np^{-\frac{m-s-\nu}{4}}.$$

5. Discrepancy bounds

Equidistribution and statistical independence properties (unpredictability) of the pseudorandom numbers can be analyzed based of the discrepancy of certain point sets in $[0,1)^d$. For N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1} \in [0,1)^d$, the discrepancy is defined by

$$D(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}) = \sup_I \left| \frac{A_N(I)}{N} - |I| \right|, \tag{5.1}$$

where the supremum is extended over all subintervals I of $[0,1)^d$, $A_N(I)$ is the number of points among $\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}$ falling into I, and $|I|$ denotes the d-dimensional volume I.

For study the discrepancy of points one usually uses the following lemmas.

For integers $q \geq 2$ and $d \geq 1$, let $C_q(d)$ denote the set of all nonzero lattice points $(h_1, \ldots, h_d) \in \mathbb{Z}^d$ with $-\frac{q}{2} < h_j \leq \frac{q}{2}$, $1 \leq j \leq d$. We define

$$r(h,q) = \begin{cases} q \sin \frac{\pi |h|}{q} & \text{if } h \in C_1(q), \\ 1 & \text{if } h = 0 \end{cases}$$

and

$$r(\mathfrak{h}, q) = \prod_{j=1}^{d} r(h_j, q) \quad \text{for } \mathfrak{h} = (h_1, \ldots, h_q) \in C_d(q).$$

Lemma 6. *Let $N \geq 1$ and $q \geq 2$ be integers. For N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1} \in [0,1)^d$, the discrepancy $D(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1})$ satisfies*

$$D_N(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}) \leq \frac{d}{q} + \frac{1}{N} \sum_{\mathfrak{h} \in C_d(q)} \frac{1}{r(\mathfrak{h}, q)} \left| \sum_{n=0}^{N-1} e(\mathfrak{h} \cdot \mathfrak{t}_n) \right|.$$

(Proof see in [29]).

Lemma 7. *Let $\{\mathfrak{y}_k\}$, $\mathfrak{y}_k \in \{0, 1, \ldots, q-1\}^d$, is a purely periodic sequence with a period τ. Then for the discrepancy of the points $\mathfrak{t}_k = \frac{\mathfrak{y}_k}{q} \in [0,1)^d$, $k = 0, 1, \ldots, N-1$; $N \leq \tau$, the following estimate*

$$D_N(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}) \leq \frac{d}{q} + \frac{1}{N} \sum_{\mathfrak{h} \in C_d(q)} \sum_{h_0 \in \left(-\frac{\tau}{2}, \frac{\tau}{2}\right]} r^{-1}(\mathfrak{h}, q) r^{-1}(h_0, \tau) \cdot |\mathfrak{S}|$$

holds, where

$$\mathfrak{S} := \sum_{k=0}^{\tau-1} e\left(\mathfrak{h}\cdot\mathfrak{t}_k + \frac{kh_0}{\tau}\right).$$

This assertion follows from Lemma 1 and from an estimate of uncomplete exponential sum through complete exponential sum.

Lemma 8. *The discrepancy of N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1} \in [0,1)^d$ satisfies*

$$D_N(\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1}) \geq \frac{\pi}{2N((\pi+1)^\ell - 1)\prod\limits_{j=1}^{d}\max(1,|h_j|)}\left|\sum_{n=0}^{N-1} e(\mathfrak{h}\cdot\mathfrak{t}_n)\right|$$

for any nonzero lattice point $\mathfrak{h} = (h_1, \dots, h_d) \in \mathbb{Z}^d$, where ℓ denotes the number of nonzero coordinates of $\mathfrak{h}$.

(Proof see [28], Lemma 1).

Lemma 9. ([7], Lemma 3) *Let $q \geq 2$ be an integer. Then*

$$\sum_{\substack{\mathfrak{h}\in C_d(q)\\ \mathfrak{h}\equiv 0 (\mathrm{mod}\ v)}} \frac{1}{r(\mathfrak{h},q)} \leq \frac{1}{v}\left(\frac{2}{\pi}\log q + \frac{7}{5}\right)^d$$

for any divisor v of q with $1 \leq v < q$.

Theorem 5. *Let $p > 2$ be a prime number and m, a, b, c and ω be integers, $m \geq 3$, $(a,p) = (\omega,p) = 1$, $0 < \nu_p(b) < \nu_p(c)$, $a \not\equiv \omega^2 \pmod p$. Then for the sequence $\{x_k\}$, $x_k = \frac{\omega_k}{p^m}$, $k = 0, 1, \dots$, where ω_k defined by the recursion (3.1), we have*

$$D_N(x_0, x_1, \dots, x_{N-1}) \leq \frac{1}{p^m} + \frac{2p^{m-\nu 2}}{N}\left(\frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^2 + 1\right), \tag{5.2}$$

where $1 \leq N \leq \tau$, and τ is the least period length for $\{\omega_k\}$.

Proof. Since $a \not\equiv \omega^2 \pmod p$ and $0 < 2\nu_p(b) < \nu_p(c)$ we get that the sequence $\{\omega_k\}$, $k = 0, 1, \ldots$, has the period τ, $\tau = 2p^{m-\nu}$, $\nu = \nu_p(b)$. Let $D_N := D_N(x_0, x_1, \ldots, x_{N-1})$. Hence, by Lemma 7 (for $d = 1$) we have

$$\begin{aligned} D_N \leq & \frac{1}{p^{m-\nu}} + \frac{1}{N} \sum_{0<|h|<\frac{1}{2}p^{m-\nu}} \sum_{|h_0|\leq\frac{1}{2}\tau} \left(r\left(h, \frac{1}{2}p^{m-\nu}\right) r\left(h_0, \tau\right)\right)^{-1} \times \\ & \times \left| \sum_{k=0}^{\tau-1} e^{2\pi i\left(\frac{hx_k}{p^m} + \frac{kh_0}{\tau}\right)} \right| \leq \\ \leq & \frac{1}{p^{m-\nu}} + \frac{1}{N} \sum_{h,h_0} \left(r\left(h, \frac{1}{2}p^{m-\nu}\right) r\left(h_0, \tau\right)\right)^{-1} \times \\ & \times \left(\left| \sum_{k=0}^{p^{m-\nu}-1} e^{2\pi i\left(\frac{h\omega_{2k}}{p^m} + \frac{kh_0}{p^{m-\nu}}\right)} \right| + \left| \sum_{k=0}^{p^{m-\nu}-1} e^{2\pi i\left(\frac{h\omega_{2k+1}}{p^m} + \frac{kh_0}{p^{m-\nu}}\right)} \right| \right). \end{aligned}$$

Applying Corollary 1 from Lemma 5 and Lemma 3 we obtain easily that

$$D_N(x_0, x_1, \ldots, x_{N-1}) \leq \frac{1}{p^{m-\nu}} + \frac{2p^{\frac{m-\nu}{2}}}{N} \left(\frac{1}{p} \left(\frac{2}{\pi} \log p^m + \frac{7}{5} \right)^2 + 1 \right). \tag{5.3}$$

Consider the inversive congruential sequence $\{\omega_k\}$ with the conditions of Theorem 5 and organize the new sequence $\{\mathfrak{y}_k\}$, where $\mathfrak{y}_k \in \mathbb{Z}^d$, $d \in \mathbb{N}$, $\mathfrak{y}_k = (\omega_k, \omega_{k+1}, \ldots, \omega_{d-1})$.

The statistical independence properties of the sequence are analyzed by means of the d-dimensional serial tests ($d = 2, 3, \ldots$) which employ the discrepancy of d-dimensional vectors $\mathfrak{t}_k$, where $\mathfrak{t}_k = \frac{\mathfrak{y}_k}{p^m}$, $k = 0, 1, \ldots$.

We shall consider only the cases $d = 2$ or 3. Let $D_\tau^{(d)}$ denote the discrepancy of points $\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{\tau-1}$.

Theorem 6. *The discrepancy $D_\tau^{(2)}$ of the points constructed by inversive congruential sequence (3.1) with the least period length $\tau = 2p^{m-\nu}$, satisfies*

$$D_\tau^{(2)} \leq \frac{1}{p^{m-\nu}} + \frac{\sqrt{p}}{\sqrt{p}-1} p^{-\frac{m-2\nu}{2}} \left(\frac{1}{\pi} \log p^{m-\nu} + \frac{3}{5} \right)^2.$$

Proof. In order to apply Lemma 6 we must have an estimate for the sum

$$\sum_{k=0}^{\tau-1} e_{p^m}(h_1\omega_k + h_2\omega_{k+1}) = \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_{2k} + h_2\omega_{2k+1}) + \\ + \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_{2k+1} + h_2\omega_{2k+2}) = \sum\nolimits_1 + \sum\nolimits_2,$$

say. By Corollary 1 of Lemma 5 we get

$$h_1\omega_{2k} + h_2\omega_{2k+1} \equiv$$

$$\equiv \left(h_1\omega + h_2(b + c\omega + a\omega^{-1})\right) + \\ + k(h_1(b(1 - a^{-1}\omega^2) + a^{-1}c\omega) + h_2(b(1 - a\omega^{-2}) + 2c\omega)) + \\ + k^2(h_1(a^{-2}b^2\omega^3 + a^{-1}c\omega) + h_2(-a^{-1}c - \omega^{-1}c)) \pmod{p^{\delta+\ell}},$$

where $\delta = \min(3\nu, \mu)$, $\ell = \nu_p((h_1, h_2, p^m))$.

Since the congruences

$$h_1(b(1 - a^{-1}\omega^2) + a^{-1}c\omega) + h_2(b(1 - a\omega^{-2}) + 2c\omega) \equiv 0 \pmod{p^{\ell+\nu+1}},$$

$$h_1(a^{-2}b^2\omega^3 + a^{-1}c\omega) + h_2(-a^{-1}c - \omega^{-1}c) \equiv 0 \pmod{p^{\ell+\nu+1}}$$

cannot hold simultaneously (taking into account that $1 - a^{-1}\omega^2 \not\equiv 0 \pmod{p}$), we obtain (by Lemma 2):

$$\left|\sum\nolimits_1\right| = \begin{cases} p^{\frac{m-\ell}{2}} & \text{if } \nu_p(h_1) = \nu_p(h_2) = \ell,\ h_1 - a\omega^{-2}h_2 \equiv 0 \pmod{p^\nu}, \\ 0 & \text{else.} \end{cases}$$

Similarly, we have

$$\left|\sum\nolimits_2\right| = \begin{cases} p^{\frac{m-\ell}{2}} & \text{if } \nu_p(h_1) = \nu_p(h_2) = \ell,\ h_1 - a\omega^{-2}h_2 \equiv 0 \pmod{p^\nu}, \\ 0 & \text{else.} \end{cases}$$

Now, Lemmas 6 and 9 give for $q = 2p^{m-\nu}$

$$D_\tau^{(2)} \le \frac{1}{p^{m-\nu}} + \frac{1}{p^{\frac{m-2\nu}{2}}} \sum_{\ell=0}^{m-\nu-1} p^{-\frac{\ell}{2}} \left(\sum_{\substack{h \in C_1(p^{m-\nu}) \\ \nu_p(h)=\ell}} \frac{1}{r(h, p^{m-\nu})} \right)^2 \le \\ \le \frac{\sqrt{p}}{\sqrt{p}-1} \cdot p^{-\frac{m-2\nu}{2}} \left(\frac{1}{\pi} \log p^{m-\nu} + \frac{3}{5} \right)^2 + \frac{1}{p^{m-\nu}}.$$

Theorem 7. *The discrepancy $D_\tau^{(3)}$ which is constructed by the inversive congruential sequence (3.1) with maximal period length $\tau = 2p^{m-\nu}$ satisfies*

$$D_\tau^{(3)} \le \frac{\sqrt{p}}{\sqrt{p}-1} p^{-\frac{m}{2}+\nu} \left(\frac{1}{\pi}\log p^{m-\nu} + \frac{3}{5}\right)^3 + \frac{3}{2}p^{-m+\nu}.$$

Proof. As above we have

$$\begin{aligned}
&\sum_{k=0}^{\tau-1} e_{p^m}(h_1\omega_k + h_2\omega_{k+1} + h_3\omega_{k+2}) = \\
&= \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_{2k} + h_2\omega_{2k+1} + h_3\omega_{k+2}) + \\
&\quad + \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_{2k+1} + h_2\omega_{2k+2} + h_3\omega_{2k+3}) := \sum\nolimits_1 + \sum\nolimits_2.
\end{aligned}$$

Corollary 1 from Lemma 5 gives

$$\begin{aligned}
&h_1\omega_{2k} + h_2\omega_{2k+1} + h_3\omega_{2k+2} = A_0(h_1,h_2,h_3) + \\
&+ k((h_1+h_3)(1-a^{-1}\omega^2)b + h_2 b(1-a\omega^{-2}) + A_1(h_1,h_2,h_3)) + \\
&+ k^2((h_1+h_3)a^{-2}\omega^3 b^2 + A_2(h_1,h_2,h_3))
\end{aligned} \tag{5.4}$$

and also

$$\begin{aligned}
&h_1\omega_{2k+1} + h_2\omega_{2k+2} + h_3\omega_{2k+3} = B_0(h_1,h_2,h_3) + \\
&+ k((h_1+h_3)(1-a\omega^{-2})b + h_2 b(1-a^{-1}\omega^2) + B_1(h_1,h_2,h_3)) + \\
&+ k^2(h_2 a^{-2}\omega^3 b^2 + B_2(h_1,h_2,h_3)),
\end{aligned} \tag{5.5}$$

where

$$\begin{cases}
A_1(h_1,h_2,h_3) \equiv B_1(h_1,h_2,h_3) \equiv 0 \pmod{p^{2\nu+\ell}}, \\
A_2(h_1,h_2,h_3) \equiv B_2(h_1,h_2,h_3) \equiv 0 \pmod{p^{\delta+\ell}}, \\
\ell = \nu_p((h_1,h_2,p^m)) \;\; \delta = \min(3\nu,\mu).
\end{cases}$$

Thus, by Lemma 2 we obtain

$$\left|\sum\nolimits_1\right| = \begin{cases}
0 & \text{if } \nu_p((h_1+h_2) - a\omega^{-2}h_2) < \nu_p((h_1+h_3)b) \le m, \\
p^{m-\nu} & \text{if } m-\nu \le \nu_p((h_1+h_3)b) \le \nu_p((h_1+h_3)b - a\omega^{-2}h_2 b), \\
p^{\frac{m+\ell}{2}} & \text{if } m-\nu > \nu_p((h_1+h_3)b) \ge \nu_p((h_1+h_3)b - a\omega^{-2}h_2 b),
\end{cases}$$

where $\ell_1 = \nu_p(h_1 + h_3 - h_2 a^{-1} y_0^2)$. An analogous estimate holds for the sum $\sum_2$.

Hence, from Lemmas 6 and 9 we obtain

$$D_\tau^{(3)} \le \frac{\sqrt{p}}{\sqrt{p}-1} p^{-\frac{m}{2}+\nu} \left(\frac{1}{\pi} \log p^{m-\nu} + \frac{3}{5} \right)^3 + \frac{3}{2} p^{-m+\nu}.$$

In conclusion we prove the lower bound for $D_\tau^{(2)}$.

Theorem 8. *Let p be a prime and m, a, b, c and ω be integers with $m \ge 3$. Suppose that $(a,p) = 1$, $0 < 2\nu_p(b) < \nu_p(c)$, and $a \not\equiv \omega^2 \pmod p$, $a \not\equiv -\omega^2 \pmod{p^\nu}$. Then*

$$D_\tau^{(2)} \ge \frac{1}{4(\pi+2)} p^{-\frac{m}{2}+\nu} h_*^{-1},$$

where $h_* = |h_1 h_2 h_3|$ under condition $h_1, h_2, h_3 \in C_1(p^m)$, $h_1 h_2 h_3 \ne 0$, $(h_1, h_2, h_3) = 1$, $h_1 + h_2 \equiv h_* a \omega^{-2} \pmod{p^\nu}$.

Proof. By the Lemma 8 for $d = 2$, $N = 2p^{m-\nu}$, we have

(5.6)

$$\begin{aligned} D_\tau^{(2)} \ge & \frac{1}{4(\pi+2)p^{m-\nu}} \left| \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_k + h_2\omega_{k+1}) \right| = \\ = & \frac{1}{4(\pi+2)p^{m-\nu}} \left| \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_{2k} + h_2\omega_{2k+1}) + \right. \\ & \left. + \sum_{k=0}^{p^{m-\nu}-1} e_{p^m}(h_1\omega_{2k+1} + h_2\omega_{2k+2}) \right| = \frac{1}{4(\pi+2)p^{m-\nu}} \left| \sum\nolimits_1 + \sum\nolimits_2 \right|, \end{aligned}$$

say.

Let $(h_1, h_2, p^m) = p^\ell$, $h = p^\ell h_1^0$, $h_2 = h_2^0 p^\ell$, $(h_1^0, h_2^0) = 1$. From (5.4)–(5.5) we can see easily that the congruences

$$\begin{aligned} (h_1^0 + h_3^0)(1 - a\omega^{-2}) + h_2^-(1 - a^{-1}\omega^2) &\equiv 0 \pmod{p^\nu}, \\ (h_1^0 + h_3^0)(1 - a^{-1}\omega^2) + h_2^-(1 - a\omega^{-2}) &\equiv 0 \pmod{p^\nu} \end{aligned}$$

cannot be satisfied simultaneously if $a \not\equiv \omega^2 \pmod p$, $a \not\equiv -\omega^2 \pmod{p^\nu}$. We select h_1, h_2, h_3 so that $(h_1, h_2, h_3) = 1$, $h_1 + h_3 - h_2 a \omega^{-2} \equiv 0 \pmod{p^\nu}$, $(h_1 + h_3, p) = 1$. Then Lemma 2 gives

$$\left| \sum\nolimits_1 \right| = p^{\frac{m+\nu}{2}}, \quad \left| \sum\nolimits_2 \right| = 0. \tag{5.7}$$

Hence, from (5.6)-(5.7) we infer

$$D_\tau^{(2)} \geq \frac{1}{4(\pi+2)} p^{-\frac{m}{2}+\nu} h_*^{-1},$$

where

$$h_* = \min_{\substack{h_1,h_2,h_3 \in C_1(p^m) \\ h_1 h_2 h_3 \neq 0 \\ (h_1,h_2,h_3)=1 \\ h_1+h_3 \equiv h_2 a \omega^{-2} \pmod{p^\nu}}} |h_1 h_2 h_3|.$$

Remark. Theorems 7 and 8 show that, in general, the upper bound is the best possible up to the logarithmic factor for any inversive congruential sequence $\{(x_k, x_{k+1})\}$, $k = 0, 1, \ldots$ (defined by the recursion (3.1)), since there exists inversive congruential sequence $\{(x_k, x_{k+1})\}$ with $D_\tau^{(2)} \geq \frac{1}{8(\pi+2)} p^{-\frac{m}{2}+\nu}$. (Example, if $a\omega^{-2} \equiv 2 \pmod{p^\nu}$, $h_1 = h_2 = h_3 = 1$).

Hence, on the average discrepancy $D_\tau^{(2)}$ has an order of magnitude between $p^{-\left(\frac{m}{2}-\nu\right)}$ and $p^{-\left(\frac{m}{2}-\nu\right)} \log^2 p^m$. An analogous statement can be proved for $D_\tau^{(3)}$. Thus we can conclude that the inversive congruential sequences pass the test on unpredictability if the parameters a, b, c, ω satisfy conditions

$$(a, p) = 1, \ 0 < 2\nu_p(b) < \nu_p(c), \ a \not\equiv \omega^2 \pmod{p}.$$

References

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

[2] **Eichenauer-Herrmann J.,** Inversive congruential pseudorandom numbers: a tutorial, *Internat. Statist. Rev.,* **60** (1992), 167-176.

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

[4] **Eichenauer-Herrmann J.,** Statistical independence of a new class of inversive congruential pseudorandom numbers, *Math. Comp.,* **60** (1993), 375-384.

[5] **Eichenauer-Herrmann J.,** Compound nonlinear congruential pseudorandom numbers, *Monatsh. Math.,* **117** (1994), 213-222.

[6] **Eichenauer-Herrmann J.,** Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers, *Math. Comp.,* **62** (1994), 783-786.

[7] **Eichenauer-Herrmann J.,** A unified approach to the analysis of compound pseudorandom numbers, *Finite Fields and their Appl.,* **1** (1995), 102-114.

[8] **Eichenauer-Herrmann J.,** Pseudorandom number generation by nonlinear methods, *Internat. Statist. Rev.,* **63** (1995), 247-255.

[9] **Eichenauer-Herrmann J. and Emmerich F.,** Compound inversive congruential pseudorandom numbers: an average-case analysis, *Math. Comp.,* **65** (1996), 215-225.

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

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

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

[13] **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.

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

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

[16] **Knuth D.E.,** *The art of computer programming, Vol.2, Seminumerical algorithms,* 2nd ed., Addison-Wesley, Reading, MA, 1981.

[17] **L'Ecuyer P.,** Uniform random number generation, *Ann. Oper. Res.,* **53** (1994), 77-120.

[18] **Levin M.B.,** Discrepancy estimates of completely uniform distributed sequences and pseudorandom sequence, *Intern. Math. Res. Notes,* **22** (1999), 1231-1251.

[19] **Levin M.B.,** Explicit digital inversive pseudorandom numbers, *Math. Slovaca.,* **50** (5) (2000) 581-598.

[20] **Levin M.B.,** On the statistical independence of compound pseudorandom numbers over part of the period, *ACM Trans. on Modeling and Computer Simulation,* **11** (3) (2001), 294-311.

[21] **Niederreiter H.,** Some new exponential sums with applications to pseudorandom numbers, *Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. Janos Bolyai* **13**, North-Holland, Amsterdam, (1976), 209-232.

[22] **Niederreiter H.,** Pseudo-random numbers and optimal coefficients, *Adv. Math.,* **26** (1977), 99-181.

[23] **Niederreiter H.,** Quasi-Monte Carlo methods and pseudorandom numbers, *Bull. Amer. Math. Soc.,* **84** (1978), 957-1041.

[24] **Niederreiter H.,** The serial test for congruential pseudorandom numbers generated by inversions, *Math. Comp.,* **52** (1989), 135-144.

[24] **Niederreiter H.,** Lower bounds for the discrepancy of inversive congruential pseudorandom numbers, *Math. Comp.,* **55** (1990), 277-287.

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

[27] **Niederreiter H.,** Recent trends in random number and random vector generation, *Ann. Oper. Res.,* **31** (1991), 323-345.

[28] **Niederreiter H.,** Nonlinear methods for pseudorandom number and vector generation, *Simulation and Optimization,* eds. G. Pflug and U. Dieter, Lecture Notes in Econom. and Math. Systems **374**, Springer Verlag, Berlin, 1992, 145-153.

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

[30] **Niederreiter H.,** Finite fields, pseudorandom numbers and quasirandom points, *Finite Fields, Coding Theory and Advances in Communications and Computing,* eds. G.L. Mullen and P.J.-S. Shiue, Dekker, New York, 1993, 375-394.

[31] **Niederreiter H.,** On a new class of pseudorandom numbers for simulation methods, *J. Comput. Appl. Math.,* **56** (1994), 159-167.

[32] **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.

[33] **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.

[34] **Niederreiter H. and Shparlinski I.,** On the distribution of inversive congruential pseudorandom numbers in parts of the period, *Math. of Comput.,* **70** (2000), 1569-1574.

[35] **Niederreiter H. and Shparlinski I.,** Recent advances in the theory of nonlinear pseudorandom number generators, *Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods 2000,* Springer Verlag, Berlin, 2002, 86-102.

[36] **Stonaham R.,** On the uniform ε-distribution of residue within the periods of rational fractions with applications to normal numbers, *Acta Arith.,* **22** (1973), 371-389.

[37] **Varbanets S.,** Exponential sums on the sequences of inversive congruential pseudorandom numbers, *Šiauliai Math. Semin.,* **3** (11) (2008), 247-261.

[38] **Varbanets S.,** On inversive congruential generator for pseudorandom numbers with prime power modulus, *Annales Univ. Sci. Budapest. Sect. Comp.,* **29** (2008), 277-296.

(Received February 16, 2009)

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

S. Varbanets
Dept. of Mathematical Ware
of Computer Systems
Odessa National University
Dvoryanskaya 2
65026 Odessa, Ukraine
varb@sana.od.ua