П.Д.Варбанец (Одесса)

ЛИНЕЙНО-ИНВЕРСНЫЙ КОНГРУЭНТНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

В данной статье мы рассматриваем обобщение инверсного конгруэнтного ПСЧ генератора псевдослучайных чисел по модулю степени простого и получаем оценки экспоненциальных сумм на последовательности псевдослучайных чисел. Также мы получили оценку среднего значения экспоненциальных сумм от инициального значения y_0 и оценки для дискрепансии s -мерных "перекрывающихся" точек.

1 Введение

Нелинейные методы генерирования равномерно распределенных в интервале [0,1) псевдослучайных чисел были введены и изучались в течение последних двадцати пяти лет.

Этапы развития данной области исследования представлены в обзорных статьях (Chou [1], Eichenauer and Lehn [2], Eichenauer-Herrmann and Topuzo ğ lu [3], Niederreiter Shparlinski [5]) и в монографии Niederreiter [4]. Инверсные конгруэнтные генераторы занимают особое место среди нелинейных генераторов преимущественно ввиду простоты реализации вычислений. В случае модуля степени нечетного простого числа инверсный конгруэнтный генератор определяется следующим образом:

Пусть $p \geq 3$ простое, m -натуральное. Для заданных $a, b \in \mathbb{Z}$ мы выбираем начальное значение y_0, и пусть y_n^{-1} есть мультипликативное обратное к y_n из $\mathbb{Z}_{p^m}^*$, если $(y_n, p) = 1$, и $y_n^{-1} = 0$, если $m = 1$ и $y_n \equiv 0 (mod\ p)$. Рекурентное соотношение

$$y_{n+1} \equiv a y_n^{-1} + b (mod\ p^m) \qquad (1.1)$$

порождает последовательность $y_0, y_1, \ldots$, которую мы называем инверсной конгруэнтной последовательностью по модулю p^m.

Случай $p >= 3$, $m = 1$ был изучен в [2]. Далее мы будем полагать, что $m >= 3$. В таком случае порождаемая последовательность $\{y_n\}$, $n >= 0$ может существовать только, если $(y_n, p) = 1$ для всех n = 0,1,2. В работе [1] были указаны условия, при которых последовательность $\{y_n\}$ не обрывается.

Пусть $\{y_n\}$ бесконечная последовательность, порожденная конгруэнцией (1.1). Нормализуя её,

$$x_n = \frac{y_n}{p^m},$$

мы получаем последовательность чисел из интервала [0,1) .

Последовательность $\{x_n\}$ называется последовательностью псевдослучайных чисел (ПСЧ) в интервале [0,1), если она удовлетворяет требованиям равнораспределенности и непредсказуемости (статистической независимости). Свойство статистической независимости является чрезвычайно важным криптографическим требованием.

Ещё одной важной характеристикой последовательности ПСЧ $\{x_n\}$ является её период τ. Ясно, что $\tau \le p^{m-1}(p-1)$.

В работах Chou [1], Eichenauer и Lehn [2], Eichenauer и Topuzuglu [3], Niederreiter [4] была изучена проблема, когда последовательность ПСЧ (порожденная (1.1)) имеет максимальный период.

В данной статье мы изучаем нелинейный генератор (подобный (1.1)) следующего вида:

$$y_{n+1} \equiv a y_n^{-1} + b + c y_n (mod\ p^m), \qquad (1.2)$$

при условии $(a,p) = (y_0,p) = 1$, $b \equiv c \equiv 0 (mod p)$.

Заметим, что условия $(a,p) = 1$, $b = c = ti(mod p)$ гарантируют бесконечность процесса генерирования.

Генератор (1.2) с условиями $a \equiv b \equiv 0 (mod p)$, $(c,p) = 1$, также может быть изучен. Генератор (1.2) мы называем линейно-инверсным конгруэнтным генератором ПСЧ.

Цель нашей работы – показать, что последовательность ПСЧ $\{x_n\} = \left\{\frac{y_n}{p^m}\right\}, n = 0,1,\ldots,$ порожденная рекурсией (1.2), удавлетворяет требованиям равнораспределенности на [0,1) и проходит сериальный тест на непредсказуемость.

Обозначения. Переменные суммирования пробегают все целые числа, удовлетворяя соответствующим условиям. Символом p обозначаем простое число, $p \ge 3$. Для $m \in \mathbb{N}$ запись $\mathbb{Z}_{p^m}$ (соответственно, $\mathbb{Z}_{p^m}^*$) обозначает полную (соответственно, приведенную) систему вычетов по модулю p^m. Мы пишем $gcd(a,b) = (a,b)$ для обозначения общего наибольшего делителя чисел a и b. Для $z \in \mathbb{Z}$, $(z,p) = 1$ пусть z^{-1} означает мультипликативное обратное по модулю p^m. Мы пишем $\nu_p(A) = \alpha$, если $p^\alpha \mid A$, $p^{\alpha+1} \nmid A$. Для вещественного t мы используем запись $e(t) = e^{2\pi i t}$.

2 Вспомогательные результаты

ЛЕММА 1. *Пусть p простое и пусть $f(x)$, $g(x)$ многочлены над Z*

$$f(x) = A_1 x + A_2 x^2 + p(A_3 x^3 + \cdots),$$
$$g(x) = B_1 x + + p(B_2 x^2 + \cdots),$$

и пусть, кроме того, $\nu_p(A_2) = \alpha > 0$, $\nu_p(A_j) \ge \alpha$, $j = 3,4,\ldots$.

Тогда мы имеем следующие оценки

$$\left|\sum_{x \in \mathbb{Z}_{p^m}} e\left(\frac{f(x)}{p^m}\right)\right| \le \begin{cases} 2p^{\frac{m+\alpha}{2}}, if\ \nu_p(A_1) \ge \alpha \\ 0, \quad else \end{cases} \qquad (2.1)$$

$$\left|\sum_{x \in \mathbb{Z}_{p^m}^*} e\left(\frac{f(x)+g(x^{-1})}{p^m}\right)\right| \le \begin{cases} (\overline{N} \cdot p)^{\frac{m}{2}}, if\ (B_1, p) = 1 \\ 2p^{\frac{m+\alpha}{2}}, if\ \nu_p(A_1) \ge 0, \nu_p(B_j) \ge \alpha, \ldots \\ 0, if\ \nu_p(A_1) < \alpha \le \nu_p(B_j),\ j \ge 1 \end{cases} \qquad (2.2)$$

где $\overline{N} = \overline{N}(A_1, B_1; p)$ *число решений сравнения* $A_1 - B_1 u^2 \equiv 0 (mod\ p)$ в $\mathbb{Z}^*_{p^m}$. (Это утверждение является следствием оценок Гауссовой суммы и суммы Клостермана).

Пусть $\{y_n\}$ порождено рекурсивным соотношением (1.2). Пользуясь выкладками из [6], мы получаем следующие результаты.

ЛЕММА 2. *Пусть* $\{y_n\}$ *последовательность ПСЧ, порожденная рекурсией (1.2) при условиях* $(y_0, p) = (a, p) = 1$, $0 < \nu_p(b) < \nu_p(c)$. *Тогда существуют многочлены* $F_0(u, v, w)$, $G_0(u, v, w)$ *над* Z, $F_0(0, v, w) = G_0(0, v, w) = 0$ *такие, что для любого* $k \geq 2m+1$:

$$y_{2k} = kb + kacy_0^{-1} + (1 - k(k-1)a^{-1}b^2)y_0 + (-ka^{-1}b)y_0^2 + (-ka^{-1}c + k^2a^{-2}b^2)y_0^3 + p^{\alpha}F_0(k, y_0, y_0^{-1}), \quad (2.3)$$

$$y_{2k+1} = (k+1)b + (a - k(k+1)b^2)y_0^{-1} + (-kab)y_0^{-2} + (-ka^2c + k^2ab^2)y_0^{-3} + (k+1)cy_0 + p^{\alpha}G_0(k, y_0, y_0^{-1}), \quad (2.4)$$

где $\alpha := \min(\nu_p(b^3), \nu_p(bc))$;

$F_0(u, v, w), G_0(u, v, w) \in \mathbb{Z}[u, v, w]$, $F_0(0, v, w) = G_0(0, v, w) = 0$.

СЛЕДСТВИЕ 1. *Пусть справедливы условия Леммы 2. Тогда для* $p > 2$ *последовательность* $\{y_n\}$ *является чисто периодической с периодом* $2p^{m-\ell}$, *где*

(i) $\ell = \nu_p(b) + \nu_p(a - y_0^2)$, if $\nu_p(a - y_0^2) < \nu_p(b) \leq \frac{1}{2}m$;

(ii) $\ell = 2\nu_p(b)$, if $\nu_p(a - y_0^2) > \nu_p(b)$, $\nu_p(b) \leq \frac{1}{2}m$.

Для $p = 2$ также можно получить аналогичное утверждение и следующее

СЛЕДСТВИЕ 2. *Пусть* $p = 2$ *и* $m \geq 3$. *Тогда последовательность* $\{y_n\}$, *определенная рекурсией (1.2), является чисто периодической, где* $b = 2^{\nu} b_0$, $(b_0, 2) = 1$, $c = 2^{\mu} c_0$, $(c_0, p) = 1$, $\mu > \nu > 0$; $\nu_2(a - y_0^2) = \nu_0 \geq 1$. *И этот период* τ *равен*

(i) $2^{m-2\nu+1}$, *if* $m \geq 2\nu, \nu_0 > \nu$;

(ii) $2^{m-2\nu-\beta_0+1}$, *if* $m > 2\nu, \nu_0 = \nu, \beta_0 = \nu_p\left(\frac{y_0^2 - a}{2^{\nu_0}} + b_0\right)$;

(iii) $2^{m-\nu-\nu_0+1}$, *if* $m \geq \nu + nu_0, \nu_0 < \nu$.

3 Экспоненциальные суммы на последовательности ПСЧ

В этом разделе мы получаем оценки экспоненциальных сумм над линейно-инверсной конгруэнтной последовательностью $\{y_n\}$, которая была определена в (1.2).

Для $h_1, h_2 \in \mathbb{Z}$ мы определяем

$$\sigma_{k,l}(h_1, h_2; p^m) := \sum_{y_0 \in \mathbb{Z}^*_{p^m}} e\left(\frac{h_1 y_k + h_2 y_l}{p^m}\right), \ (h_1, h_2 \in \mathbb{Z}) \quad (3.1)$$

Здесь y_k, y_ℓ, порожденные в (1.2), рассматриваются как функции от инициального значения y_0 (см., формулы (2.3)-(2.4)).

ТЕОРЕМА 1. *Пусть* $(h_1, h_2, p) = 1$, $\nu_p(h_1 + h_2) = \beta$, $\nu_p(h_1 k + h_2 \ell) = \gamma$. *Справедливы следующие оценки:*

$$|\sigma_{k,\ell}(h_1,h_2;p^m)| \le \begin{cases} N(h_1,ah_2;p)\,p^{\frac{m}{2}} & k \not\equiv \ell (mod\,2); \\ 0 & k \equiv \ell (mod\,2) \\ & \beta < \gamma+\nu, m-\beta-\nu > 0; \\ p^{m-1}(p-1) & k \equiv \ell (mod\,2) \\ & \beta \ge \gamma+\nu, m-\nu-\gamma \le 0; \\ 2p^{\frac{m+\nu+\gamma}{2}} & k \equiv \ell (mod\,2) \\ & \beta \ge \gamma+\nu, m-\nu-\gamma > 0. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Мы рассматриваем два случая:

(I) Пусть k и ℓ неотрицательные целые различной четности, например, $k := 2k$, $\ell := 2\ell+1$. Из (2.6), (2.7) имеем

$$\begin{aligned} h_1 y_{2k} + h_2 y_{2\ell+1} &= A_0 + A_1 y_0 + A_2 y_0^2 + A_3 y_0^3 + \\ &+ A_{-1} y_0^{-1} + A_{-2} y_0^{-2} + A_{-3} y_0^{-3} + \\ &+ p^{\alpha} H(y_0, y_0^{-1}) := F_1(y_0, y_0^{-1}), \end{aligned}$$

где

$$A_1 \equiv h_1 (mod\ p^{\nu}), A_2 \equiv -h_1 kab (mod\ p^{\nu+1}),$$
$$A_{-1} \equiv ah_2 (mod\ p^{\nu}), A_{-2} \equiv -h_2 ab\ell (mod\ p^{\nu+1}),$$
$$A_3 \equiv A_{-3} \equiv 0 (mod\ p^{\mu}), \mu = \nu_p(c) > \nu_p(b) = \nu.$$

Применяя Лемму 1, мы сначала получим утверждение теоремы для $k \not\equiv \ell (mod\,2)$.

(II) Пусть k и ℓ целые числа одинаковой четности. Тогда для $k := 2k$, $\ell := 2\ell$ мы имеем по модулю p^m:

$$\begin{aligned} h_1 y_{2k} + h_2 y_{2\ell} &= B_0 + B_1 y_0 + B_2 y_0^2 + B_3 y_0^3 + B_{-1} y_0^{-1} + p^{\alpha} K(y_0, y_0^{-1}) = \\ &:= F_2(y_0, y_0^{-1}), \end{aligned}$$

где

$$\begin{aligned} B_1 &= h_1 + h_2 + p^{2\nu} B_1', \\ B_2 &= -ab(h_1 k + h_2 \ell) + p^{\alpha} B_2', \\ B_3 &= -a^{-2} b^2 (h_1 k^2 + h_2 \ell^2) - a^{-1} c(h_1 k + h_2 \ell) + p^{\alpha} B_3', \\ B_{-1} &= ac(h_1 k + h_2 \ell) + p^{\alpha} B_{-1}'; \end{aligned}$$

кроме того, B_1', B_2', B_3', B_{-1}' и коэффициенты в $K(y_0, y_0^{-1})$ содержат множители вида $h_1 k^j + h_2 \ell^j$, $j \ge 0$.

Теперь, для того, чтобы применить оценку полной линейной суммы к сумме

$$\sum_{y_0 \in \mathbb{Z}_{p^m}^*} e\left(\frac{h_1 y_{2k} + h_2 y_{2\ell}}{p^m}\right) = \sum_{y_0 \in \mathbb{Z}_{p^m}^*} e\left(\frac{F_2(y_0, y_0^{-1})}{p^m}\right)$$

мы должны определить значения $\nu_p(B_1)$, $\nu_p(B_2)$, $\nu_p(B_3)$, $\nu_p(B_{-1})$.

Для $\nu_p(h_1 + h_2) = \beta \ge \nu$, $\nu_p(h_1 k + h_2 \ell) = 0$ мы получаем

$$|\sigma_{k,\ell}(h_1, h_2, p^m)| \le 2p^{\frac{m+\nu}{2}}.$$

Для $\nu_p(h_1 + h_2) = \beta \ge \nu$, $\nu_p(h_1 k + h_2 \ell) = \gamma > 0$ мы обозначаем $\delta = \min(\beta, \gamma)$.

Кроме того, в таком случае имеем

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

и тогда индукцией по j получаем

$$\nu_p(h_1 k^j + h_2 \ell^j) \ge \delta, j = 2,3,\ldots$$

Таким образом, мы можем применить оценку полной линейной экспоненциальной суммы.

Следовательно,

$$|\sigma_{2k,2\ell}(h_1,h_2;p^m)| \le \begin{cases} 0 & \beta < \gamma+\nu, m-\beta-\nu > 0, \\ 2p^{\frac{m+\nu+\gamma}{2}} & \beta \ge \gamma+\nu, m-\nu-\gamma > 0, \\ \varphi(p^m) & \beta \ge \gamma+\nu, m-\nu-\gamma \le 0, \end{cases}$$

где $\varphi(n)$ функция Эйлера.

Для $k \equiv \ell \equiv 1 (mod\,2)$ получаются аналогичные результаты.

Это завершает доказательство Теоремы 1.

Пусть h целое, $(h,p^m)=p^s$, $0\le s<m$, и пусть τ наименьшая длина периода последовательности ПСЧ $\{y_n\}$, $n=0,1,\ldots$, определенной из (1.2). Для $1\le N\le\tau$ мы полагаем

$$S_N(h,y_0)=\sum_{n=0}^{N-1}e\left(\frac{hy_n}{p^m}\right). \tag{3.2}$$

Сумма $S_N(h,y_0)$ называется экспоненциальной суммой на последовательности ПСЧ $\{y_n\}$.

ТЕОРЕМА 2. *Пусть линейно-инверсная конгруэнтная последовательность, порожденная рекурсией (1.2), имеет период τ, и пусть $\nu_p(b)=\nu$, $\nu_p(a-y_0^2)=\nu_0$, $2\nu\le m$. Тогда мы имеем следующие оценки:*

$$|S_\tau(h,y_0)|\le\begin{cases}O(m) & p>2,\nu_0<\nu,\nu_p(h)<m-\nu-\nu_0\\ & or\quad p=2,\nu_0<\nu,\nu_2(h)<m-2\nu;\\ 4\cdot p^{\frac{m+\nu_p(h)}{2}} & \nu_0\ge\nu,\nu_p(h)<m-2\nu;\\ \tau & ,\quad else\end{cases}$$

ДОКАЗАТЕЛЬСТВО. Аналогично доказательству Теоремы 1 имеем

$$\begin{aligned}|S_\tau(h,y_0)| &=\left|\sum_{n=0}^{\tau-1}e\left(\frac{hy_n}{p^m}\right)\right|=\left|\sum_{n=0}^{p^\ell-1}e\left(\frac{hy_n}{p^m}\right)\right|\le\\ &\le\left|\sum_{\substack{k_1=0\\k=2k_1}}^{p^\ell-1}e\left(\frac{hy_{2k_1}}{p^m}\right)\right|+\left|\sum_{\substack{k_1=0\\k=2k_1+1}}^{p^\ell-1}e\left(\frac{hy_{2k_1+1}}{p^m}\right)\right|= \qquad (3.3)\\ &=\left|\sum_{k=0}^{p^\ell-1}e\left(\frac{hF(k)}{p^m}\right)\right|+\left|\sum_{k=0}^{p^\ell-1}e\left(\frac{hG(k)}{p^m}\right)\right|+O(m).\end{aligned}$$

В последней части формулы (3.3) мы принимаем во внимание, что представление y_n в виде многочлена от k справедливо только для $k\ge 2m+1$.

Из следствий 1 и 2 и леммы 1 мы легко получаем

$$|S_\tau(h,y_0)|\le\begin{cases}O(m) & p>2,\nu_0<\nu,\nu_p(h)<m-\nu-\nu_0,\\ O(m) & p=2,\nu_0<\nu,\nu_2(h)<m-2\nu,\\ 4p^{\frac{m+\nu_p(h)}{2}} & \nu_0\ge\nu,\nu_p(h)<m-2\nu,\\ \tau & .\quad else\end{cases}$$

Константы в символах "O" являются абсолютными.

ТЕОРЕМА 3. *Пусть a, b, c параметры линейно-инверсного конгруэнтного генератора (1.2) и пусть $(a,p)=1$, $0<\nu=\nu_p(b)<\nu_p(c)$, $1\le N\le 2p^{m-1}$, $\nu_p(h)=p^s$, $s<m$. Тогда среднее значение суммы $S_N(h,y_0)$ над $y_0\in Z_{p^m}^*$ удовлетворяет*

$$\overline{S}_N(h)=\frac{1}{\varphi(p^m)}\sum_{y_0\in Z_{p^m}^*}|S_N(h,y_0)|\le N^{\frac12}p^{-\frac{m}{4}}\left(2\left(\varepsilon_p(a)\right)^{\frac{m}{4}}+\sqrt{10}p^{\frac{\nu+s}{4}}\right)$$

где $s=\nu_p((h,p^m))$, $h=h_0p^s$,

$$\varepsilon_p(a)=\begin{cases}1 & p=2\\ 1+\left(\frac{-a}{p}\right) & p>2,\left(\left(\frac{-a}{p}\right)-\textit{символ Лежандра}\right)\end{cases}$$

ДОКАЗАТЕЛЬСТВО. Сначала рассмотрим случай s = 0, т.е. *(h,p)* = 1. Из неравенства Коши-Шварца мы получаем

$$|\overline{S}_N(h)|^2 \le \frac{1}{\varphi(p^m)} \sum_{y_0 \in Z^*_{p^m}} |S_N(h,y_0)|^2 =$$

$$= \frac{1}{\varphi(p^m)} \sum_{k,\ell=0}^{N-1} \sum_{y_0 \in Z^*_{p^m}} e\left(\frac{h(y_k - y_\ell)}{p^m}\right) \le$$

$$\le \frac{1}{\varphi(p^m)} \sum_{k,\ell=0}^{N-1} |\sigma_{k,\ell}(h,-h;p^m)| =$$

$$= N + \frac{1}{\varphi(p^m)} \sum_{\gamma=0}^{m-1} \sum_{\substack{k,\ell=0 \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}(h,-h;p^m)|.$$

Далее

$$|\overline{S}_N(h)|^2 \le$$

$$\le N + \frac{1}{\varphi(p^m)} \sum_{\gamma=0}^{m-1} \left(\sum_{\substack{k,\ell=0 \\ k \equiv \ell (mod\ 2) \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell(h,-h;p^m)}| + \sum_{\substack{k,\ell=0 \\ k \equiv \ell (mod\ 2) \\ \nu_p(k-\ell)=\gamma}}^{N-1} |\sigma_{k,\ell}(h,-h;p^m)| \right)$$

Используя теорему 1, после простых вычислений мы получаем

$$|\overline{S}_N(h)|^2 \le N\left(4\varepsilon_p(a)^{\frac{m}{2}} p^{-\frac{m}{2}} + 8p^{\frac{-m+\nu}{2}} + 2p^{\nu-m}\right) \le$$

$$\le Np^{-\frac{m}{2}}\left(4(\varepsilon_p(a))^{\frac{m}{2}} + 10p^{\frac{\nu}{2}}\right),$$

поэтому мы можем заключить, что для $(h,p)=1$:

$$|\overline{S}_N(h)| \le N^{\frac{1}{2}} p^{-\frac{m}{4}}\left(2(\varepsilon(a))^{\frac{m}{4}} + \sqrt{10}p^{\frac{\nu}{4}}\right) \qquad (3.4)$$

Теперь простыми рассуждениями, использованными для доказательства формулы (3.4), мы приходим к общей оценке

$$|S_N(h)| \le N^{\frac{1}{2}} p^{-\frac{m-s}{4}}\left(2(\varepsilon_p(a))^{\frac{m}{4}} + \sqrt{10}p^{\frac{\nu}{4}}\right).$$

Оценки экспоненциальных сумм, полученные в этом разделе, могут быть использованы для изучения свойств последовательности ПСЧ $\{y_n\}$.

Для нашей последовательности $\{x_n\}$ мы порождаем последовательность $\{X_n^{(s)}\}$ точек из $[0,1)^s$, полагая $X_n^{(s)} := (x_n, x_{n+1}, \ldots, x_{n+s-1})$. Из теорем 1 и 2 и неравенства для дискрепансии (см., Niederreiter [4, ch. 8]) мы имеем

ТЕОРЕМА 4. *Дискрепансия $D_N^{(s)}$, $s = 2,3,4$, точек, порожденных линейно-инверсным конгруэнтным генератором (1.2) с параметрами a, b, c, которые удовлетворяют условиям*

$$0 < \nu_p(b) = \nu, 2\nu < \mu = \nu_p(c), a \not\equiv y_0^2 (mod\ p),$$

удовлетворяет следующим неравенствам:

$$D_\tau^{(s)} \le \frac{s}{2p^{m-\nu}} + p^{-\frac{m-2\nu}{2}} \log^s p^m. \qquad (3.5)$$

Наконец заметим, что, как показывает теорема 3, для почти всех $y_0 \in \mathbb{Z}^*_{p^m}$ оценка дискрепансии не может быть улучшена.

Оценка (3.5) дискрепансии $D_\tau^{(s)}$ означает, что последовательность $\{x_n\}$, порожденная рекурсией (1.2), проходит s-мерный сериальный тест на статистическую независимость (непредсказуемость) для $s = 2,3,4$.

Литература

1. *Chou W.-S.* The period lengths of inversive congruential recursions, Acta Arith., 73:325-341, 1995.
2. *Eichenauer J., Lehn J.* A non-linear congruential pseudorandom number generator, Statist. Hefte, 27:315-326, 1986.
3. *Eichenauer-Herrmann J., Topuzoglu A.* On the period of congruential pseudorandom number sequences generated by inversions, J. Comput. Appl. Math., 31:87-96, 1990.

4. *Niederreiter H.* Random Number Generation и Quasi-Monte Carlo Methods. SIAM, 1992, Philadelphia,Pa.

5. *Niederreiter* //., *Shparlinski* /. Exponential sums и the distribution of inversive congruential pseudorandom numbers with prime-power modulus, Acta Arith., 90:89-98, 2000.

6. *Varbanets P., Varbanets S.* Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus, Voronol's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory и Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine, September 22-28, pages 112-130, Kyiv, 2008.

Варбанец Павел Дмитриевич, varbanetspd@mail.ru Одесский национальный университет им. И.И. Мечникова, Дворянская, 2, 65026, Одесса, Украина