УДК 511

S. P. Varbanets
Odessa National University

INVERSIVE CONGRUENTIAL GENERATOR WITH PRIME POWER MODULUS

Варбанець С. П. Iнверсний конгруенцiальний генератор за модулем степеня простого. Розглядається узагальнений iнверсний конгруентний генератор, який породжує послiдовнiсть псевдовипадкових чисел. Будуються оцiнки експоненцiальних сум на таких послiдовностях. Отриманi нетривiальнi границi для функцiї ухилення s-мiрних точок вiд рiвномiрного розподiлу.
Ключовi слова: iнверсний конгруентний генератор, дискрепансiя, псевдовипадковi числа, експоненцiальнi суми.

Варбанец С. П. Инверсный конгруенциальный генератор по модулю степени простого. Рассматривается обобщенный инверсный конгруэнтный генератор, порождающий последовательность псевдослучайных чисел. Строятся оценки экспоненциальных сумм на таких последовательностях. Получены нетривиальные границы для функции уклонения s-мерных точек от равномерного распределения.
Ключевые слова: инверсный конгруэнтный генератор, дискрепансия, псевдослучайные числа, експоненциальные суммы.

Varbanets S. P. Inversive congruential generator with prime power modulus. Consider the generalized inversive congruential generator which generates the sequence of pseudorandom numbers. Construct estimates of the exponential sums on these sequence. Obtain nontrivial bounds for the discrepancy s-dimensional vectors from the uniform distribution.
Key words: inversive congruential generator, discrepancy, pseudorandom numbers, exponential sums.

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 fields of research is described in the survey articles ([2, 6, 7, 13, 14, 16, 17, 18]) and in Niederreiter's monograph [18]. 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, 13]). Four types of inversive congruential generators can be distinguished, depending on whether the modulus is a prime ([1, 7, 15]), an odd prime power([20, 21, 22]), a power of two([8, 11]) or a product of distinct prime numbers([5, 12]).

In the case of an odd prime-power modulus the inversive congruential generator is defined in the following way:
Let p be a prime, $p \geq 3$, n be a natural number, $n \geq 2$. For given $a, b \in \mathbb{Z}$, $(a, p) = 1$, $b \equiv 0 (mod\ p)$, we take an initial value $\omega_0 = \omega \in \mathbb{Z}$, $(\omega, p) = 1$, and then the recurrence relation

$$\omega_{k+1} \equiv a\omega_k^{-1} + b (mod\ p^n) \tag{1}$$

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

It is clear that the numbers $\frac{\omega_0}{p^n}, \frac{\omega_1}{p^n}, \ldots$ belong to the interval $[0,1)$ and form a sequence of inversive congruential pseudorandom numbers with modulus p^n.
Such method of pseudorandom number generation was introduced in [10]. In practice, one works with a large power p^n of a small prime p. Surveys of results of inversive congruential pseudorandom numbers see in [9], [15], [17].

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

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

where $N \leq \tau$, τ is a least period length of the sequence $\omega_0, \omega_1, \ldots$ considered modulo p^n, $(h_1, \ldots, h_d) \in \mathbb{Z}^d$, $(h_1, \ldots, h_d) \neq 0 \in \mathbb{Z}^d$.
The sums $S^d(h_1, \ldots, h_d)$ are considered in [20, 22].

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

And now we consider the generator

$$\omega_{k+1} \equiv a\omega_k^{-1} + b + (k+1)c\omega_k (mod\ p^n)$$

Notations. The letter p denotes a prime number, $p \geq 3$. For $n \in \mathbb{N}$ the notation R_n(accordingly, R_n^*) denotes the complete(accordingly, reduced) system of residues modulo p^n. 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^n. 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 $\mathfrak{u}, \mathfrak{v} \in \mathbb{R}^d$.

In the sequel we shall apply the following statements.

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

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

Lemma 2. *Let* $p > 3$ *be a prime,* $n \in \mathbb{N}, n \geq 2$ *and let* $f(x) = A_1x + A_2x^2 + p(A_3x^3 + \cdots)$ *be a polynomial over* $\mathbb{Z}$*, moreover,* $(A_1, A_2, p) = 1$*. Then*

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

These lemmas are well-known.

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 using the estimates of the Kloosterman sums and Lemma 2 in[23] we proved

Lemma 3. *For $\nu \le n$, $n \ge 2$, the following estimates*

$$\left|\sum_{x\in R_n} e^{2\pi i\frac{f(x)}{p^n}}\right| = \begin{cases} p^{\frac{n+\nu}{2}} & \text{if } \nu_p(A_1)\ge \nu, \\ 0 & \text{else,} \end{cases} \tag{3}$$

$$\left|\sum_{x\in R_n^*} e^{2\pi i\frac{f(x)+g(x^{-1})}{p^n}}\right| \le 4p^{\frac{n}{2}} \tag{4}$$

hold.

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

$$\Psi_{k+1}(\omega) = \frac{a}{\Psi_k(\omega)} + b + (k+1)c\omega_k\,(mod\ p^n),\ k = 0,1,2,\dots, \tag{5}$$

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

In subsequent we shall write $\Psi_k(\omega) = \omega_k$, $\omega_0 = \omega$ is the initial value. The sequence $\{\omega_k\}$ defined by (5) can be considered as the generalization of the inversive congruential sequence $\{u_k\}$, which has been studied H. Niederreiter and I. Shparlinski([20]), S. Varbanets([22, 23]), P. Varbanets and S. Varbanets ([24]). In order to show that the sequence ω_k is defined by the parameters a, b, c, ω we shall denote it as $\Omega(\omega,a,b,c;p^n)$. We shall obtain two representations for $\omega_k \in \Omega(\omega,a,b,c;p^n)$:

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

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

Lemma 4. *Let Ψ_k be the transformation defined by (5) and let $c^r \equiv 0(mod\ p^n)$, $r > 1$. Then for $k = 0,1,2,\dots$*

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

(ii) $\Psi_k(\omega) := \omega_k \equiv \frac{A_0^{(k)}+A_1^{(k)}\omega+\dots+A_r^{(k)}\omega^r}{B_0^{(k)}+B_1^{(k)}\omega+\dots+B_r^{(k)}\omega^r}\,(mod\ p^n)$

where the following congruences mod p^γ, $\gamma = \min(-3\nu, \mu+\nu)$, $\nu = \nu_p(b) < \nu_p(c) = \mu$, hold:

$$\begin{cases} \Psi_{2k}(\omega) = \frac{A_0^{(2k)}+A_1^{(2k)}\omega+\dots+A_r^{(2k)}\omega^r}{B_0^{(2k)}+B_1^{(2k)}\omega+B_2^{(2k)}\omega^2+\dots+B_r^{(2k)}\omega^r}, \\ \\ \Psi_{2k+1}(\omega) = \frac{C_0^{(2k+1)}+C_1^{(2k+1)}\omega+C_2^{(2k+1)}\omega^2+\dots+C_r^{(2k)}\omega^r}{D_0^{(2k+1)}+D_1^{(2k+1)}\omega+\dots+D_r^{(2k)}\omega^r}, \end{cases} \tag{6}$$

$$\begin{cases} A_0^{(2k)} = ka^k b, \;\; A_1^{(2k)} = a^k + k\overline{A}_1^{(2k)} b^2, \\ B_0^{(2k)} = a^k + \overline{B}_0^{(2k)} b^2, \;\; B_1^{(2k)} = ka^{k-1} b, \\ B_2^{(2k)} = ka^{k-1} c; \\ \\ C_0^{(2k+1)} = a^{k+1} + \overline{C}_0^{(2k+1)} b^2, \\ C_1^{(2k+1)} = (k+1)a^k b, \\ C_2^{(2k+1)} = (k+1)a^k c; \\ \\ D_0^{(2k+1)} = ka^k b, \\ D_1^{(2k+1)} = a^k + ka^k c + \overline{D}_1^{(2k+1)} b^2. \end{cases} \tag{7}$$

$$\begin{cases} A_{2\ell-1}^{(2k)} \equiv 0(mod\ c^\ell), \;\; A_{2\ell}^{(2k)} \equiv 0(mod\ bc^\ell), \\ B_{2\ell-1}^{(2k)} \equiv 0(mod\ bc^{\ell-1}), \;\; B_{2\ell}^{(2k)} \equiv 0(mod\ c^\ell), \\ C_{2\ell-1}^{(2k+1)} \equiv 0(mod\ bc^{\ell-1}), \;\; C_{2\ell}^{(2k+1)} \equiv 0(mod\ c^\ell), \\ D_\ell^{(2k+1)} = A_\ell^{(2k)}, \;\; \ell = 2, 3, \dots \end{cases} \tag{8}$$

The proof of this lemma is similar to proof of Lemma 4 ([25]).

Cosequence 1. *For $k = 0, 1, 2, \dots$ we have*

$$\omega_{2k} = (kca + p^\gamma f_0(k))\omega^{-1} + (kb + A_k p^\gamma) + (1 + f_1(k)b^2)\omega + \\ + (-ka^{-1}b + p^\gamma f_2(k))\omega^2 + f_3(f)p^\mu \omega^3 + p^\gamma F(k, \omega, \omega^{-1})$$

$$\omega_{2k+1} = p^\nu g_0(k) + (2k+1)c\omega + (a + g_{-1}(k)p^\delta)\omega^{-1} + \\ + p^\gamma G(k, \omega, \omega^{-1})$$

where

$$F(u, v, w), G(u, v, w) \in R_n[u, v, w], \;\; f_1, f_2, f_3 \in R_n[k], \;\; \delta = \min(2\nu, \mu).$$

Cosequence 2. *For any $\omega \in R_n^*$ we have*

$$\omega_{2k} = \omega + k(ac\omega^{-1} + b - a^{-1}b\omega^2 + p^\delta A_1(\omega, \omega^{-1})) + \\ + k^2(-a^{-1}b^2\omega + a^{-2}b^2\omega^3 + a^{-1}c\omega(1 - \omega^2) + p^\gamma A_2(\omega, \omega^{-1})) + \\ + p^\gamma k^3 A_3(k, \omega, \omega^{-1})$$

$$\omega_{2k+1} = (a\omega^{-1} + b + c\omega) + \\ + k(b(1 - a\omega^{-2}) + c\omega^{-1}(2\omega^2 - a^2) + p^\gamma B_1(\omega, \omega^{-1})) + \\ + k^2 \big(2bc(1 - a^{-1}\omega^2) + 2ac^2\omega^{-1} + b^2(1 - a^{-1}\omega^2) + \\ + c(1 - \omega^2) + p^\gamma B_2(\omega, \omega^{-1})\big) + p^\gamma k^3 B_3(k, \omega, \omega^{-1}),$$

where $A_i, B_i \in R_n[\omega, \omega^{-1}]$, $A_3, B_3 \in R_n[k, \omega, \omega^{-1}]$.

Cosequence 3. *Let τ be the period length of $\Omega(\omega, a, b, c; p^n)$ and $\nu_p(b) = \nu$, $\nu_p(c) = \mu > \nu$.*

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

(B) If $0 < \nu_p(a-\omega^2) = \eta < \gamma$*, then* $\tau = 2p^{n-\nu-\eta}$*,*

(C) In other cases: $\tau \le 2p^{n-\nu-\gamma}$*.*

Main Results. 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

$$\sum_{n=0}^{N-1} e^{2\pi i m x_n}, \ (N \to \infty) \tag{9}$$

where m is any non-zero integer.

Thus first we obtain the estimates of certain exponential sums over the inversive congruential sequence which was defined (5).

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

$$\sigma_{k,\ell}(h_1,h_2) := \sum_{\omega \in R_m^*} e_{p^m}(h_1\omega_k + h_2\omega_\ell) \tag{10}$$

Here we consider ω_k, ω_ℓ as a function at ω generated by (5).

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

$$|\sigma_{k,\ell}(h_1,h_2)| \le$$

$$\le \begin{cases} 0, & \text{if } t \ne \kappa+\nu, \\ & \text{and } \min(t,\kappa+\nu) < n-s-\nu, \\ 2p^{\frac{n+\nu+s+t}{2}}, & \text{if } t = \kappa+\nu \\ & \text{and } n-\nu-s-t > 0, \\ p^{n-1}(p-1), & \text{if } \min(t,\kappa+\nu) \ge n-s-\nu. \end{cases} \tag{11}$$

hold.

Proof. Put $n_1 = n-s$. First, let k, ℓ be non-negative integers of different parity, for example, $k := 2k$, $\ell := 2\ell+1$. By Cosequence 1 from Lemma 4 we obtain

$$\begin{aligned} h_1^0\omega_{2k} + h_2^0\omega_{2\ell+1} &= \big(A_0 + A_1\omega + A_2\omega^2 + A_3\omega^3 + b^3\omega^4 H(\omega)\big) + \\ &+ \big(A_{-1}\omega^{-1} + A_{-2}\omega^{-2} + A_{-3}\omega^{-3} + b^3\omega^{-4}G(\omega^{-1})\big) = \\ &= F(\omega,\omega^{-1}), \end{aligned} \tag{12}$$

where

$$\begin{aligned} A_1 &\equiv h_1^0 (mod\ p^\nu), \ A_2 \equiv -kba^{-1}h_1^0 (mod\ p^{\nu+1}) \\ A_{-1} &\equiv ah_2^0 (mod\ p^\nu), \ A_{-2} \equiv h_2^0 a\ell b (mod\ p^{\nu+1}) \\ A_3 &\equiv A_{-3} \equiv 0 (mod\ p^{\nu+1}) \end{aligned} \tag{13}$$

We put $\omega = u + p^{n_1-1}z$, $u \in R_{n_1-1}^*$, $z \in R_1$.

Then we have

$$\begin{aligned} \omega^{-1} &\equiv u^{-1} - p^{n-1}u^{-2}z (mod\ p^n) \\ \omega^j &\equiv u^j + jp^{n-1}u^{j-1}z (mod\ p^n) \\ \omega^{-j} &\equiv u^{-j} - jp^{n-1}u^{-j-1}z (mod\ p^n) \end{aligned}$$

Therefore we can write

$$\left(h_1^0\omega_{2k} + h_2^0\omega_{2\ell+1}\right) \equiv \left(F\left(u, u^{-1}\right) + \right. \\ \left. + \left(h_1^0 - h_2^0 a u^{-2}\right) p^{n_1} z\right) (mod\ p^{n_1}) \tag{14}$$

Hence, from (10), (14) and Lemma 1 we get

$$|\sigma_{k,\ell}(h_1, h_2)| = p^{s+1} \left| \sum_{\substack{u \in R^*_{n_1-1} \\ h_1^0 u^2 \equiv h_2^0 a (mod\ p)}} e_{p^{n_1}}\left(F\left(u, u^{-1}\right)\right) \right| \leq \\ \leq 2p^{s+1} \left| \sum_{u \in R^*_{n_1-2}} e_{p^{n_1-2}}\left(F_1\left(u, u^{-1}\right)\right) \right|, \tag{15}$$

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 for $k \not\equiv \ell (mod\ 2)$.

Now, let k and ℓ be integers of identical parity. Then for $k := 2k$, $\ell := 2\ell$, we have modulo p^{n_1}

$$(h_1^0\omega_{2k} + h_2^0\omega_{2\ell}) \equiv B_0 + B_1\omega + B_2\omega^2 + B_3\omega^3 + \omega^4 B_4(\omega) := F(\omega), \tag{16}$$

where

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

moreover the coefficients of $B_4'(\omega)$(as a polynomial on ω) contain multipliers of type $h_1^0 k^j + h_2^0 \ell^j$, $i \geq 0$, and B_1', B_2', B_3' consist out of the summand of type $c \cdot \left(h_1 k^j + H_2 \ell^j\right)$, $c \in \mathbb{Z}$.

It will be observed that $h_1^0 k^j + h_2^0 \ell^j \equiv 0 (mod\ p^t)$, $j = 2, 3, \ldots$, if $\nu_p(h_1^0 + h_2^0) = \nu_p(h_1^0 k + h_2^0 \ell) = t$. (Indeed, we have $h_1^0 k^j + h_2^0 \ell^j = (h_1^0 k^{j-1} + h_2^0 \ell^{j-1})(k + \ell) - k\ell(h_1 k^{j-2} + h_2^0 \ell^{j-2})$, and then we apply an induction over j).

Now, as above we infer

$$\left(h_1^0\omega_{2k} + h_2^0\omega 2\ell\right) \equiv F(u) + p^{n_1-1} z (B_1 + 2B_2 u)(mod\ p^{n_1})$$

Hence, by Lemma 1 and Lemma 3 we obtain easily

$$|\sigma_{k\ell}(h_1, h_2)| \leq \begin{cases} 0, & if\ t \neq \kappa + \nu,\ \min(t, \kappa + \nu) < n - s - \nu, \\ 2p^{\frac{n+\nu+s+t}{2}}, & if\ t = \kappa + \nu\ and\ n - \nu - s - t > 0, \\ p^{n-1}(p-1), & if\ \min(t, \kappa + \nu) \geq n - s - \nu. \end{cases}$$

For $k \equiv \ell \equiv 1 (mod\ 2)$ we have the analogous estimates.

□

Theorem 2. *Let* $h_1, h_2, h_3 \in \mathbb{Z}$, $(h_1, h_2, h_3, p^n) = p^d, d \le n$, $h_i = h_i^0 p^d$, $i = 1,2,3$, $(h_1^0, h_2^0, h_3^0, p) = 1$, *and let* $(h_1 + h_2 + h_3, p^n) = p^t$, $t \ge d$, $(h_1^0 k + h_2^0 \ell + h_3^0 m, p^{n-d}) = p^\kappa$. *Then we have*

$$|\sigma_{k,\ell,m}(h_1, h_2, h_3)| \le$$

$$\le \begin{cases} 0, & \text{if } t \ne \kappa + \nu \\ & \text{and } \min(t, \kappa+\nu) < n - d - \nu, \\ 2p^{\frac{n+\nu+d+t}{2}}, & \text{if } t = \kappa + \nu \\ & \text{and } n - \nu - d - t > 0, \\ p^{n-1}(p-1), & \text{if } \min(t, \kappa+\nu) \ge n - s - \nu. \end{cases} \tag{17}$$

if in the middle of k, ℓ, m *are numbers of opposite parity.*

Proof. The estimate of the sum $\sigma_{k,\ell,m}(h_1, h_2, h_3)$ can be obtain by similar arguments which we used for the case $\sigma_{k,\ell}(h_1, h_2)$ when k and ℓ are of opposite parity.

□

Let h be integer, $(h, p^n) = p^s$, $0 \le s < n$, and let τ be a least period length of the sequence $\{\omega_k\}$, $k = 0, 1, 2, \ldots$, defined in (5). For $1 \le N \le \tau$ we denote

$$S_N(h, \omega) = \sum_{k=0}^{N-1} e_{p^n}(h\omega_k). \tag{18}$$

We shall obtain the bound for $S_N(h, \omega)$.

Theorem 3. *Let the inversive congruential sequence* $\{\omega_k\}$ *has the maximal period* τ, $\tau = 2p^{n-\nu}$ *and let* $2\nu < \mu$. *Then the following bound*

$$|S_\tau(h, \omega)| = \left|\sum_{k=0}^{\tau-1} e_{p^n}(h\omega_k)\right| \le \begin{cases} 0 & \text{if } \nu + s < n \\ \tau & \text{if } \nu + s \ge n, \end{cases} \tag{19}$$

holds.

Proof. By Cosequence 3 from Lemma 4 we conclude that $(a - \omega^2, p) = (1 - a\omega^{-2}, p) = 1$. By Cosequence 1 from Lemma 4 we obtain

$$\begin{aligned} |S_\tau(h, \omega)| &= \left|\sum_{\substack{k_1=0 \\ k=2k_1}}^{p^{n-\nu}-1} e_{p^n}(h\omega_k) + \sum_{\substack{k_1=0 \\ k=2k_1+1}}^{p^{n-\nu}-1} e_{p^n}(h\omega_k)\right| \le \\ &\le \left|\sum_{k_1=0}^{p^{n-\nu}-1} e_{p^n}(hF(k_1))\right| + \left|\sum_{k_1=0}^{p^{n-\nu}-1} e_{p^n}(hG(k_1))\right| \end{aligned} \tag{20}$$

where

$$\begin{cases} \omega_{2k} = \omega + A_1(\omega)k + A_2(\omega)k^2 + A_3(\omega,k)k^3 := F(k), \\ \omega_{2k+1} = (a\omega^{-1} + b + c\omega) + B_1(\omega)k + B_2(\omega)k^2 + B_3(\omega,k)k^3 := G(k), \end{cases} \tag{21}$$

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

We recall that $(a,p) = 1$, $b = b_0p^\nu$, $c = c_0p^\mu$, $h = h_0p^s$, $(b_0,p) = (c_0,p) = (h_0,p) = 1$, $\gamma = \min(3\nu, \nu + \mu)$.
Now Lemma 1 gives

$$|S_\tau(h,\omega)| = 2p^s \begin{cases} 0, & if\ \nu + s < n \\ p^{n-\nu-s}, & if\ \nu + s \geq n \end{cases} = \begin{cases} 0, & if\ \nu + s < n \\ \tau, & if\ \nu + s \geq n. \end{cases}$$

□

Theorem 4. *Let $\{\omega_k\}$ be the sequence generated by the recurrent formula (5) 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*

$$|S_\tau(h,\omega)| \leq \begin{cases} 0, & if\ 0 < \nu_p(a-\omega^2) < \nu \\ & and\ \nu_p(a-\omega^2) < n - \nu - s, \\ \tau, & if\ 0 < \nu_p(a-\omega^2) < \nu \\ & and\ \nu_p(a-\omega^2) \geq n - \nu - s, \\ 4p^{\frac{n+s+2\nu}{2}}, & if\ \nu_p(a-\omega^2) \geq \nu\ and\ 2\nu + s < n, \\ \tau, & if\ \nu_p(a-\omega^2) \geq \nu\ and\ 2\nu + s \geq n, \end{cases} \tag{22}$$

holds.

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

□

Cosequence 4. *Let $\{\omega_k\}$ be the sequence generator by recurrent formula (5) with a least period length τ and let $0 \leq \nu_p(a - \omega^2) < \nu$, $2\nu < \mu$, $\nu_p(h) = s$. Then for $0 < N \leq \tau$ we have*

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

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

$$\begin{aligned} |S_N(h,\omega)| &= \left|\sum_{\ell=0}^{N-1}\frac{1}{\tau}\sum_{k=0}^{\tau-1}\sum_{x=0}^{\tau-1} e_{p^n}(h\omega_k)e_\tau(x(k-\ell))\right| \leq \\ &\leq \frac{N}{\tau}\left|\sum_{k=0}^{\tau-1} e_{p^n}(h\omega_k)\right| + \sum_{x=1}^{\tau-1}\frac{1}{\min(x,\tau-x)}\left|\sum_{k=0}^{\tau-1} e^{2\pi i\left(\frac{h\omega_k}{p^n}+\frac{kx}{\tau}\right)}\right| \leq \\ &\leq \frac{N}{\tau}|S_N(h,\omega)| + \sum_{x=1}^{\tau-1}\frac{1}{\min(x,\tau-x)}\left|\sum_{j=0}^{1}\sum_{k=0}^{\frac{\tau}{2}-1} e^{2\pi i\frac{\Phi_j(k)}{p^{n-\nu}}}\right|, \end{aligned} \tag{23}$$

where

$$\begin{aligned} &\Phi_j(k) = A_1^{(j)}k + A_2^{(j)}k^2 + \cdots,\ j=0,1;\ h = h_0p^s,\ (h_0,p)=1; \\ &A_1^{(0)}(x) \equiv hb_0(1-a^{-1}\omega^2) + x\,(mod\ p^{\nu+s}), \\ &A_1^{(1)}(x) \equiv hb_0(1-a\omega^{-2}) + x\,(mod\ p^{\nu+s}), \\ &A_2^{(j)} \equiv (-1)^{j+1}h_0a^{-2}b_0^2\omega^3p^{\nu+s}\,(mod\ p^{2\nu+s}),\ j=0,1; \\ &A_i^j \equiv 0\,(mod\ p^{2\nu+s}),\ i=3,4,\dots;\ j=0,1. \end{aligned} \tag{24}$$

From (24) and Lemma 3 we conclude that the sums

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

allow nontrivial estimate only in the case when

$$A_1^{(0)}(x) \equiv 0\,(p^\nu)\ or\ A_1^{(1)}(x) \equiv 0\,(mod\ p^\nu) \tag{25}$$

It may occur only if $x \equiv 0\,(mod\ p^s)$.
Therefore, from (23)-(25), Lemma 3 and Theorems 1-2 we derive

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

This complete the proof of Cosequence

□

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 5. *Let a,b,c be parameters of the inversive congruential sequence (5) 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 $\omega \in R_n^*$ satisfies

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

Proof. By the Cauchy-Schwarz inequality we obtain

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

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

$$
\begin{aligned}
|\overline{S}_N|^2 &\leq \frac{1}{\phi(p^n)} \left(\sum_{t=0}^{n-\nu-s-1} p^{\frac{n+\nu+s+t}{2}} \sum_{\substack{k,\ell \leq N \\ k \equiv \ell (mod\ p^t)}} 1 + \sum_{t=n-\nu-s}^{n} p^n \sum_{\substack{k,\ell \leq N \\ k \equiv \ell (mod\ p^t)}} 1 \right) \leq \\
&\leq \frac{N^2}{\phi(p^n)} \left(\sum_{t=n-\nu-s-1} p^{\frac{n+\nu+s-t}{2}} + \sum_{t=n-\nu-s}^{n} p^{n-t} \right) \leq \\
&\leq 4\frac{N^2}{p^n} \left(p^{\frac{n+s+\nu}{2}} + p^{\nu+s} \right).
\end{aligned}
$$

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

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

□

Now we shall apply the obtained estimates to study of uniformity and independence of the sequence $\{x_k\}$, $k = 0,1,2,\ldots$ which are generated by recursion (5).

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

$$
D(\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{N-1}) = \sup_I \left| \frac{A_N(I)}{N} - |I| \right|, \tag{26}
$$

where the supremum is extended over all subintervals I of $[0,1)^s$, $A_N(I)$ 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.

The little value of a discrepancy means that the sequence x_k is uniformly distributed random sequence. The second fundamental statistical property of pseudorandom numbers $\{x_k\}$ is independence. In order this fact determine we derive a sequence $x_0, x_1, x_2, \ldots$ of points in $[0,1]^s$, $(s = 1,2,3,\ldots)$ by putting

$$
X_n := (x_n, \ldots, x_{n+s-1}) \ \ (''overlapping\ s-tuples'')
$$

or

$$X_n := (x_{ns}, x_{ns+1} \dots, x_{ns+s-1}) \ (''nonoverlapping\ s-tuples'')$$

There is no strict rule of how to construct those s-tuples. If the pseudorandom numbers $x_0, x_1, x_2, \dots$ are independent from each other, then the points $X_1, X_2, X_3, \dots$ should be approximately uniformly distributed in $[0,1]^s$.

For study the discrepancy of points usually use the following lemmas. For integers $q \geq 2$ and $s \geq 1$, let $C_s(d)$ denote the set of all nonzero lattice points $(h_1, \dots, h_s) \in \mathbb{Z}^s$ with $-\frac{q}{2} < h_j \leq \frac{q}{2}$, $1 \leq j \leq s$. We define

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

and

$$r(\mathfrak{h}, q) = \prod_{j=1}^{s} r(h_j, q) \quad for\ \mathfrak{h} = (h_1, \dots, h_q) \in C_s(q).$$

Lemma 5. *Let $N \geq 1$ and $q \geq 2$ be integers. For N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1} \in [0,1)^s$, the discrepancy $D(\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1})$ satisfies*

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

(Proof see in [17]).

Lemma 6. *Let $\{\mathfrak{y}_k\}$, $\mathfrak{y}_k \in \{0, 1, \dots, q-1\}^s$, is a purely periodic sequence with a period τ. Then for the discrepancy of the points $\mathfrak{t}_k = \frac{\mathfrak{y}_k}{q} \in [0,1)^s$, $k = 0, 1, \dots, N-1$; $N \leq \tau$, the following estimate*

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

holds,
where

$$\mathfrak{S} := \sum_{k=0}^{\tau-1} e(\mathfrak{h} \cdot \mathfrak{t}_k + \frac{k h_0}{\tau}).$$

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

Lemma 7. *The discrepancy of N arbitrary points $\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{N-1} \in [0,1)^s$ satisfies*

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

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

(Proof see[16], Lemma 1).

Lemma 8. *Let $q \geq 2$ be an integer. Then*

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

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

Theorem 6. *Let $p > 2$ be a prime and n, a, b, c and ω be integers, $n \geq 3$, $(a, p) = (\omega, p) = 1$, $0 < \nu_p(b) < \nu_p(c)$, $a \not\equiv \omega^2 (mod\ p)$. Then for the sequence $\{x_k\}$, $x_k = \frac{\omega_k}{p^n}$, $k = 0, 1, \ldots$, where ω_k defined by the recursion (5), we have*

$$D_N(x_0, x_1, \ldots, x_{N-1}) \leq \frac{1}{p^n} + \frac{2p^{\frac{n-\nu}{2}}}{N} \left(\frac{1}{p} \left(\frac{2}{\pi} \log p^n + \frac{7}{5} \right)^2 + 1 \right), \qquad (27)$$

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

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

$$D_N \leq \frac{1}{p^{n-\nu}} + \frac{1}{N} \sum_{0 < |h| < \frac{1}{2}p^{n-\nu}} \sum_{|h_0| \leq \frac{1}{2}\tau} \left(r\left(h, \frac{1}{2}p^{n-\nu}\right) r(h_0, \tau) \right)^{-1} \times$$
$$\times \left| \sum_{k=0}^{\tau-1} e^{2\pi i \left(\frac{h x_k}{p^n} + \frac{k h_0}{\tau} \right)} \right| \leq$$
$$\leq \frac{1}{p^{n-\nu}} + \frac{1}{N} \sum_{h, h_0} \left(r\left(h, \frac{1}{2}p^{n-\nu}\right) r(h_0, \tau) \right)^{-1} \times$$
$$\times \left(\left| \sum_{k=0}^{p^{n-\nu}-1} e^{2\pi i \left(\frac{h\omega_{2k}}{p^n} + \frac{k h_0}{p^{n-\nu}} \right)} \right| + \left| \sum_{k=0}^{p^{n-\nu}-1} e^{2\pi i \left(\frac{h\omega_{2k+1}}{p^n} + \frac{k h_0}{p^{n-\nu}} \right)} \right| \right)$$

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

$$D_N(x_0, x_1, \ldots, x_{N-1}) \leq \frac{1}{p^{n-\nu}} + \frac{2p^{\frac{n-\nu}{2}}}{N} \left(\frac{1}{p} \left(\frac{2}{\pi} \log p^n + \frac{7}{5} \right)^2 + 1 \right) \qquad (28)$$

□

Consider the inversive congruential sequence $\{\omega_k\}$ with the conditions of Theorem 5 and organize the new sequence $\{\mathfrak{y}_k\}$, where $\mathfrak{y}_k \in \mathbb{Z}^s$, $d \in \mathbb{N}$, $\mathfrak{y}_k = (\omega_k, \omega_{k+1}, \ldots, \omega_{s-1})$. The statistical independence properties of the sequence are analyzed by means of the s-dimensional serial tests($s = 2, 3, \ldots$) which employ the discrepancy of s-dimensional vectors $\mathfrak{t}_k$, where $\mathfrak{t}_k = \frac{\mathfrak{y}_k}{p^n}$, $k = 0, 1, \ldots$. We shall consider only the cases $s = 2$ or 3. Let $D_\tau^{(s)}$ denote the discrepancy of points $\mathfrak{t}_0, \mathfrak{t}_1, \ldots, \mathfrak{t}_{\tau-1}$.

Theorem 7. *The discrepancy $D_\tau^{(s)}$, $s=2,3$ of the points constructed by inversive congruential sequence (5) with the least period length $\tau = 2p^{n-\nu}$, satisfies*

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

Proof. Consider only the case $s=2$. In order to apply Lemma 5 we must have an estimate for the sum

$$\sum_{k=0}^{\tau-1} e_{p^n}(h_1\omega_k + h_2\omega_{k+1}) = \sum_{k=0}^{p^{n-\nu}-1} e_{p^n}(h_1\omega_{2k} + h_2\omega_{2k+1}) + \\ + \sum_{k=0}^{p^{n-\nu}-1} e_{p^n}(h_1\omega_{2k+1} + h_2\omega_{2k+2}) = \sum_1 + \sum_2,$$

say.
By Cosequence 2 of Lemma 4 we get

$$\begin{aligned} h_1\omega_{2k} + h_2\omega_{2k+1} \equiv & \big(h_1\omega + h_2(b + c\omega + a\omega^{-1})\big) + \\ & + k(h_1(b(1-a^{-1}\omega^2) + ac\omega^{-1}) + \\ & + h_2(b(1-a\omega^{-2}) + c\omega^{-1}(2\omega^2 - a^2))) + \\ & + k^2(h_1(a^{-2}b^2\omega^3 + a^{-1}c\omega(1-\omega^2) - a^{-1}b^2\omega) + \\ & + h_2(-a^{-1}c - \omega^{-1}c + b^2(1-a^{-1}\omega^2)))\,(mod\ p^{\delta+\ell}) \end{aligned}$$

where $\delta = \min(3\nu, \mu)$, $\ell = \nu_p((h_1, h_2, p^n))$.
Since the congruences

$$\begin{aligned} & h_1(b(1-a^{-1}\omega^2) + ac\omega^{-1}) + \\ & + h_2(b(1-a\omega^{-2}) + c\omega^{-1}(2\omega^2 - a^2)) \equiv 0\,(mod\ p^{\ell+\nu+1}) \end{aligned}$$

$$\begin{aligned} & h_1(a^{-2}b^2\omega^3 + a^{-1}c\omega(1-\omega^2) - a^{-1}b^2\omega) + \\ & + h_2(-a^{-1}c - \omega^{-1}c + b^2(1-a^{-1}\omega^2)) \equiv 0\,(mod\ p^{\ell+\nu+1}) \end{aligned}$$

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

$$|\sum_1| = \begin{cases} p^{\frac{n-\ell}{2}} & if\ \nu_p(h_1) = \nu_p(h_2) = \ell,\ h_1 - a\omega^{-2}h_2 \equiv 0(mod\ p^\nu), \\ 0 & else \end{cases}$$

Similarly, we have

$$|\sum_2| = \begin{cases} p^{\frac{n-\ell}{2}} & if\ \nu_p(h_1) = \nu_p(h_2) = \ell,\ h_1 - a\omega^{-2}h_2 \equiv 0\,(mod\ p^\nu), \\ 0 & else \end{cases}$$

Now, Lemmas 5 and 8 give for $q = 2p^{n-\nu}$

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

The case $s = 3$ can be consider similarly.

□

In conclusion we prove the lower bound for $D_\tau^{(s)}$, $s = 2, 3, 4$.

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

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

where $h_* = |h_1 \cdots h_s|$ under condition $h_1, \ldots, h_s \in C_1(p^n)$, $h_1 \cdots h_s \ne 0$, $(h_1, \ldots, h_s) = 1$, $h_1 + h_2 \equiv h_* a \omega^{-2} (mod\ p^\nu)$.

Proof. By the Lemma 7 for $d = 2$, $N = 2p^{n-\nu}$, we have

$$D_\tau^{(s)} \ge \frac{1}{4(\pi+2)p^{n-\nu}} \left| \sum_{k=0}^{p^{n-\nu}-1} e_{p^n}(h_1\omega_k + h_2\omega_{k+1} + \ldots + h_s\omega_{k+s-1}) \right| =$$
$$= \frac{1}{4(\pi+2)p^{n-\nu}} \left| \sum_{k=0}^{p^{n-\nu}-1} e_{p^n}(h_1\omega_{2k} + \ldots + h_s\omega_{2k+s-1}) + \right. \tag{29}$$
$$\left. + \sum_{k=0}^{p^{n-\nu}-1} e_{p^n}(h_1\omega_{2k+1} + \ldots + h_s\omega_{2k+s}) \right| = \frac{1}{4(\pi+2)p^{n-\nu}} \left| \sum\nolimits_1 + \sum\nolimits_2 \right|,$$

say.
Let $(h_1, \ldots, h_s, p^n) = p^\ell$, $h_i = h_i^0 p^\ell$, $i = 1, \ldots, s$, $(h_1^0, \ldots, h_s^0, p) = 1$.
As above we can see easily that the congruences for $s = 4$

$$(h_1^0 + h_3^0)(1 - a\omega^{-2}) + (h_2^0 + h_4^0)(1 - a^{-1}\omega^2) \equiv 0 (mod\ p^\nu)$$
$$(h_1^0 + h_3^0)(1 - a^{-1}\omega^2) + (h_2^0 + h_4^0)(1 - a\omega^{-2}) \equiv 0 (mod\ p^\nu)$$

cannot be satisfied simultaneously if $a \not\equiv \omega^2 (mod\ p)$, $a \not\equiv -\omega^2 (mod\ p^\nu)$.
For $s = 2, 3$ in the previous congruences it is necessary to exclude summands h_3, h_4 (for $s = 2$) or h_4 (if $s = 3$).

We select h_1, h_2, h_3, h_4 so that $(h_1, h_2, h_3, h_4, p^n) = 1$, $h_1 + h_3 - (h_2 + h_4)a\omega^{-2} \equiv$ $\equiv 0 (mod\ p^\nu)$, $(h_1 + h_3, p) = 1$ for the case $s = 4$. A similar assortment of conditions we can make for the cases $s = 2, 3$. Then Lemma 2 gives

$$\left| \sum\nolimits_1 \right| = p^{\frac{n+\nu}{2}}, \quad \left| \sum\nolimits_2 \right| = 0. \tag{30}$$

Hence, from (29)–(30) we infer

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

where $h_* = \min\limits_{\substack{h_1,\dots,h_s \in C_1(p^n) \\ h_1\cdots h_s \neq 0 \\ (h_1,\dots,h_s)=1 \\ h_1+h_3 \equiv (h_2+h_4)a\omega^{-2} (mod\ p^{\nu})}} |h_1 \cdots h_s|.$

□

Conclusion. Theorems 6 and 7 show that, in general, the upper bound is the best possible up to the logarithmic factor for any inversive congruential sequence $\{(x_k,\dots,x_{k+s-1})\}$, $k=0,1,\dots$, $s=2,3$(defined by the recursion (5)), since there exist inversive congruential sequence $\{(x_k,x_{k+1})\}$ with $D_{\tau}^{(2)} \geq \frac{1}{8(\pi+2)} p^{-\frac{n}{2}+\nu}$. (Example, if $a\omega^{-2} \equiv 2(mod\ p^{\nu})$, $h_1=h_2=1$).
Hence, on the average discrepancy $D_{\tau}^{(2)}$ has an order of magnitude between $p^{-\left(\frac{n}{2}-\nu\right)}$ and $p^{-\left(\frac{n}{2}-\nu\right)} \log^2 p^n$. An analogous statement can be prove 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

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

From the proof of the Theorem 7 it can be see that lower bound for $D_{\tau}^{(s)}$ can be prove for any $s \geq 2$. Unfortunately, the upper bound for $D_{\tau}^{(s)}$ it is a very difficult to obtain.

1. **Chou W.-S.** The period lengths of inversive congruential recursions [text] / Chou W.-S. // Acta Arith. – 1995. – V. 73, 4. – P. 325–341.
2. **Eichenauer-Herrmann J.** Inversive congruential pseudorandom numbers: a tutorial [text] / Eichenauer-Herrmann J. // Internat. Statist. Rev. – 1992. – V. 60. – P. 167–176.
3. **Eichenauer-Herrmann J.** Construction of inversive congruential pseudorandom number generators with maximal period length [text] / Eichenauer-Herrmann J. // J. Comput. Appl. Math. – 1992. – V. 40. – P. 345-–349.
4. **Eichenauer-Herrmann J.** Statistical independence of a new class of inversive congruential pseudorandom numbers [text] / Eichenauer-Herrmann J. // Math. Comp. – 1993. – V. 60. – P. 375–384.
5. **Eichenauer-Herrmann J.** Compound nonlinear congruential pseudorandom numbers [text] / Eichenauer-Herrmann J. // Monatsh. Math. – 1994. – V. 117. – P. 213–222.
6. **Eichenauer-Herrmann J.** Pseudorandom number generation by nonlinear methods [text] / Eichenauer-Herrmann J. // Internat. Statist. Rev. – 1995. – V. 63. – P. 247–255.
7. **Eichenauer J.** A non-linear congruential pseudorandom number generator [text] / Eichenauer J., Lehn J. // Statist. Hefte. – 1986. – V. 27. – P. 315–326.

8. **Eichenauer J.** A nonlinear congruential pseudorandom number generator with power of two modulus [text] / Eichenauer J., Lehn J., Topuzoğlu A. // Math. Comp. – 1988. – V. 51. – P. 757–759.

9. **Eichenauer-Herrmann J.** A survey of quadratic and inversive congruential pseudorandom numbers [text] / Eichenauer-Herrmann J., Herrmann E., Wegenkittl S. // B.: Monte Carlo and Quasi-Monte Carlo Methods, 1996, H. Niederreiter et al(eds.), Lecture Notes in Statist. 127, Springer, New York. – 1998. – P. 66–97.

10. **Eichenauer-Herrmann J.** On the period of congruential pseudorandom number sequences generated by inversions [text] / Eichenauer-Herrmann J., Topuzoğlu A. // J. Comput. Appl. Math. – 1990. – V. 31. – P. 87–96.

11. **Kato T.** On a nonlinear congruential pseudorandom number generator [text] / Kato T., Wu L.-M., Yanagihara N. // Math. of Comp. – 1996. – V. 65, 213. – P. 227–233.

12. **L'Ecuyer P.** Uniform random number generation [text] / L'Ecuyer, P. // Ann. Oper. Res. – 1994. – V. 53. – P. 77-–120.

13. **Niederreiter H.** Pseudo-random numbers and optimal coefficients [text] / Niederreiter H. // Adv. Math. – 1977. – V. 26. – P. 99—181.

14. **Niederreiter H.** Lower bounds for the discrepancy of inversive congruential pseudorandom numbers [text] / Niederreiter H. // Math. Comp. – 1990. – V. 55. – P. 277–287.

15. **Niederreiter H.** Finite fields and their applications [text] / Niederreiter H. // B.: Contributions to General Algebra, Vol. 7, Vienna,(1990), Teubner, Stuttgart. – 1991. – V. 7. – P. 144.

16. **Niederreiter H.** Recent trends in random number and random vector generation [text] / Niederreiter H. // Ann. Oper. Res. – 1991. – V. 31. – P. 323–345.

17. **Niederreiter H.** Nonlinear methods for pseudorandom number and vector generation [text] / Niederreiter H. // Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems, vol. 374, Springer, Berlin. – 1992. – V. 374. – P. 145–153.

18. **Niederreiter H.** Random Number Generation and Quasi-Monte Carlo Methods [text] / Niederreiter H. // B.: SIAM, Philadelphia,Pa. – 1992. – P. 82.

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

20. **Niederreiter H.** New developments in uniform pseudorandom number and vector generation [text] / Niederreiter H. // B.: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, H. Niederreiter and P.J.-S. Shine(eds), Lecture Notes in Statist. 106, Springer, New York. – 1995. – V. 106. – P. 87–120.

21. **Niederreiter H.** Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus [text] / Niederreiter H., Shparlinski I. // Acta Arith. – 2000. – V. 90, 1. – P. 89–98.

22. **Varbanets S.** Exponential sums on the sequences of inversive congruential pseudorandom numbers [text] / Varbanets S. // Šiauliai Math. Semin. 2008. – V. 3, 11. – P. 247–261.

23. **Varbanets S.** On inversive congruential generator for pseudorandom numbers with prime power modulus [text] / Varbanets S. // Annales Univ. Sci. Budapest, Sect. Comp. – 2008. – V. 29. – P. 277–296.

24. **Varbanets P.** Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus [text] / Varbanets P., Sergey Varbanets // VoronoÏ's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine, September 22–28. – 2008. – V. 4, 1. – P. 112–130.

25. **Varbanets P.** On inversive congruential generator with a variable shift for pseudorandom numbers with prime power modulus [text] / Varbanets P., Varbanets S. // Annales Univ. Sci. Budapest, Sect. Comp.(to appear).