LINEAR INVERSIVE SEQUENCE OF PSEUDORANDOM NUMBERS

Rudetsky V.

I.I. Mechnikov Odessa National University, Ukraine

1. Literature review. The sequences of pseudorandom numbers are widely used in the applied tasks of statistics and modern cryptography. Last decade large attention is spared to the construction of sequences of pseudorandom numbers. Two types of generators of pseudorandom numbers are usually used: linear congruent generator and nonlinear congruent generators. Linear generators have comparatively a small period and does not possess property of unpredictable, therefore they are not used in the tasks of cryptography. On changing linear congruential generators came nonlinear generators. Their cryptographic properties and research of inverse congruent generator can be found in, see, [5]. Eichenauer and Lehn [2], and later Niederreiter studied recursive sequence generated by the recursive relation

$$x_{N+1} = \begin{cases} ax_N^{-1} + b, & \text{if } x_N \neq 0 \\ b, & \text{if } x_N = 0 \end{cases},$$

with some coefficients $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, where $\mathbb{F}_q$ is the field of q elements, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Some results on the period and distribution of this sequence can be found in work Niederreiter [5], see also [1].

Niederreiter and Shparlinski [4] investigated the problem of distribution of inverse congruential pseudorandom numbers with prime power modules p^n, $p > 2$.

$$y_{n+1} = ay_n^{-1} + b(\mathrm{mod}\, p^n), (y_0, p) = 1, n = 0,1,2,...$$

They obtained the nontrivial discrepancy bound for the appropriate normalized sequence of pseudorandom numbers $\left\{\frac{x_k}{p^n}\right\}, k = 0,1,2,...$, for parts of the period of this sequence. W.-S. Chou [1] gave a detailed study of the possible values of periods τ.

T. Kato, L.-M. Wu and N. Yanagihara studied [3] a nonlinear congruent pseudorandom number generator with modulus $M = 2^n$ of the form

$$y_{n+1} = ay_n^{-1} + b + cy_n (\mathrm{mod}\, M), (y_n, 2) = 1, n = 0,1,2,...$$

For it, they obtained a condition to generate sequences of maximal period length.

S. Varbanets [7] gave a detailed study of properties linear inversive congruential generator of the form

$$w_{k+1} = aw_k^{-1} + b + cw_k (\mathrm{mod}\, p^n),\ (w_0, p) = 1,\ k = 1,2,3,...,$$

with $a,b,c \in \mathbb{Z}$, $(a,p)=1$, $b \equiv c \equiv 0 (\mathrm{mod}\, p)$, $bc \equiv 0 (\mathrm{mod}\, p^n)$.

In the present paper, we investigate the distribution of inverse congruent pseudorandom numbers which are generated by the recurrent formula

$$w_{k+1} = aw_k^{-1} + b + cw_k (\mathrm{mod}\, p^n), \quad (w_0, p) = 1, \quad k = 1,2,3,... \qquad (1)$$

with $a,b,c \in \mathbb{Z}$ $a \equiv b \equiv 0 (\mathrm{mod}\, p)$, $(c,p)=1$, $ab \equiv 0 (\mathrm{mod}\, p^n)$.

As we will see in future, the examined generator has substantial differences from a previous generator.

Notations. The letter p denotes a prime number, $p \geq 3$. For $n \in \mathbb{N}$, the notation R_n denotes the complete (accordingly, reduced) residue system modulo p^n. The implied constants in symbols «O» and «<<» may in obvious cases depend on a small positive parameter ε. For each u $(u,p)=1$ we define u^{-1} as $u^{-1}u \equiv 1 (\mathrm{mod}\, p^n)$. For any $t \in \mathbb{R}$ and $q \in \mathbb{N}$, we write $\exp(t) = e^t$, $e(t) = e^{2\pi i t}$, $e_q(t) = e(t/q)$.

2. Preliminaries. Let $a,b,c \in \mathbb{Z}$, $p \geq 3$ be a prime, and $n > 1, n \in \mathbb{N}$. We consider the transformation φ, defined on $R_n^* := \{a \in R_n \mid (a,p)=1\}$ by $\varphi(w) = aw^{-1} + b + cw$.

It is clear that φ is a permutation on R_n^*, if $(c,p)=1$ и $a \equiv b \equiv 0 (\mathrm{mod}\, p)$. So, the sequence w_k is purely periodic with the period $\tau \leq p^{n-1}(p-1)$, where $w_k = \varphi(w_{k-1})$, $k = 1,2,..., w_0 = w$.

In this paper, we always assume that $ab \equiv 0 (\mathrm{mod}\, p^n)$. For the case $c \equiv 0 (\mathrm{mod}\, p^n)$, Chou [1] studied completely the dependence of period on the parameters a,b,w. We also investigate this problem for our case.

Now we state some lemmas necessary for the proof of theorems.

Lemma 1. *Let* $f(x) = Bx + Cx^2 + p(Dx^3 + ...)$ *be a polynomial over* $\mathbb{Z}$, $(C,p)=1$. *Then, for any* $A \in \mathbb{Z}$ *we have*

$$T := \left| \sum_{w \in R_n^*} e_{p^n}(Aw + f(w^{-1})) \right| \leq 2p^{\frac{n}{2}}.$$

Proof. The proof of this assertion has in [7].

We put $w^{-1} = u + p^{n-1}z$, $u \in R_{n-1}^*, z \in R_1$. Thus, we have $w = u^{-1} - p^{n-1}zu^{-2}$, $w^{-j} = u^j + jp^{n-1}zu^{j-1} (\mathrm{mod}\, p^n)$.

Below we will consider some special cases of the entered generator at first.

Lemma 2. *Let* $a^2 \equiv 0 \pmod{p^n}$. *Then, for* $k = 1,2,3,...$ *we will get next presentation of elements to the sequence*

$$w_k = c^k w + b\frac{c^0 - c^k}{1-c} + aw^{-1}\frac{c^{-k+1} - c^{k+1}}{1-c^2} \pmod{p^n}.$$

Proof. From the definition of the transformation φ we obtain that

$$w_0 = w\ ,\ w_1 = cw + b + aw^{-1},\ w_2 = \frac{a}{aw^{-1} + b + cw} + b + c(aw^{-1} + b + cw) =$$

$$= \frac{a}{cw(1 + bc^{-1}w^{-1} + ac^{-1}w^{-2})} + b + acw^{-1} + cb + c^2 w =$$

$$= ac^{-1}w^{-1}(1 - (bc^{-1}w^{-1} + ac^{-1}w^{-2}) + (bc^{-1}w^{-1} + ac^{-1}w^{-2})^2 - ...) =$$

$$= (ac^{-1}w^{-1} - abc^{-2}w^{-2} - a^2c^{-2}w^{-3} + ...) + b + acw^{-1} + cb + c^2 w =$$

$$= c^2 w + (1+c)b + a(c^{-1} + c^1)w^{-1},$$

$$w_3 = \frac{a}{c^2 w + (1+c)b + a(c^{-1} + c^1)w^{-1}} + b + c(c^2 w + (1+c)b + a(c^{-1} + c^1)w^{-1}) =$$

$$= c^3 w + (1 + c + c^2)b + a(c^{-2} + c^0 + c^2)w^{-1},$$

$$w_4 = \frac{a}{c^3 w + (1 + c + c^2)b + a(c^{-2} + c^0 + c^2)w^{-1}} + b + c(c^3 w + (1 + c + c^2)b +$$

$$+ a(c^{-2} + c^0 + c^2)w^{-1}) = c^4 w + (1 + c + c^2 + c^3)b + a(c^{-3} + c^{-1} + c^1 + c^3)w^{-1}.$$

We will suppose that

$$w_{k-1} = c^{k-1}w + b(1 + c + ... + c^{k-2}) + aw^{-1}(c^{-k+2} + c^{-k+4} + ... + c^{k-4} + c^{k-2}) =$$

$$= c^{k-1}w + b\frac{c^0 - c^{k-1}}{1-c} + aw^{-1}\frac{c^{-k+2} - c^k}{1-c^2}$$

Then, it is possible to write a general formula for k member of sequence

$$w_k = c(aw^{-1}\frac{c^{-k+2} - c^k}{1-c^2} + b\frac{1-c^{k-1}}{1-c} + cw^{k-1}) + b +$$

$$+ \frac{a}{aw^{-1}\frac{c^{-k+2} - c^k}{1-c^2} + b\frac{1-c^{k-1}}{1-c} + cw^{k-1}} =$$

$$= c^k w + b\frac{c^0 - c^k}{1-c} + aw^{-1}\frac{c^{-k+1} - c^{k+1}}{1-c^2}$$

Lemma 2 is proved.

Lemma 3. *Let* $a^3 \equiv 0 \pmod{p^n}$. *Then, for* $k = 1,2,3,...$ *we will get next presentation of elements to the sequence*

$$w_k = c^k w + b\frac{c^0 - c^k}{1-c} + aw^{-1}\frac{c^{-k+1} - c^{k+1}}{1-c^2} - a^2 w^{-3}F(c).$$

with $F(c)$ *some polynomial, depends on* c.

Proof. Using the same algorithm as in Lemma 2, we will get

$w_0 = w$, $w_1 = cw + b + aw^{-1}$,

$w_2 = c^2 w + b(1+c) + aw^{-1}(c^{-1} + c^{+1}) - a^2 c^{-2} w^{-3}$,

$w_3 = c^3 w + b(1+c+c^2) + aw^{-1}(c^{-2} + c^0 + c^{+2}) - a^2 w^{-3}(c^{-1} + c^{-3} + c^{-5})$.

Then, by recursion, we can get the next presentation of $\{w_k\}$ elements

$$w_k = c^k w + b\frac{c^0 - c^k}{1-c} + aw^{-1}\frac{c^{-k+1} - c^{k+1}}{1-c^2} - a^2 w^{-3} F(c),$$

with $F(c)$ some polynomial, depends on c. Lemma 3 is proved.

Lemma 4. For $l > 3$ *we can consider the general case:*
Let $a^l \equiv 0 (\mathrm{mod}\, p^n)$:

$$w_k = c^k w + b\frac{c^0 - c^k}{1-c} + aw^{-1}\frac{c^{-k+1} - c^{k+1}}{1-c^2} + a^2 w^{-3} F_k(a,c,w)) \quad (2)$$

with $F_k(a,c,w)$ *is a polynomial on* a,c,w.

Let w_k, w_l to be elements of the sequence $\{w_k\}$, generated by (1). We will define

$$\sigma_{k,l}(h,p^n) = \sigma_{k,l} := \sum_{w \in R_n^*} e_{p^n}(h(w_k - w_l)).$$

Lemma 5. *Let* k *and* l *non negative integers and* $(h,p^n) = p^\delta, \delta < n$. *Then*

$$\left|\sigma_{k,l}\right| << \begin{cases} p^{\frac{n+1}{2}}, & \text{if}\,(h(c^k - c^l) \equiv 0 (\mathrm{mod}\, p)) \\ 0, & \text{else} \end{cases}.$$

Proof. We will consider more detailed this sum. For definiteness we will consider that $k > l$. Then

$$h(w_k + w_l) = h(c^{k-l} - 1)c^l w + bh(F_k(c) - F_l(c)) + aw^{-1}h(G_k(c) - G_l(c)) +$$
$$+ a^2 w^{-3} h(F_k(a,c,w) - F_k(a,c,w))$$

where F, G are polynomials defined before.

Let $w = u + p^{n-1}z$, with $u \in R_{n-1}^*, z \in R_1$. Then $w^{-1} = u^{-1} - p^{n-1}zu^{-2}$, $w^j = u^j - jp^{n-1}zu^{j-1}$, $w^{-j} = u^{-j} + jp^{n-1}zu^{-j-1} (\mathrm{mod}\, p^n)$.

We will rewrite our sum in the form: $\sigma_{k,l} = \sum_{w \in R_n^*} e_{p^n}(h(w_k - w_l)) =$

$$= \sum_{u \in R_{n-1}^*} e_{p^n}(h(c^{k-1}-1)c^l u + Aau^{-1}h + Ba^2u^{-3}h) \times$$

$$\times \sum_{z \in R_1} e_{p^n}(p^{n-1}z(h(c^{k-1}-1)u + Aau^{-2}h + 3Ba^2u^{-4}h)$$

with $A = G_k(c) - G_l(c), B = F_k(a,c,w) - F_k(a,c,w)$

For an internal sum we have

$$\sum_{z \in R_1} e_{p^n}(p^{n-1}z(h(c^{k-1}-1)u + Aau^{-2}h + 3Ba^2u^{-4}h)) = \begin{cases} p\ , & \text{if } c^{k-1} \equiv 1 (\mathrm{mod}\, p)) \\ 0\ , & \text{else} \end{cases}$$

Taking into account estimation for the sums of Kloosterman, we have

$$\sigma_{k,l} = p \sum_{u \in R_{n-1}^*} e_{p^n}(h(c^{k-1}-1)c^l u + Aau^{-1}h + Ba^2u^{-3}h) << \begin{cases} p^{\frac{n+1}{2}}, \text{if } (h(c^k - c^l) \equiv 0 (\mathrm{mod}\, p)) \\ 0\ , \text{else} \end{cases}$$

Lemma is proved.

Lemma 6. *Maximal period of sequence* $\{w_k\}$ *generated by (1) equals to* p^{n-1}*, and arrived at subject to condition* $(c,p) = 1$, $c = 1 + pt$, $(p,t) = 1$.

Proof. In our definition $w_0 = w$, we will find such k that $w_k \equiv w_0 = w (\mathrm{mod}\, p^n)$. By Lemma 4 we have

$$w_k = c^k w + b\frac{c^0 - c^k}{1-c} + aw^{-1}\frac{c^{-k+1} - c^{k+1}}{1-c^2} + a^2 w^{-3} F_k(a,c,w)).$$

$$w_k = c^k w + p\left(p^{\beta-1} b_0 \frac{c^0 - c^k}{1-c} + a_0 w^{-1} p^{\alpha-\beta}\frac{c^{-k+1} - c^{k+1}}{1-c^2} + a_0 p^{\alpha-\beta} a w^{-3} F_k(a,c,w))\right)$$

It is clear that $w_k \equiv w (\mathrm{mod}\, p^n)$ only if $c^k \equiv 1 (\mathrm{mod}\, p^n)$. So $k = p^{n-1}$.

Taking into account $c = 1 + pt$ have

$$w_k = (c^k - 1)w + p(p^{\beta-1} b_0 (k + k(k-1)pt + ...) + a_0 w^{-1} p^{\alpha-\beta}(k + k(k-1)A_1 pt + ...) +$$
$$+ a_0 p^{\alpha-\beta} a w^{-3} F_k(a,c,w)))$$

$$(c^k - 1) \equiv 0 (\mathrm{mod}\, p^n),$$

$$p(p^{\beta-1} b_0 (k + k(k-1)pt + ...) + a_0 w^{-1} p^{\alpha-\beta}(k + k(k-1)A_1 pt + ...) +$$
$$+ a_0 p^{\alpha-\beta} a w^{-3} F_k(a,c,w))) =$$

$$= pp^{n-1}(p^{\beta-1} b_0 (1 + 1(k-1)pt + ...) + a_0 w^{-1} p^{\alpha-\beta}(1 + 1(k-1)A_1 pt + ...) +$$
$$+ a_0 p^{\alpha-\beta} a w^{-3} F_k(a,c,w)))$$

$$\equiv 0 (\mathrm{mod}\, p^n)$$

From this we get that maximal period of sequence $\{w_k\}$ equals to p^{n-1}.

3. Exponential sums on pseudorandom numbers. Let *h* and *N* be integers, $(h,p)=p^{\delta}, 0\le\delta<n$ and let τ be the least period length of the sequence $w=\{w_k\}, k=0,1,2,\ldots$. Denote

$$S_N(h,w)=\sum_{k=0}^{N-1} e_{p^n}(hw_k).$$

Estimations of S_N are got in the next theorems.

Theorem 1. *Let* $w=\{w_k\}, k=0,1,2,\ldots$ *sequence generated by (1),* $w\in\mathbb{R}_n^*$ *have maximal period* $\tau=p^{n-1}$ *with* $(c,p)=1$, $c=1+pt$, $(p,t)=1$. *Then the following bound*

$$|S_\tau(h,w)|<<\begin{cases}2p^{\frac{n+\delta}{2}}, & \text{if } \alpha=\beta=1, w+b_0t^{-1}+2a_0t^{-1}\equiv 0(\mathrm{mod}\, p)\\ 0, & \text{else}\end{cases}.$$

holds.

Proof. $|S_\tau(h,w)|=\left|\sum_{k=0}^{\tau-1} e_{p^n}(hw_k)\right|=$

$$=\left|\sum_{k=0}^{\tau-1} e_{p^n}\left(h\left(c^k w+b\frac{1-c^k}{1-c}+aw^{-1}\frac{c^{-k+1}-c^{k+1}}{1-c^2}+a^2w^{-3}F_k(a,c,w)\right)\right)\right|=$$

$$=\left|\sum_{k=0}^{\tau-1}\exp\left(2\pi ihp^{-n}\left(c^k w+b\frac{1-c^k}{1-c}+aw^{-1}\frac{c^{-k+1}-c^{k+1}}{1-c^2}+a^2w^{-3}F_k(a,c,w)\right)\right)\right|$$

We will paint a value for c^k and c^{-k}:

$$c^k=(1+pt)^k=1+kpt+\frac{k(k-1)}{2}p^2t^2+\ldots=1+kpt\left(1+\frac{1}{2}pt+\ldots\right)+$$

$$+k^2p^2t^2\left(\frac{1}{2}+\frac{1}{2}pt+\ldots\right)+\ldots,$$

$$c^{-k}=\frac{1}{(1+pt)^k}=\frac{1}{1+kpt\left(1+\frac{1}{2}pt+\ldots\right)+k^2p^2t^2\left(\frac{1}{2}+\frac{1}{2}pt+\ldots\right)+\ldots}=$$

$$=1-\left(kpt\left(1+\frac{1}{2}pt+\ldots\right)+k^2p^2t^2\left(\frac{1}{2}+\frac{1}{2}pt+\ldots\right)+\ldots\right)+$$

$$+\left(kpt\left(1+\frac{1}{2}pt+\ldots\right)+k^2p^2t^2\left(\frac{1}{2}+\frac{1}{2}pt+\ldots\right)+\ldots\right)^2-\ldots.$$

Then

$$c^k w + b\frac{1-c^k}{1-c} + aw^{-1}\frac{c^{-k+1}-c^{k+1}}{1-c^2} + a^2 w^{-3} F_k(a,c,w) = (1 + kpt(1+\frac{1}{2}pt+...) +$$

$$+k^2p^2t^2(\frac{1}{2}+...)+...)w + b\frac{1-1-kpt(1+\frac{1}{2}pt+...)-k^2p^2t^2(\frac{1}{2}+\frac{1}{2}pt+...)-...}{1-1-pt} +$$

$$+aw^{-1}c\frac{1-\left(kpt(1+\frac{1}{2}pt+...)+...\right)+...-1-kpt(1+\frac{1}{2}pt+...)-...}{1-1-2pt-p^2t^2} + +a^2w^{-3}F_k(a,c,w) =$$

$$= w + kpt(w + bt^{-1}(1+2^{-1}pt+...) + aw^{-1}(-2(1+2^{-1}pt+...+))) + k^2p^2t^2((2^{-1}+...)w +$$

$$+bt^{-1}(2^{-1}+2^{-1}pt+...) + acw^{-1}(2\times 2^{-1}-1)) + ...$$

We will put this presentation in a formula for a sum

$$|S_\tau(h,w)| = |\sum_{k=0}^{\tau-1}\exp(2\pi i h p^{-n}(w + kpt(w + bt^{-1}(1+...) + aw^{-1}(-2(1+...))) +$$

$$+k^2p^2t^2((2^{-1}+...)w + bt^{-1}(2^{-1}+...))+...))| =$$

$$= |\sum_{k=0}^{\tau-1}\exp(2\pi i h p^{1-n} kt\left(w + bt^{-1}(1+...) + aw^{-1}(-2(1+...))\right) +$$

$$+k^2p^2t^2\left((2^{-1}+...)w + bt^{-1}(2^{-1}+...)\right))| =$$

$$= |\sum_{k=0}^{\tau-1}\exp(2\pi i h k t p^{1-n}((w + bt^{-1}(1+...) + aw^{-1}(-2(1+...))) +$$

$$+hk^2pt^2((2^{-1}+...)w + bt^{-1}(2^{-1}+...))+...))| =$$

$$= p^\delta\,|\sum_{k=0}^{\tau-1}\exp(2\pi i h_0 k t p^{1-n+\delta}((w + b_0 p^\beta t^{-1}(1+...) + a_0 p^\alpha w^{-1}(-2(1+...))) +$$

$$+h_0k^2pt^2((2^{-1}+...)w + b_0p^\beta t^{-1}(2^{-1}+...)+...))| =$$

$$= p^\delta\,|\sum_{k=0}^{\tau-1}\exp(2\pi i h_0 k t p^{1-n+\delta}(w + p^{\beta-1}(b_0 t^{-1}(1+...) + a_0 w^{-1}p^{\alpha-\beta}(-2(1+...))) +$$

$$+hk^2pt^2((2^{-1}+...)w + b_0p^{\beta-1}t^{-1}(2^{-1}+...)+...))|$$

Then, using Lemma 1 we get the bound for S_τ

$$|S_\tau(h,w)| << \begin{cases} 2p^\delta p p^{\frac{n-\delta-2}{2}}, & \text{if } \alpha=\beta=1, w + b_0 t^{-1} + 2a_0 t^{-1} \equiv 0 (\mathrm{mod}\, p) \\ 0, & \text{else} \end{cases}$$

Theorem 2. *Let* $w = \{w_k\}, k = 0,1,2,\ldots$ *sequence generated by recurrent formula (1), and* τ *its least period,* $(h,p) = p^{\delta}$ *and* $N \in \mathbb{N}, 1 \le N < p^n$.

$$|S_N(h,w)| \le \begin{cases} 2\frac{N}{p^n} p^{\frac{n+\delta}{2}} + 2p^{\frac{n+\delta}{2}} \log\tau, & \text{if } \alpha = \beta = 1, w + b_0 t^{-1} + 2a_0 t^{-1} \equiv \\ & \equiv 0 (\mathrm{mod}\, p), x_0 t^{-1} \equiv 0 (\mathrm{mod}\, p) \\ 2p^{\frac{n+\delta}{2}} \log\tau, & \text{if } \beta > 0,\ w + x_0 t^{-1} \equiv 0 (\mathrm{mod}\, p) \\ 2p^{\frac{n+\delta}{2}} \log\tau, & \text{if } \beta = 1,\ \alpha - \beta > 0,\ w + x_0 t^{-1} + b_0 t^{-1} \equiv \\ & \equiv 0 (\mathrm{mod}\, p),\ w + b_0 t^{-1} \not\equiv 0 (\mathrm{mod}\, p) \\ 2p^{\frac{n+\delta}{2}} \log\tau, & \text{if } \alpha = \beta = 1, w + b_0 t^{-1} + a_0 t^{-1} + x_0 t^{-1} \equiv \\ & \equiv 0 (\mathrm{mod}\, p),\ w + b_0 t^{-1} \not\equiv 0 (\mathrm{mod}\, p) \end{cases}$$

Proof. We will estimate the sum using $S_N(h,w)$ bounds for incomplete sums. We have

$$|S_N(h,w)| = \left| \sum_{l=0}^{N-1} \frac{1}{p^n} \sum_{k=0}^{p^n-1} \sum_{x=0}^{p^n-1} e_{p^n}(hw_k) e_{p^n}(x(k-l)) \right| \le$$

$$\le \frac{N}{p^n} \left| \sum_{k=0}^{p^n-1} e_{p^n}(hw_k) \right| + \sum_{x=0}^{\tau-1} \frac{1}{\min(x, \tau - x)} \left| \sum_{k=0}^{\tau-1} e^{2\pi i \left(\frac{hw_k}{p^n} + \frac{kx}{\tau} \right)} \right|.$$

Let $x = x_0 p^{\delta}$. We will consider an internal sum

$$\sum_{k=0}^{\tau-1} \exp\left(2\pi i \left(\frac{hw_k}{p^n} + \frac{kx}{\tau} \right) \right) = \sum_{k=0}^{\tau-1} \exp\left(2\pi i \left(\frac{hw_k + kpx}{p^n} \right) \right) = p^{\delta} \sum_{k=0}^{\tau-1} \exp(2\pi i h_0 k t p^{1-n+\delta} (w + x_0 t^{-1} +$$

$$+ p^{\beta-1} (b_0 t^{-1} (1 + 2^{-1} pt + \ldots) + a_0 p^{\alpha-\beta} c w^{-1} (-2(1 + 2^{-1} pt + \ldots +)))) + h_0 k^2 p t^2 ((2^{-1} + \ldots) w +$$

$$+ b_0 p^{\beta-1} t^{-1} (2^{-1} + 2^{-1} pt + \ldots)) + \ldots)$$

Then for $S_N(h,w)$ we get

$$\left|S_N(h,w)\right| \le \begin{cases} 2\dfrac{N}{p^n}p^{\frac{n+\delta}{2}} + 2p^{\frac{n+\delta}{2}}\log\tau, & \text{if } \alpha=\beta=1, w+b_0t^{-1}+2a_0t^{-1} \equiv \\ & \equiv 0(\mathrm{mod}\, p), x_0t^{-1} \equiv 0(\mathrm{mod}\, p) \\ 2p^{\frac{n+\delta}{2}}\log\tau, & \text{if } \beta>0,\ w+x_0t^{-1} \equiv 0(\mathrm{mod}\, p) \\ 2p^{\frac{n+\delta}{2}}\log\tau, & \text{if } \beta=1,\ \alpha-\beta>0,\ w+x_0t^{-1}+b_0t^{-1} \equiv \\ & \equiv 0(\mathrm{mod}\, p),\ w+b_0t^{-1} \not\equiv 0(\mathrm{mod}\, p) \\ 2p^{\frac{n+\delta}{2}}\log\tau, & \text{if } \alpha=\beta=1, w+b_0t^{-1}+a_0t^{-1}+x_0t^{-1} \equiv \\ & \equiv 0(\mathrm{mod}\, p),\ w+b_0t^{-1} \not\equiv 0(\mathrm{mod}\, p) \end{cases}$$

Using estimations of exponential sums got in theorem 1 and theorem 2 allows investigating the sequence of pseudorandom numbers on unpredictable and uniform distribution how it is done for authors [6], [9], [12]

REFERENCES

1. Chou W.-S. The period lengths of inversive congruential recursions // Acta Arithm. – 1995. – v. 73(4). – P. 325–341.
2. Eichenauer J., Lehn J. A non-linear congruential pseudorandom number generator // Stat. Hefte. – 1986. – v. 27. – P. 315–326.
3. Kato T., Wu L.-M., Yanagihara N. On a nonlinear congruential pseudorandom number generator // Math. Comput. – 1996. – v. 65(213). – P. 227–233.
4. Niederreiter H. Random Number Generation and Quasi-Monte Carlo Methods. – SIAM, Philadelphia, 1992.
5. Niederreiter H., Shparlinski I.E. On the distribution of pseudorandom numbers and vectors by inversive methods // Appl. Algebra Eng. Commun. Comput. – 2000. – v. 10(3). – P. 189–202.
6. Niederreiter H., Shparlinski I. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus // Acta Arithm. – 2000. – v. 90(1). – P. 89–98.
7. Varbanets S. Exponential sums on the sequences of inversive congruential pseudorandom numbers // Siauliai Math. Semin. – 2008. – v. 3 (11). – P. 247–261.