УДК 511.9

Е. В. Вернигора
Одесский национальный университет имени И. И. Мечникова

СОСТАВНОЙ ИНВЕРСНЫЙ КОНГРУЕНТНЫЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Выражаю искреннюю благодарность доктору физ.-мат. наук, проф. Варбанцу Павлу Дмитриевичу

Вернигора О. В. Складений інверсний конгруентний генератор псевдовипадкових чисел. Досліджуються властивості рівнорозподіленості та непередбачуваності послідовностей дійсних чисел, породжених складеним інверсним конгруентним генератором. Отримані результати узагальнюють дослідження J. Eichenauer-Hermann та F. E. Emmerich.
Ключові слова: дискрепансія, псевдовипадкові числа, конгруентний генератор.

Вернигора Е. В. Составной инверсный конгруентный генератор псевдослучайных чисел. Исследуются свойства равнораспределенности и непредсказуемости последовательностей вещественных чисел, порожденных составным инверсным конгруентным генератором. Найденные результаты обобщают исследование J. Eichenauer-Hermann и F. E. Emmerich.
Ключевые слова: дискрепансия, псевдослучайные числа, конгруентный генератор.

Vernygora O. V. Compound inversive congruential generator of pseudorandom numbers. Properties of equidistribution and unpredictability of sequences of real numbers, which generated by compound inversive congruential generator are examinating. Our results are generalized by examinations J. Eichenauer-Hermann of and F. E. Emmerich.
Key words: discreapancy, pseudorandom numbers, congruential generator.

Введение. Наиболее простым методом генерирования псевдослучайных чисел (обозначается как ПСЧ) является линейный конгруентный метод, который определяется рекурсией:

$$y_{n+1} \equiv ay_n + b(mod\ M), \tag{1}$$

где $a, b, y_0 \in Z_M = \{0, 1, ..., M-1\}$.

Последовательность ПСЧ на $[0, 1)$ получается из последовательности $\{y_n\}$ нормировкой

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

Ясно, что период последовательности x_n не превосходит M. Последовательность x_n удовлетворяет требованию равнораспределенности на $[0, 1)$. Линейный метод широко использовался, пока не было установлено, что последовательность ПСЧ, порожденная генератором (1), имеет грубую решетчатую структуру, а потому не гарантирует непредсказуемость членов этой последовательности. Всякий нелинейный конгруентный генератор проходит решетчатый тест на непредсказуемость (см. [2]). Другой важной характеристикой последовательности ПСЧ

© Вернигора Е. В., 2010

является ее период. Для стохастического моделирования так же, как и для криптографических приложений, необходимо обеспечить достаточно большую длину минимального периода последовательности ПСЧ.

В настоящей работе мы строим составной инверсный конгруентный генератор ПСЧ, который обобщает составной генератор из работы Eichenauer-Herrmann и Emmerich [1].

Зафиксируем натуральные r_0 и r, $r_0 \leq r$. Пусть $p_1, ..., p_r$ — различные простые числа и $m_i, i = 1, ..., r$ — натуральные числа, и пусть для каждого $i = 1, ..., r_0$ заданы числа $A_i \,(mod\ p_i)$ такие, что

$$\text{многочлен } x^2 - x - A_i \text{ примитивен над полем } F_{p_i}, i = 1, ..., r_0; \qquad (i) \tag{2}$$

а для $i = r_0 + 1, ..., r$ пары чисел (a_i, b_i) такие, что

$$(a_i, p_i) = 1, b_i \equiv 0 \,(mod\ p_i)\,, b \not\equiv 0 \left(mod\ p_i^2\right), i = r_0 + 1, ..., r. \qquad (ii)$$

Пусть $M = p_1^{m_1} ... p_r^{m_r}$ — каноническое разложение M, причем $m_1 = m_2 = ... = m_{r_0} = 1, m_j \geq 2$ при $r_0 < j \leq r$.

Рассмотрим два типа инверсных конгруентных генераторов:

$$Z_{n+1} \equiv A y_n^{-1} + 1 \,(mod\ p)\,, \tag{3}$$

где Z_n^{-1} определяется сравнением $Z_n \cdot Z_n^{-1} \equiv 1 \,(mod\ p)$, если$(Z_n, p) = 1$ и $Z_n^{-1} = 0$, если $Z_n = 0$.

$$y_{n+1} \equiv a y_n^{-1} + b \,(mod\ p^m)\,, \tag{4}$$

где $y_n \cdot y_n^{-1} \equiv 1 \,(mod\ p^m)$, $m \geq 2$.

Известно, что условие (i) обеспечивает существование периодической последовательности $\{y_n\}$ периода p, сгенерированной генератором (3) при любом инициальном значении z_0, а последовательность $\{y_n\}$, порожденная генератором (4), имеет максимально возможный период $2p^{m-1}$, если $(y_0, p) = 1, y_0 \not\equiv a \,(mod\ p)$ и выполнены условия (ii).

В дальнейшем считаем, что для генераторов типа (3) числа $A_i \in Z_{p^i}^*$ удовлетворяют условию (i) для каждого $i = 1, ..., r_0$, причем соответствующие инициальные значения $z_0^{(i)}$ берутся равными $1 \,(mod\ p_i)$, а для генераторов типа (4) определяющие параметры $a_i, b_i, i = r_0 + 1, ..., r$ удовлетворяют условию (ii).

Пусть $c_i \in Z_{p_i}^*$, $i = 1, ..., r_0$.

Легко проверить, что последовательности $\left\{z_n^{(i)}\right\}, z_0^{(i)} = 1$, сгенерированные рекурсией типа (3) с $p = p_i$, $i = 1, ..., r_0$, порождают последовательности $\left\{y_n^{(i)}\right\}$, $y_0^{(i)} = c_i z_0^{(i)}$, которые удовлетворяют рекурсии

$$y_{n+1}^{(i)} \equiv c_i^2 A_i (y_n^{(i)})^{-1} + c_i (mod\ p_i), y_0^{(i)} = c_i, i = 1, ..., r_0. \qquad (iii)$$

Для $r_0 < i \leq r$ мы рассматриваем последовательности, порожденные генераторами типа (4) с инициальными значениями $c_i \in Z^*_{p_i^{m_i}}$ и генерируем поток инверсных конгруентных псевдослучайных чисел $\{x_n\}$ в интервале [0,1), полагая

$$x_n \equiv x_1^{(1)} + ... + x_n^{(r)} (mod\ 1), \quad n = 0, 1, 2, ..., \qquad (5)$$

где $x_n^{(i)} = \frac{y_n^{(i)}}{p^{m_i}}, \quad i = 1, ..., r_0, r_0 + 1, ..., r.$

Поскольку все последовательности $\left\{y_n^{(i)}\right\}$ являются чисто периодическими со взаимно простыми периодами, то последовательность $\{x_n\}$ является чисто периодической с периодом
$M = 2^r p_1 ... p_{r_0} p_{r_1}^{m_1 - 1} ... p_r^{m_r - 1}$, где $r_1 = r - r_0$.

Построенную последовательность $\{x_n\}$, n=0,1,... будем называть обобщенной составной последовательностью ПСЧ. Большой период этой последовательности достигается за счет выбора определенного количества различных простых чисел и роста показателей простых при $i > r_0$. Дополнительным достоинством последовательности $\{x_n\}$ является возможность использования r параллельных процессоров.

Свойства равнораспределенности и непредсказуемости $\{x_n\}$ мы будем исследовать в среднем по инициальным значениям с помощью оценок соответствующих дискрепансий s-мерных точек, s=1,2,... .

1. Вспомогательные утверждения

Рассмотрим последовательность s-мерных точек $\{t_n\}$, n=0,1,..., $t_n \in [0,1)^s$ и обозначим через $D_N^{(s)}(t_0, t_1, ..., t_{N-1}) = D_N^{(s)}$ функцию уклонения (дискрепансию), определяемую равенством:

$$D_N^{(s)}(t_0, ..., t_{N-1}) := \sup_{\Delta \subset [0,1)^s} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

где супремум берется по всем параллелепипедам Δ из s-мерного единичного гиперкуба $[0,1)^s$, $A_N(\Delta)$ — число точек $t_0, t_1, ..., t_{N-1}$, попавших в Δ, а $|\Delta|$ — объем параллелепипеда Δ.

Пусть $q \geq 2$ и $k \geq 1$ — натуральные числа, и пусть $C_k(q)$ обозначает множество точек $(h_1, ..., h_k) \in Z^k$ при условии $(h_1, ..., h_k) \neq (0, ..., 0)$ и $-\frac{1}{2}q < h_j \leq \frac{1}{2}q$ для всех j, $1 \leq j \leq k$.

Положим

$$r(h,q) = \begin{cases} q \sin\left(\frac{\pi |h|}{q}\right), & \text{для } h \in C_k(q), \\ 1, & \text{для h=0}, \end{cases}$$

и

$$r(\overline{h}, q) = \prod_{j=1}^{k} r(h_j, q), \text{ для } \overline{h} = (h_1, ..., h_k).$$

Лемма 1. [*см.* 3]. *Для любого делителя* d *числа* q, $d \neq q$, *имеем*

$$\sum_{\substack{\overline{h}\in C_k(q)\\ \overline{h}\equiv 0(mod\ d)}} \left(r\left(\overline{h},q\right)\right)^{-1} < \frac{1}{d}\left(\frac{2}{\pi}\log q + \frac{7}{5}\right)^k. \tag{6}$$

Следующие две леммы доказаны Нидеррайтером ([2], [3]).

Лемма 2. *Пусть* $N \geq 1$ *и* $q \geq 2$ — *натуральные* $y_n = \{0,1,\ldots,q-1\}^s$, $t_n = \frac{1}{q}y_n$, $n = 0,1,...,N-1$. *Тогда*

$$D_N^{(s)}(t_0,t_1,...,t_{N-1}) \leq \frac{s}{q} + \frac{1}{N}\sum_{\overline{h}\in C_k(q)} \left(r(\overline{h},q)\right)^{-1} \left|\sum_{n=0}^{N-1} e(\overline{h}\cdot t_n)\right|, \tag{7}$$

где $\overline{h}\cdot t_n$ — *скалярное произведение векторов* $\overline{h}$ *и* t_n.

Лемма 3. *Пусть* $\overline{h}$ — *ненулевая точка из* Z_n^s, l — *число ненулевых координат* $\overline{h}$. *Тогда для любой последовательности точек* $t_0,t_1,...,t_{N-1} \in (0,1]^s$ *справедлива оценка*

$$D_N^{(s)}(t_0,t_1,...,t_{N-1}) \geq \frac{\pi}{2N\left((\pi+1)^l-1\right)\prod_{j=1}^s max(1,|h_j|)} \left|\sum_{n=0}^{N-1} e(\overline{h}\cdot t_n)\right|. \tag{8}$$

Пусть последовательность $\left\{y_n^{(i)}\right\}$, $n \geq 0$, порождена рекуррентным соотношением

$$y_{n+1}^{(i)} \equiv c_i^2 A_i (y_n^{(i)})^{-1} + c_i (mod\ p_i), (y_i^0 = c_i, i = 1,...,r_0).$$

Построим последовательность $Y_{n,i}^{(s)} = \left(y_{sn}^{(i)}, y_{sn+1}^{(i)}, ..., y_{sn+s-1}^{(i)}\right)$.

Мы видели выше, что если многочлены $x^2 - x - A_i$ примитивны над F_{p_i}, то период $\left\{y_n^{(i)}\right\}$ равен p_i для каждого $i = 1,...,r_0$. Значит, и период $Y_{n,i}^{(s)}$ равен p_i.

Напомним, что мы обозначили $y_n^{(i)} \equiv c_i z_n^{(i)} \equiv y_0^{(i)} z_n^{(i)} (mod\ p_i)$.

Лемма 4. *Пусть* $h \in Z^s$ *и пусть* J — *подмножество множества* $\{1,...,r_0\}$, *такое, что для каждого* $j \in J$ *имеем* $h \equiv 0(mod\ p_j)$. *Тогда для каждого* $N \leq$ $\leq p_1...p_{r_0}$ *имеет место неравенство*

$$\sum_{y_0^{(1)}\in Z_{p_1}^*}\ \dots\ \sum_{y_0^{(r_0)}\in Z_{p_{r_0}}^*}\left|\sum_{n=0}^{N-1} e\left(\sum_{j=1}^{r_0}\frac{h\cdot Y_{n,j}^{(s)}}{p_j}\right)\right| \le$$
$$\le \sqrt{N\prod_{i=1}^{r_0}(p_i-1)}\cdot\prod_{i\in J}p_i\sqrt{\prod_{\substack{i\in 1\\ i\notin J}}^{r_0}(2s(p_i-1)+1)}. \tag{9}$$

Доказательство.
Обозначим оцениваемую сумму через S. В силу неравенства Коши–Шварца:

$$|S|^2 \le \sum_{\substack{y_0^{(i)}\in Z_{p_i}^*\\ i=1,\dots,r_0}} 1\cdot \sum_{\substack{y_0^{(i)}\in Z_{p_i}^*\\ i=1,\dots,r_0}}\left|\sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r_0}\frac{y_0^{(i)}\cdot h\cdot z_{n,i}}{p_i}\right)\right|^2 =$$

$$=\prod_{i=1}^{r_0}(p_i-1)\sum_{k,l=0}^{N-1}\sum_{\substack{y_0^{(i)}\in Z_{p_i}^*\\ i=1,\dots,r_0}} e\left(\sum_{i=1}^{r_0}\frac{y_0^{(i)}\cdot h\cdot(z_{k,i}-z_{l,i})}{p_i}\right) =$$

$$=\prod_{i=1}^{r_0}(p_i-1)\sum_{k,l=0}^{N-1}\sum_{\substack{y_0^{(i)}\in Z_{p_i}^*\\ i=1,\dots,r_0}}\prod_{i=1}^{r_0}\frac{e(y_0^{(i)}\cdot h(\dots))}{p_i} \le$$

$$\le\prod_{i=1}^{r_0}(p_i-1)\cdot\sum_{k,l=0}^{N-1}\prod_{i=1}^{r_0}\left|\sum_{y_0\in Z_{p_i}^*}\frac{e(y_0\cdot h\cdot(z_{k,i}-z_{l,i}))}{p_i}\right|. \tag{10}$$

Далее, имеем для каждого $i=1,\dots,r_0$ и всех k,l, $0\le k,n\le N-1$, мы имеем

$$\sum_{y_0\in Z_{p_i}^*}\frac{e(y_0h(z_{k,i}-z_{l,i}))}{p_i}=\begin{cases} p_i-1\ , & \text{если } h\cdot(z_{k,i}-z_{l,i})\equiv 0(mod\ p_i),\\ -1\ , & \text{если } h\cdot(z_{k,i}-z_{l,i})\not\equiv 0(mod\ p_i).\end{cases}$$

Следовательно, из (10) мы получаем

$$|S|^2\le\sum_{k,l=0}^{N-1}\prod_{\substack{i=1\\ h\cdot(z_{k,i}-z_{l,i})\equiv 0(mod\ p_i)}}(p_i-1)=$$
$$=\sum_{I\subset\{1,\dots,r_0\}}\sum_{k,l=0}^{N-1}\prod_{\substack{i\in I\\ h\cdot(z_{k,i}-z_{l,i})\equiv 0(mod\ p_i),i\in I\\ h\cdot(z_{k,i}-z_{l,i})\not\equiv 0(mod\ p_i),i\notin I}}(p_i-1). \tag{11}$$

Выражение справа в последнем соотношении означает, что для каждого подмножества

$I \subset \{1, ..., r_0\}$ слагаемое, соответствующее паре (k,l), есть произведение чисел $(p_i - 1), i \in I$, если для каждого $i \in I$ имеем $h \cdot (z_{k,i} - z_{l,i}) \equiv 0(mod\ p_i)$ и для каждого $i \notin I$ имеем $h \cdot (z_{k,i} - z_{l,i}) \not\equiv 0(mod\ p_i)$.

Зафиксируем l, $0 \leq l \leq N - 1$. Тогда для каждого $h \in Z^s$ нас интересует количество тех k, для которых

$$h \cdot z_{k,l} \equiv h_0(mod\ p_i), \tag{12}$$

где $h_0 = h \cdot z_{l,i}(mod\ p_i), i \notin J$.

Мы имеем:

$$h \cdot z_{k,l} = h_1 z_k^{(i)} + h_2 z_{k+1}^{(i)} + ... + h_s z_{k+s-1}^{(i)}.$$

Из сравнения, определяющего z_{n+1} через z_n, видно, что если $z_{k,i}, ..., z_{k+s-2,i} \not\equiv \not\equiv 0(mod\ p_i)$, то мы можем представить все $z_{k+t,i}$ через $z_{k,i}$ в виде $z_{k+t,i} = = \dfrac{a_t z_{n,i} + b_t}{c_t z_{n,i} + d_t}(mod\ p_i)$. И тогда условие (12) превращается в сравнение $P(z_k) \equiv \equiv 0(mod\ p_i)$, где $P(u)$ — многочлен степени $\leq s$ относительно u, так что рассматриваемое сравнение имеет не более s решений. Случаев, когда среди первых $s - 1$ компонент набора $(z_{k,i}, ..., z_{k+s-1,i})$ имеется нулевая, не более $s - 1$, так как каждый в наборе нуль однозначно определяет весь набор (поскольку период наших последовательностей равен p_i). Этим показано, что сравнение (12) может выполняться не более $2s - 1$ раз, если $i \notin J$.

Поэтому получаем

$$|S'|^2 \leq N p_1 ... p_{r_0} \sum_{I \subset \{1,...,r_0\}} \sum_{i \in I/J} (2s-1) \frac{1}{p_i} \prod_{i \in I} (p_i - 1) =$$

$$= N \prod_{i \in J} p_i^2 \prod_{\substack{i=1 \\ i \notin J}}^{r_0} \left[\left(\frac{(2s-1)(p_i-1)}{p_i} + 1 \right) p_i \right] = N \prod_{i \in J} p_i^2 \prod_{\substack{i=1 \\ i \notin J}}^{r_0} (2s(p_i - 1) + 1).$$

Отсюда следует утверждение леммы.

Лемма 5. *Пусть последовательность $\{y_n\}$, n=0,1,... определена рекурсией (4), причем (a,p)=1, $b = b_0 p$, $(b_0, p) = 1$, $(y_0, p) = 1$. Тогда справедливы следующие сравнения по модулю p^m:*

$$y_n = \frac{A_0^{(n)} + A_1^{(n)} y_0}{B_0^{(n)} + B_1^{(n)} y_0}, \qquad n = 1, 2, ...,$$

где

$$\begin{cases} A_0^{(2k)} = k a^k b + \overline{A}_0^{(2k)} b^3, & A_1^{(2k)} = a^k + k \overline{A}_1^{(2k)} b^2; \\ B_0^{(2k)} = a^k + \overline{B}_0^{(2k)} b^2, & B_1^{(2k)} = k a^{k-1} b + \overline{B}_1^{(2k)} b^3; \end{cases}$$

$$\begin{cases} B_0^{(2k+1)} = k a^{k+1} b + \overline{B}_0^{(2k+1)} b^3, & B_1^{(2k+1)} = a^k + k \overline{B}_1^{(2k+1)} b^2; \\ A_0^{(2k+1)} = a^{k+1} + \overline{A}_0^{(2k+1)} b^2, & A_1^{(2k+1)} = (k+1) a^k b + \overline{A}_1^{(2k+1)} b^3; \end{cases}$$

$\overline{A}_i^{(2k)}$, $\overline{B}_i^{(2k)}$, $\overline{A}_i^{(2k+1)}$, $\overline{B}_i^{(2k+1)}$, *i=1,2,...* — *многочлены от k с целыми коэффициентами.*

Доказательство.
Рассмотрим две матрицы:

$$A = \begin{pmatrix} a+b^2 & ab \\ b & a \end{pmatrix}, A_1 = \begin{pmatrix} a^{-1}b^2 & b \\ a^{-1}b & 0 \end{pmatrix}.$$

Очевидно,

$$A = a(E + A_1), \quad A_1^s \equiv O(mod\ p^s),\ (\text{s=1,2,...}),$$

где — единичная матрица.
Кроме того,

$$A^k \equiv a^k(E + kA_1 + \frac{k(k-1)}{2}A_1^2 + ...)(mod\ p^m).$$

Теперь, предполагая верным утверждение леммы для номера k и вычисляя y_{k+1}, y_{k+2} по рекурсии (4), мы простыми вычислениями приходим к утверждению леммы.

Следствие 1. *Существуют многочлены* $G_i(u)$, $i = 0,1,2,3$; *многочлены* $H_0(u), H_1(u), H_{-1}(u), H_{-2}(u)$ *и* $G(u,v), H(u,v)$ *с целыми коэффициентами, такие, что*

$$\begin{aligned} y_{2k} \equiv &\left(kb - \frac{k(k^2-1)}{2}a^{-1}b^3 + b^4G_0(k)\right) + \left(1 + p^4G_1(k)\right)y_0 + \\ &+ \left(-ka^{-1}b + (2^{-1}\cdot 3k^3 + 2^{-1}k)a^{-2}b^3 + b^4G_2(k)\right)y_0^2 + \\ &+ \left(k^2a^{-2}b^2 + p^4G_3(k)\right)y_0^3 + b^4G(k,y_0)y_0^4(mod\ p^m); \\ y_{2k+1} \equiv &\left((k+1)b + k(k-1)a^{-1}b^3 + b^4H_0(k)\right) + \\ &+ b^4H_1(k)y_0 + \left(a - 2k^2b^2 + b^4H_{-1}(k)\right)y_0^{-1} + \\ &+ (-kab + b^3H_{-2}(k))y_0^{-2} + b^4H(k,y_0^{-1})y_0^{-3}(mod\ p^m), \end{aligned} \tag{13}$$

где $a^{-1}, y_0^{-1}, 2^{-1}$ *рассматриваются как мультипликативные обратные к* $a, y_0, 2$ *(соответственно) по mod* p^m.

Следствие 2. *Существуют многочлены* $C_1(u)$, $C_2(u)$, $C_3(u,v)$, $D_1(u,v)$, $D_2(u,v)$, $D(u,v,w)$ *с целыми коэффициентами такие, что*

$$\begin{aligned} y_{2k} \equiv &\ y_0 + (b(1 - y_0^2a^{-1}) + 2a^{-1}b^3(a + y_0^3) + b^3C_1(y_0))k + \\ &+ (-a^{-1}b^2y_0 + b^3(y_0))k^2 + b^3C_3(y_0,k)k^3(mod\ p^m); \\ y_{2k+1} = &\ (ay_0^{-1} + b) + b(1 - ay_0^{-2} + D_1(y_0,y_0^{-1}))k + \\ &+ b^3(D_3(y_0,y_0^{-1})k^2 + D(y_0,y_0^{-1},k)k^3). \end{aligned} \tag{14}$$

Доказательства следствий 1 и 2 легко получить из леммы 5, если учесть, что

$(1+pz)^{-1} \equiv 1 - pz + p^2z^2 - ...(mod\ p^m)$.

Следствие 3. *Пусть τ — наименьшая длина периода последовательности $\{y_n\}$, порожденной рекуррентным сравнением (4). Тогда*

(i) $\tau = 2p^{m-1}$, *если* $y_0^2 \not\equiv a(mod\ p)$;

(ii) $\tau = 2p^{m-1-\delta}$, *если* $a - y_0^2 \equiv 0(mod\ p^\delta), a - y_0^2 \not\equiv 0(mod\ p^{\delta+1})$ *и* $\delta < 3$;

(iii) $\tau < 2p^{m-1-\delta}$ *в остальных случаях.*

2. Оценки тригонометрических сумм на последовательности ПСЧ

Пусть $h \in N$, $(h, p^m) = p^{m_0}$. Определим тригонометрическую сумму для неотрицательных целых l и k.

$$\sigma_{k,l}(h, p^m) = \sigma_{k,l} := \sum_{y \in Z^*_{p^m}} e\left(\frac{h(\omega_k - \omega_l)}{p^m}\right).$$

Теорема 1. *Пусть $k - l \equiv 0(p^\kappa), k - l \not\equiv 0(p^{\kappa+1})$. Тогда справедлива оценка*

$$|\sigma_{k,l}| \le \begin{cases} 2p^{\frac{m+m_0}{2}}, & \text{если } k \not\equiv l(mod\ 2), \\ p^{m-1}(p-1), & \text{если } k \equiv l(mod\ 2), \kappa + m_0 \ge m-1; \\ 2p^{\frac{m+m_0+\kappa+1}{2}}, & \text{если } k \equiv l(mod\ 2), \kappa + m_0 + 1 < m. \end{cases} \quad (15)$$

Доказательство.

Пусть сначала k и l — числа одинаковой четности. В этом случае следствие 1 показывает, что сумма $\sigma_{k,l}$ имеет вид

$$\sum_0 = \sum_{y_0 \in Z^*_{p^m}} e^{2\pi i h \frac{A_0 + A_1 y_0 + B_1 y_0^{-1} + p^2 F(y_0, y_0^{-1})}{p^m}},$$

где A_0, A_1, B_1 — целые числа, зависящие от k и l, а $F(u,v)$ — многочлен с целыми коэффициентами.

Сумма $\sum\limits_0$ оценивается аналогично классической сумме Клостермана $2p^{\frac{m}{2}}\sqrt{HOD(hA_1, hB_1, p^m)} = 2p^{\frac{m+m_0}{2}}$.

Для $k \equiv l(mod\ 2)$ сумма $\sigma_{k,l}$ сводится к сумме одного из двух следующих видов:

$$\sum_0^{(1)} = \sum_{y_0 \in Z^*_{p^m}} e^{2\pi i h \frac{A_0 + p^4(k-l)A_1 y_0 + p(k-l)A_2 y_0^2 + p^2(k-l)F(y_0)y_0^3}{p^m}}, \quad (16)$$

если $k \equiv l \equiv 0(mod\ 2)$ или

$$\sum_0^{(2)} = \sum_{y_0 \in Z^*_{p^m}} e^{2\pi i h \frac{A_0 + p^4(k-l)A_1 y_0 + p^2(k-l)A_2 y_0^{-1} + p(k-l)(-ab_0 + F(y_0^{-1})y_0^{-2}}{p^m}},$$

если $k \equiv l \equiv 1(mod\ 2)$.

Суммы $\sum_0^{(1)}$ и $\sum_0^{(2)}$ сводятся к оценкам классических сумм Гаусса и мы получаем после простых вычислений оценку:

$$\left| \sum_0^{(i)} \right| \leq 2p^{\frac{m + m_0 + \kappa + 1}{2}}, \tag{17}$$

если $m_0 + \kappa + 1 < m$, а иначе мы оцениваем эти суммы тривиально по числу слагаемых, т. е. $\varphi(p^m)$.

Теорема доказана.

Пусть $h \in N$, $(h, p^m) = p^\delta$, и пусть τ- период последовательности $\{y_n\}$, порожденной рекурсией (4) и инициальным значением y_0. В этом случае мы имеем:

Теорема 2. *Для каждого N,* $p^{\frac{m-\delta-1}{2m^{-\frac{1}{2}}}} \leq N \leq \tau$ *справедливо неравенство:*

$$\left|\overline{S}_N(h)\right| \leq 3Np^{-\frac{m-\delta-1}{4}} + m^{\frac{1}{2}} N^{\frac{1}{2}}.$$

Доказательство. Неравенство Коши–Шварца дает:

$$\left|\overline{S}_N(h)\right|^2 \leq \frac{1}{\varphi(p^m)} \sum_{y_0} |S_N(h, y_0)|^2 = \frac{1}{\varphi(p^m)} \sum_{k,l=0}^{N-1} \sum_{y_0 \in Z^*_{p^m}} e^{2\pi i \frac{h(y_k - y_l)}{p^m}} \leq$$

$$\leq \frac{1}{\varphi(p^m)} \sum_{t=0}^{m} \sum_{\substack{k,l=0 \\ k \equiv l(mod\ p^t)}}^{N-1} |\sigma_{k,l}(h)|.$$

Теперь, в силу теоремы 1, выводим

$$\left|\overline{S}_N(h)\right|^2 \leq \frac{1}{\varphi(p^m)} \left(2 \sum_{s=0}^{m-\delta-1} p^{\frac{m+\delta+1+s}{2}} \sum_{\substack{k,l \leq N \\ k \equiv l(mod\ p^s)}} 1 + \sum_{s=m+\delta+1}^{m} p^m \sum_{\substack{k,l \leq N \\ k \equiv l(mod\ p^s)}} 1 \right) \leq$$

$$\leq \frac{N^2}{\varphi(p^m)} \left(2 \sum_{s \leq m-\delta} p^{\frac{m+\delta+1-s}{2}} + \sum_{s=m-\delta+1} p^m \left(p^{-s} + \frac{1}{N} \right) \right) \leq$$

$$\leq 3N^2 p^{-m}\left(p^{\frac{m+\delta+1}{2}}+p^{\delta+1}\right)+mN. \tag{18}$$

Таким образом, для каждого $N \leq \tau$ мы получаем

$\left|\overline{S}_N(h)\right| \leq \frac{5}{2}N\left(p^{-\frac{m-\delta-1}{4}}+p^{-\frac{m-\delta-1}{2}}\right)+m^{1/2}N^{1/2} \leq 3Np^{-\frac{m-\delta-1}{4}}+m^{1/2}N^{1/2}.$

Теорема доказана.

3. Оценка дискрепансии. Основными требованиями к последовательности ПСЧ являются требования равнораспределенности и непредсказуемости. Для проверки выполнимости этих требований обычно используют различные тесты. Для равнораспределенности последовательности ПСЧ $\{x_n\}, n \geq 0$, достаточно, чтобы дискрепансия $D_N^{(1)}(x_0, x_1, ..., x_{N-1})$ оценивалась как o(1) при росте N и τ, $N \leq \tau$.

Из последовательности $\{x_n\}, n \geq 0$, можно построить две последовательности s-мерных точек $\left\{X_n^{(s)}\right\}$:

(i) $X_n^{(s)} = (x_n, x_{n+1}, ..., x_{n+s-1})$, n=0,1,... — последовательность перекрывающихся точек;

(ii) $X_n^{(s)} = (x_{ns}, x_{ns+1}, ..., x_{ns+s-1})$, n=0,1,... — последовательность неперекрывающихся точек.

Мы будем говорить, что последовательность ПСЧ $\{x_n\}, n \geq 0$ проходит сериальный тест на непредсказуемость, если перекрывающиеся (или неперекрывающиеся) последовательности $\{X_n^s\}, n \geq 0$ равномерно распределены для s=2,3,....

Теорема 3. *Пусть* $M = \prod_{i=1}^{r_0} p_i \prod_{i=r_0+1}^{r} p_i^{m_i} = M_0 M_1$, *и пусть* $\{x_n\}, n \geq 0$ — *обобщенная составная последовательность ПСЧ, порожденная генераторами (3) и (4) с условиями (i), (ii) в (2). Пусть* τ — *период этой последовательности. Тогда для любого* s, $1 \leq s < min(p_1, ..., p_r)$ *и* $1 \leq N \leq \tau$ *имеем*

$$\begin{aligned}\overline{D}_N^{(s)} = \frac{1}{\varphi(M)} \sum_{y_0^{(i)}, i=1,...,r} D_N^s\left(\left\{x_n^{(s)}\right\}; y_0^{(1)}, ..., y_0^{(r)}\right) \leq \\ \leq \sqrt{s \cdot 2^r} N^{-\frac{1}{2}} M_1^{\frac{1}{4}+\epsilon}\left(\frac{2}{\pi} log M + \frac{7}{5}\right)^s,\end{aligned} \tag{19}$$

где $D_N^s\left(\left\{x_n^{(s)}\right\}; y_0^{(1)}, ..., y_0^{(r)}\right)$ *обозначает дискрепансию последовательности* $X_0^{(s)}, ..., X_{N-1}^{(s)}$, *соответствующую набору инициальных значений последовательностей* $\left\{y_n^{(i)}\right\}, i = 1, ..., r$.

Доказательство. Применим лемму 2 с q=M. Мы имеем

$$D^{(s)}_{N, y_0^{(1)}, ..., y_0^{(r)}} \leq$$

$$\leq \frac{s}{M} + \frac{1}{N} \sum_{h \in C_s(M)} r(h, M)^{-1} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r_0} \frac{h \cdot Y_n^{(i)}}{p_i} + \sum_{i=r_0+1}^{r} \frac{h \cdot Y_n^{(i)}}{p_i^{m_i}}\right)\right|, \tag{20}$$

где $Y_n^{(i)}$ — s-мерные точки, порожденные генераторами (3) (для $1 \le i \le r_0$) и (4) (для $r_0+1 \le i \le r$) с инициальными значениями $y_0^{(i)}, i = 1, ..., r$.

Обозначим сумму под модулем справа через $S(y_0^{(1)}, ..., y_0^{(r)})$.

Поэтому среднее значение дискрепансии $D^{(s)}_{N, y_0^{(1)}, ..., y_0^{(r)}}$ по всем допустимым значениям $y_0^{(i)}$ удовлетворяет неравенству (в силу неравенства Коши–Шварца):

$$\overline{D}_N^{(s)} \le \frac{s}{M} + \frac{1}{N} \sum_{h \in C_s(M)} r(h, M)^{-1} \frac{1}{\varphi(M)} \sum_{\substack{y_0^{(i)}, \\ i=1,...,r}} S(y_0^{(1)}, ..., y_0^{(r)}). \tag{21}$$

Тогда

$$\left(\sum_{\substack{y_0^{(i)}, \\ i=1,...,r}} S(y_0^{(1)}, ..., y_0^{(r)}) \right)^2 \le$$

$$\le \varphi(M) \sum_{k,l=0}^{N-1} \prod_{i=0}^{r_0} \sum_{y_0^{(i)}} e\left(\frac{h \cdot (Y_k^{(i)} - Y_l^{(i)})}{p_i} \right) \cdot \prod_{i=r_0+1}^{r} \sum_{y_0^{(i)}} e\left(\frac{h \cdot (Y_k^{(i)} - Y_l^{(i)})}{p_i^{m_i}} \right) = \tag{22}$$

$$= \varphi(M) \sum_{k,l=0}^{N-1} \prod_{1} \cdot \prod_{2}.$$

Обозначим через J_0 подмножество в $\{1, ..., r_0\}$, такое, что для каждого $j \in J_0$ имеем $h \equiv 0 (mod\, p_j)$, и, аналогично, через $J(\alpha_1, ..., \alpha_{r_1}), r_1 = r - r_0$, подмножество в $\{r_0+1, ..., r\}$ такое, что для каждого $j \in J_1$ имеем $h \equiv 0 (mod\, p_j^{\alpha_j})$, где $0 \le \alpha_j \le$ $\le m_j$.

Тогда, используя лемму 4 и рассуждение теоремы 1, получаем

$$\left(\sum_{\substack{y_0^{(i)}, \\ i=1,...,r}} S(y_0^{(1)}, ..., y_0^{(r)}) \right)^2 \le$$

$$\le \varphi(M) N \prod_{i=1}^{r_0} (p_i - 1) \prod_{i \in J_0} p_i \sum_{\substack{i=1 \\ i \notin J_0}}^{r_0} (2S(p_i - 1) + 1) \cdot \prod_{i=r_0+1}^{r} (2 p_i^{\frac{m_i}{2}}) \cdot \tag{23}$$

$$\cdot \sum_{\alpha_1, ..., \alpha_{r_1}} \prod_{j \in J_1(\alpha_1, ..., \alpha_r)} p_j^{\frac{\alpha_j}{2}}.$$

Теперь из (21)–(23) и леммы (1) после простых вычислений получаем утверждение теоремы.

Теорема доказана.

Заключение. В заключение отметим, что лемма 3 позволяет получить и нижнюю оценку для $\overline{D}_N^{(s)}$:

$$\overline{D}_N^{(s)} \geq \sqrt{2^r} N^{-\frac{1}{2}} M_1^{\frac{1}{4}}. \tag{24}$$

Для этого достаточно соединить рассуждения из работ [3], [4].

Сравнение оценок (19) и (24) показывает, что найденная оценка дискрепансии для обобщенной составной последовательности неперекрывающихся s-мерных псевдослучайных точек $X_n^{(s)}$ может быть улучшена не более чем на множитель M^{ϵ}.

1. **Eichenauer-Herrmann J.** Compound inversive congruential pseudorandom numbers: an average case analysis, Math. Comput. [text] / J. Eichenauer-Herrmann, F. E. Emmerich. – 1996. – V. 65. – P. 215–225.
2. **Niederraiter H.** Quasi-Monte Carlo methods and pseudorandom numbers, Bull. Amer. Math. Soc. [text] / H. Niederraiter. – 1978. – V. 84. – P. 957–1041.
3. **Niederraiter H.** Lower bounds for the discrepancy of inversive congruential pseudorandom numbers, Math. Comp. [text] / H. Niederraiter. – 1990. – V. 55. – P. 277–287.
4. **Varbanets P.** Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus, Voronoi's Impact on modern science, Proc. 4th Intern. Conf. Analytic Numb. Theory and Spatial Tessllations, Book 4 [text] / P. Varbanets, S. Varbanets. – 2008. – No 1. – P. 112–130.