В. А. Орлов, М. В. Карташова

О ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ НА ОСНОВЕ ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ

Как известно, алгоритмы шифрования и расшифровывания реализуют взаимно однозначные отображения — перестановки. В шифрах гаммирования используются псевдослучайные последовательности (ПСП).

Одним из простых способов получения перестановок и ПСП является использование преобразования $y = ax + b \pmod m$, которое называют *линейным*. Здесь $x, y, a, b \in \{0, 1, 2, ..., m-1\}$ и y равен остатку от деления $ax + b$ на m. Число m называется *модулем* преобразования.

Относительно параметров линейного преобразования рассматривают две проблемы, первой из которых является взаимная однозначность. Эта проблема решается просто: преобразование $y = ax + b \pmod m$ взаимнооднозначно тогда и только тогда, когда числа a и m являются взаимно простыми (их наибольший общий делитель (НОД(a, m)) равен 1). Если $\text{НОД}(a, m) = d > 1$, то $y(0) = y\left(\frac{m}{d}\right)$ и преобразование не является перестановкой.

Таким образом, при $\text{НОД}(a, m) = 1$ линейное преобразование является перестановкой m элементов. В дальнейшем будем рассматривать такие перестановки и будем называть их *линейными*.

Любую перестановку можно представить в виде «чистых» (не имеющих предпериодов) циклов. При построении ПСП предпочтение отдают перестановкам, имеющим *один* цикл. Таким образом, возникает вторая задача: при каких параметрах линейной перестановки она является *одноцикловой*?

Представление $m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, где $p_1, p_2 \dots, p_k$ — различные простые числа, называется каноническим разложением числа m.

Ввиду особенностей для нас простого числа 2 будем каноническое разложение модуля m записывать в виде $m = 2^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$, где $s_1 \geq 0$, $p_2, \dots, p_k$ — простые *нечетные* числа.

Справедливо следующее утверждение.

Теорема 1. *Пусть* $m = 2^{s_1} p_2^{s_2} \dots p_k^{s_k}$. *Линейная перестановка* $y = ax + b \pmod m$ *является одноцикловой тогда и только тогда, когда*

1) $\text{НОД}(a, m) = \text{НОД}(b, m) = 1$;

2) *Если* $0 \leq s_1 \leq 1$, *то* $a \equiv 1 \pmod{p_2 \cdots p_k}$;

3) *Если* $s_1 \geq 2$, *то* $a \equiv 1 \pmod{4 p_2 \cdots p_k}$.

Доказательство теоремы 1 проведем с использованием *геометрических сумм*.

Сумму первых n членов геометрической прогрессии с *целым* знаменателем a и равным 1 первым членом будем называть *геометрической суммой* и обозначать через $gs(a, n)$. Таким образом,

$$gs(a, n) = 1 + a + a^2 + \dots + a^{n-1}.$$

Будем считать $gs(a, 0) = 0$.

Введение геометрических сумм обусловлено следующим.

Для выявления одноцикловости линейной перестановки достаточно рассмотреть цикл C_0, содержащий $c_0 = 0$, и случай $b = 1$. Нетрудно проверить, что в этом случае цикл состоит из элементов 0, $c_1 = 1$, $c_2 = 1 + a$, $c_3 = a(1 + a) + 1 = 1 + a + a^2, \dots$ Таким образом, $c_i = gs(a, i)$, $i \geq 0$. Для доказательства одноцикловости перестановки надо показать, что для любого i, $1 \leq i \leq m - 1$, $c_i \neq 0 \pmod m$.

При $b \neq 1$ для любого i справедливо соотношение $c_i = b \cdot gs(a,i)$. Если $\text{НОД}(b,m) = d > 1$, то цикл $C_{0,b}$ состоит из не более чем $\frac{m}{d}$ элементов, т. е. перестановка не является одноцикловой. При $\text{НОД}(b,m) = 1$ циклы $C_{0,b}$ и C_0 имеют одинаковое число элементов.

Рассмотрим свойства геометрических сумм.

Лемма 1. *Для любых натуральных* a, m *и* k

а) $gs(a,\ m\ +\ k) = gs(a,\ m) + a^m\, gs(a,\ k)$;

б) $gs(a, mk) = gs(a, m) \cdot gs(a^m, k)$.

Доказательство следует из легко проверяемых равенств

$1 + a + \ldots + a^{m+k-1} = 1 + a + \ldots + a^{m-1} + a^m(1 + a + a^2 + \ldots + a^{k-1})$,

$1 + a + \ldots + a^{mk-1} = (1 + a + \ldots + a^{m-1})(1 + a^m + a^{2m} + \ldots + a^{(k-1)m})$.

Последовательно применяя лемму 1 б), убеждаемся в том, что справедливо следующее утверждение.

Лемма 2. *Для любых* a, n, s

$$gs(a, n^s) = gs(a,n) \cdot gs(a^n, n) \cdots gs(a^{n^{s-1}}, n).$$

В дальнейшем через ρ будем обозначать простое *нечетное* число.

Лемма 3. *Если* $a \equiv 1 \pmod p$, *то*

$$gs(a,p) \equiv 0 \pmod p \text{ и } gs(a,p) \neq 0 \pmod{p^2}.$$

Доказательство следует из следующих соотношений

$$gs(a,p) = (1 + (1 + kp) + (1 + 2kp + K_2 p^2) + \ldots + (1 + (p-1)p + K_{p-2}p^2)) =$$
$$= (p + kp(1 + 2 + \ldots + p - 1) + K_{p-1}p^2) =$$
$$= p(1 + k\frac{p(p-1)}{2} + K_{p-1}p) = p(1 + K_p p) \quad .$$

Здесь k, K_i — целые числа.

Из свойства умножения сравнений следует, что *для любых* a, m и k *сравнения*

$a \equiv 1 \pmod m$ *и* $a^k \equiv 1 \pmod m$ *эквивалентны.* (1)

Отсюда и из лемм 2 и 3 следует

Лемма 4. *Если* $a \equiv 1 \pmod p$, *то для любого* $s \geq 1$

$$gs(a, p^s) \equiv 0 \pmod{p^s} \text{ и } gs(a, p^s) \neq 0 \pmod{p^{s+1}}.$$

Лемма 5. *Если* $a \equiv 1 \pmod p$ *и* $n \neq 0 \pmod p$, *то*

$$gs(a,n) \neq 0 \pmod p.$$

Доказательство следует из соотношения $gs(a,n) = (n + Np) \neq 0 \pmod p$, где N — целое число.

Перед доказательством последующих свойств геометрических сумм сформулируем известное утверждение (малая теорема Ферма):

если $\text{НОД}(a,p) = 1$, *то для любого простого числа* ρ

$$a^{p-1} \equiv 1 \pmod p. \quad (2)$$

Лемма 6. *Если* $a \neq 1 \pmod p$, *то*

$$gs(a,p) \equiv 1 \pmod p.$$

Доказательство следует из представления

$$gs(a,p) = 1 + a + \ldots + a^{p-1} = 1 + a\frac{a^{p-1} - 1}{a - 1}$$

и малой теоремы Ферма.

Лемма 7. *Если* $a \neq 1 \pmod p$ *и* $a \neq 0 \pmod p$, *то*

$$gs(a, p-1) \equiv 0 \pmod p.$$

Доказательство следует из представления $gs(a, p-1) = gs(a, p) - a^{p-1}$, леммы 6 и (2).

Рассмотрим теперь свойства геометрических сумм для модуля, являющегося степенью числа 2 (объявленные ранее особенности простого делителя 2).

Лемма 4a. *Если* $a \equiv 1 \pmod 4$, *то для любого* $s \geq 1$
$gs(a, 2^s) \equiv 0 \pmod{2^s}$ и $gs(a, 2^s) \neq 0 \pmod{2^{s+1}}$.

Доказательство. Из леммы 2 следует представление

$$gs(a, 2^s) = (1+a)(1+a^2)\cdots(1+a^{2^{s-1}}) .$$

Из условия леммы и (1) следует, что для любого n справедливо равенство $1 + a^n = 4k + 2 = 2(2k+1)$, т. е. $1 + a^n \equiv 0 \pmod 2$ и $1 + a^n \neq 0 \pmod 4$. Лемма доказана.

Степенью четности числа n назовем число s, такое, что $n = 2^s h$, где число h — нечетное. Заметим, что степень четности нечетного числа равна нулю.

Лемма 4b. *Если* $a \equiv 3 \pmod 4$, *то для любого* $s \geq 1$

$$gs(a, 2^s) \equiv 0 \pmod{2^{r+s-1}} \text{ и } gs(a, 2^s) \neq 0 \pmod{2^{r+s}},$$

где r — степень четности числа $1 + a$.

Доказательство аналогично доказательству леммы 4a с учетом легко проверяемого соотношения $(4k+3)^2 \equiv 1 \pmod 4$, из которого и из (1) следует справедливость для любого t сравнения $(4k+3)^{2t} \equiv 1 \pmod 4$. Отметим, что $r \geq 2$.

Взаимно простым числам m и a, $0 < a < m$, следующим образом будем сопоставлять число $m(a)$. Пусть $2^{s_1} p_2^{s_2} \ldots p_k^{s_k}$ — каноническое разложение числа m.

Вначале определим двоичный набор $d(m,a) = (d_2, \ldots, d_k)$: d_i, $2 \leq i \leq k$, полагаем равным 0, если $a \equiv 1 \pmod{p_i}$, и равным 1 в противном случае.

Если $0 \leq s_1 \leq 1$, то полагаем

$$m(a) = \prod_{i=2}^{k} (p_i - d_i)^{s_i} .$$

Если $s_1 \geq 2$ и $a \equiv 1 \pmod 4$, то полагаем

$$m(a) = 2^{s_1} \prod_{i=2}^{k} (p_i - d_i)^{s_i} .$$

Если $s_1 \geq 2$ и $a \equiv 3 \pmod 4$, то полагаем

$$m(a) = 2^{t} \prod_{i=2}^{k} (p_i - d_i)^{s_i} ,$$

где $t = s_1 - r$ при $(s_1 - r) \geq 1$, $t = 1$ в противном случае (здесь r — степень четности числа $1 + a$).

Нетрудно проверить, что при невыполнении условий 2) и 3) теоремы 1 имеет место неравенство $m(a) < m$.

Теорема 2. *Для любых* $m = 2^{s_1} p_2^{s_2} \ldots p_k^{s_k}$, $s_1 \geq 0$, *и* a

$$gs(a, m(a)) \equiv 0 \pmod m .$$

Доказательство.

Пусть $m_i = p_i^{s_i}$. Для любого i, $2 \leq i \leq k$, из лемм 7 и 1 б) получаем соотношения
$gs(a, m(a)) = gs(a, (p_i - d_i)^{s_i}) \cdot gs(a^{m_i}, m/m_i) \equiv 0 \pmod{p_i^{s_i}}$.

При $a \equiv 1 \pmod 4$ из леммы 4a получаем соотношение
$gs(a, m(a)) = gs(a, u) \cdot gs(a^u, m/u) \equiv 0 \pmod u$, где $u = 2^{s_1}$.

При $a \equiv 3 \pmod 4$ из леммы 4b получаем соотношение
$gs(a, m(a)) = gs(a, u) \cdot gs(a^u, m/u) \equiv 0 \pmod u$, где $u = 2^t$.

Отсюда, из взаимной простоты чисел $p_i^{s_i}, 1 \leq i \leq k$, и китайской теоремы об остатках следует справедливость теоремы 2.

Необходимость условий теоремы 1 следует из теоремы 2.

Докажем достаточность условий теоремы 1. Для этого покажем, что при выполнении условий 2) или 3) теоремы 1 для любого $n < m$ выполняется сравнение

$$gs(a,n) \neq 0 \pmod m.$$

Вначале рассмотрим случай $s_1 = 0$ или $s_1 \geq 2$. Пусть $R = \text{НОД}(n,m)$ и $R = 2^{t_1} p_2^{t_2} \cdots p_k^{t_k}$. Очевидно, что существует i, $1 \leq i \leq k$, такое, что $0 \leq t_i < s_i$. Пусть $n_i = p_i^{t_i}$. Число $T = \dfrac{n}{n_i}$ не делится на p_i. Из представления $gs(a,n) = gs(a,n_i) \cdot gs(a^{n_i},T)$ и лемм 4 и 5 следует сравнение $gs(a,n) \neq 0 \pmod{p_i^{s_i}}$, которое доказывает сравнение $gs(a,n) \neq 0 \pmod m$. Отметим, что при $t_i = 0$ лемма 4 не нужна. При $i = 1$ используем лемму 4а.

Рассмотрим теперь случай $s_1 = 1$. Поскольку $\text{НОД}(a,m) = 1$, для любого нечетного n $gs(a,n)$ — нечетно (сумма нечетного числа нечетных чисел), т. е. $gs(a,n) \neq 0 \pmod m$. Доказательство сравнения $gs(a,2n) \neq 0 \pmod m$ для любого $n, 1 \leq n \leq \dfrac{m-2}{2}$, аналогично доказательству случая $s_1 = 0$.

Теорема 1 доказана полностью.

ПСП $c_0, c_1, \ldots, c_n, \ldots$ на основе преобразования $y = ax + b \pmod m$ можно получать следующими способами.

1) Полагаем $c_i = ai + b \pmod m, 0 \leq i \leq m-1$. При этом разность соседних элементов ПСП равна a и ПСП не является случайной.

2) Выбираем c_0, $0 \leq c_0 \leq m-1$. Затем c_i, $i > 0$, полагаем равным $a \cdot c_{i-1} + b \pmod m$. Если преобразование $y = ax + b \pmod m$ является одноцикловой перестановкой, то ПСП имеет период максимально возможной длины m.

Таким образом, ПСП, построенная вторым способом, предпочтительнее.

ПСП с начальным значением c_0, полученную вторым способом из одноцикловой перестановки $y = ax + b \pmod m$, будем называть (m,a,b,c_0)-ЛПМП (линейной ПСП максимального периода).

Замечание. Из теоремы 1 следует, что если модуль m является числом, *свободным от квадратов* (все $s_i = 1$), то $a = 1$ и ЛПМП имеет вид $0, b, 2b, \ldots, (m-1)b$, т. е. не является случайной.

ЛПМП легко реализовать, но, зная m и три ее последовательные элемента, можно вычислить параметры a и b. Для этого решаем систему сравнений

$$\begin{cases} x_2 \equiv ax_1 + b \pmod m, \\ x_3 \equiv ax_2 + b \pmod m \end{cases}$$

относительно a и b. Получаем

$$\begin{cases} a = (x_3 - x_2)(x_2 - x_1)^{-1} \pmod m, \\ b = x_2 - ax_1 \pmod m. \end{cases}$$

Из соотношения

$$y = a(cx + d) + b = acx + ad + b \pmod m$$

следует, что суперпозиция (произведение) линейных перестановок является линейной перестановкой (из равенств $\text{НОД}(a,m) = \text{НОД}(c,m) = 1$ следует равенство $\text{НОД}(ac,m) = 1$).

Однако суперпозиция линейных одноцикловых перестановок может не быть одноцикловой перестановкой. Например, $a = b = d = 1$ и четный модуль m. Отметим, что суперпозиция линейных одноцикловых перестановок может быть и одноцикловой перестановкой. Например, $a = b = d = 1$ и нечетный модуль m.

Рассмотрим способ получения нелинейных перестановок и ПСП на основе линейных преобразований.

Преобразование $f: f(i) = c_i$, где c_i — i-й элемент (m,a,b,c_0)-ЛПМП, является перестановкой. Легко проверить, что при $a \neq 1$ эта перестановка нелинейна. Таким образом, из нетривиальной одноцикловой линейной перестановки получим m нелинейных перестановок.

Пусть $P_1 = c_0, c_1, ..., c_{m-1}$ является (m,a_1,b_1,c_0)-ЛПМП и пусть $h(x) = a_2x + b_2 \pmod m$ — перестановка. Переставим элементы P_1 в соответствии с $h(x)$, т. е. рассмотрим ПСП $P_2 = c_{h(0)}, c_{h(1)}, ..., c_{h(m-1)}$. Конечно, в тривиальном случае ($a_2 = 1$) P_2 является циклическим сдвигом P_1, т. е. $(m,a_1,b_1,c_{h(0)})$-ЛПМП.

Если НОД$(a_2,m) = t > 1$, то P_2 будет иметь период $\frac{m}{t} < m$ и не является ЛПМП. В дальнейшем будем полагать a_2 взаимно простым с m.

Покажем, что для выяснения вопроса о том, является ли P_2 ЛПМП, достаточно рассмотреть случай $c_0 = 0,\ b_1 = 1$.

Через (m,a,b)-ЛПМП будем обозначать (m,a,b,s)-ЛПМП при некотором s.

Нетрудно проверить справедливость следующего утверждения.

Лемма 8. *В любой (m,a,b)-ЛПМП D и в любом ее циклическом сдвиге отношение $k_i = \frac{d_{i+2} - d_{i+1}}{d_{i+1} - d_i} \pmod m,\ 0 \le i \le m-1$, и выражение $e_i = d_{i+1} - k_i \cdot d_i \pmod m$ не зависят от i.*

Отметим, что $k_i = a,\quad e_i = b$.

Справедливо и утверждение, обратное к лемме 8.

Лемма 9. *Если в ПСП D отношение $k_i = \frac{d_{i+2} - d_{i+1}}{d_{i+1} - d_i} \pmod m,\ 0 \le i \le m-1$, и выражение $e_i = d_{i+1} - k_i \cdot d_i \pmod m$ не зависят от i, то D является (m,k_i,e_i)-ЛПМП.*

При умножении всех элементов (m,a,b)-ЛПМП на любое взаимно простое с m число получим (m,a,b)-ЛПМП. Таким образом, полагаем $b_1 = 1$.

Если $c_0 \neq 0 \pmod m$, то существует j, такое, что $c_j = 0$. Следовательно, случай $c_0 \neq 0 \pmod m$ сводится к случаю $c_0 = 0$.

Из условия $b_1 = 1$ и $c_0 = 0$ получаем соотношение $c_i \equiv gs(a_1, i) \pmod m$.

Число a, удовлетворяющее условиям теоремы 1, будем называть *m-совместимым*.

Лемма 10. *Для любого m-совместимого a и любых r и s, таких, что $r \equiv s \pmod m$, справедливо сравнение*

$$gs(a,r) \equiv gs(a,s) \pmod m.$$

Доказательство следует из равенств

$$gs(a,r) = gs(a,s+tm) = gs(a,s) + a^s \cdot gs(a,tm) =$$
$$= (\text{теорема 1})\ gs(a,s) \pmod m.$$

Следующие равенства показывают соотношение соседних элементов последовательности P_2

$$c_{h(i+1)} = gs(a_1, a_2i + a_2 + b_2) = \ (\text{лемма 1а}))=$$
$$= gs(a_1, a_2) + a_1^{a_2} gs(a_1, a_2i + b_2) = a_1^{a_2} c_{h(i)} + c_{a_2}.$$

Из (1) следует, что $a_1^{a_2}$ является m-совместимым.

Таким образом, справедливо следующее утверждение.

Теорема 3. *Пусть $P_1 = c_0, c_1, ..., c_{m-1}$ — (m,a_1,b_1,c_0)-ЛПМП, пусть $h(x) = a_2x + b_2 \pmod m$ и пусть $P_2 = c_{h(0)}, c_{h(1)}, ..., c_{h(m-1)}$. Тогда для любых a_2 и b_2, таких, что НОД$(a_2,m) = 1$, P_2 является $(m,a_1^{a_2},c_{a_2})$-ЛПМП.*

Теперь будем переставлять элементы ЛПМП P_1 в соответствии с (m,a_2,b_2,h_0)-ЛПМП $H = h(0), h(1), ..., h(m-1)$, т. е. рассмотрим ПСП $P_2 = c_{h(0)}, c_{h(1)}, ..., c_{h(m-1)}$.

Вначале рассмотрим случай $m = p^n$, где p — простое число.

Ранее было показано, что для выяснения вопроса о том, является ли P_2 ЛПМП, достаточно рассматривать случай

$$c_0 = 0,\ b_1 = 1,\ h(0) = 0\ . \tag{3}$$

Известно следующее утверждение.

Для простого p *из сравнений* $a \equiv 1 \pmod p,\quad a \neq 1 \pmod{p^2}$ *следуют сравнения*

$$a^p \equiv 1 \pmod{p^2},\quad a^p \neq 1 \pmod{p^3}. \tag{4}$$

Применяя последовательно (4), получаем следующее утверждение.

Лемма 11. *Пусть* $a_1 \equiv 1 \pmod{p^u},\quad a_1 \neq 1 \pmod{p^{u+1}}$. *Тогда для любого натурального* v

$$a_1^{p^v} \equiv 1 \pmod{p^{u+v}},\quad a_1^{p^v} \neq 1 \pmod{p^{u+v+1}}.$$

Лемма 12. *Пусть*

$$a_1 \equiv 1 \pmod{p^u},\quad a_2 \equiv 1 \pmod{p^v},\ a_1 \neq 1 \pmod{p^{u+1}},\quad a_2 \neq 1 \pmod{p^{v+1}}\ .$$

Тогда $a_1^{a_2} \equiv a_1 \pmod{p^{u+v}},\quad a_1^{a_2} \neq a_1 \pmod{p^{u+v+1}}\ .$

Доказательство следует из леммы 11 и следующих равенств

$$a_1^{a_2} = a_1^{\,1+tp^v} = a_1(a_1^{p^v})^t = a_1(1+t_1p^{u+v})^t \equiv a_1 (\mathrm{mod}\ p^{u+v}).$$

Теперь докажем, что если $u+v \geq n$, то последовательность P_2 является ЛПМП. Для этого убедимся в том, что определенные ранее k_i и e_i, имеющие в нашем случае вид

$$k_i = \frac{c_{h(i+2)} - c_{h(i+1)}}{c_{h(i+1)} - c_{h(i)}} \pmod m,\ 0 \leq i \leq m-1,$$

$$e_i = c_{h(i+1)} - k_i \cdot c_{h(i)} \pmod m,$$

не зависят от i.

В нашем случае $c_i = gs(a_1, i)$. Следовательно, $c_i - c_j = a_1^{\,j} c_{i-j}$.

В нашем случае $h(i) = b_2 \cdot gs(a_2, i)$. Следовательно, $h(i+1) - h(i) = b_2 a_2^{\,i}$.

$$k_i = \frac{a_1^{\,h(i+1)} c_{h(i+2)-h(i+1)}}{a_1^{\,h(i)} c_{h(i+1)-h(i)}} = a_1^{\,h(i+1)-h(i)} \frac{c_{b_2 a_2^{\,i+1}}}{c_{b_2 a_2^{\,i}}} = a_1^{\,b_2 a_2^{\,i}} \frac{c_{b_2 a_2^{\,i+1}}}{c_{b_2 a_2^{\,i}}}.$$

Из леммы 12 получаем

$$a_1^{\,a_2^{\,i}} = \left(a_1^{\,a_2}\right)^{a_2^{\,i-1}} \equiv a_1^{\,a_2^{\,i-1}} \pmod{p^{u+v}} \equiv \ldots \equiv a_1 \pmod{p^{u+v}}.$$

Отсюда $a_1^{\,b_2 a_2^{\,i}} \equiv a_1^{\,b_2} \pmod{p^{u+v}}$.

Из леммы 1б получаем

$$\frac{c_{b_2 a_2^{\,i+1}}}{c_{b_2 a_2^{\,i}}} = \frac{gs(a_1, a_2) \cdot gs(a_1^{\,a_2}, b_2 a_2^{\,i})}{gs(a_1, b_2 a_2^{i})}\ .$$

Из леммы 12

$$a_1^{\,a_2} \equiv a_1 \pmod{p^{u+v}}.$$

Следовательно,

$$\frac{c_{b_2 a_2^{\,i+1}}}{c_{b_2 a_2^{\,i}}} \equiv gs(a_1, a_2) \pmod{p^{u+v}}\ .$$

Таким образом, при $u+v \geq n$ выражение $k_i \equiv a_1^{\,b_2} c_{a_2} \pmod m$ не зависит от i.

Покажем, что $d_i = c_{b_2}$, т. е. d_i также не зависит от i. Для этого докажем справедливость равенства

$$c_{h(i+1)} = k \cdot c_{h(i)} + c_{b_2} \tag{5}$$

для любого $i, 0 < i \leq m-1$.

Из леммы 1 а) получаем $c_{h(i+1)} = c_{a_2 h(i) + b_2} = c_{b_2} + a_1^{\,b_2} c_{a_2 h(i)}$.

Из лемм 1 б) и 12 следует

$c_{a_2 h(i)} = c_{a_2} \cdot gs(a_1{}^{a_2}, h(i)) = c_{a_2} \cdot gs(a_1, h(i) = c_{a_2} \cdot c_{h(i)}$.

Равенство (5) доказано.

Таким образом, в случае $m = p^n$, $a_1 \equiv 1 \pmod{p^u}$, $a_2 \equiv 1 \pmod{p^v}$ и $u + v \geq n$ последовательность P_2 является ЛПМП.

Применяя китайскую теорему об остатках, получаем следующее утверждение.

Теорема 4. *Пусть* $m = p_1{}^{t_1} p_2{}^{t_2} \cdots p_n{}^{t_n}$, $P_1 = c_0, c_1, ..., c_{m-1}$ – (m, a_1, b_1, c_0)-*ЛПМП*, $H = h(0), h(1), ..., h(m-1)$ – $(m, a_2, b_2, h(0))$-*ЛПМП и пусть* $P_2 = c_{h(0)}, c_{h(1)}, ..., c_{h(m-1)}$. *Пусть для любого* j, $1 \leq j \leq n$, $a_1 \equiv 1 \pmod{p_j{}^{u_j}}$, $a_2 \equiv 1 \pmod{p_j{}^{v_j}}$ *и* $u_j + v_j \geq t_j$.

Тогда P_2 *является* $(m, a_1^{a_2} c_{a_2}, c_{b_2})$-*ЛПМП*.

Можно показать, что при невыполнении условий теоремы 4 последовательность P_2 не является ЛПМП.