

**ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ
ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ
ЦЕЛОЧИСЛЕННЫХ ОПЕРАЦИЙ**

Переладова Анна Борисовна

Студентка

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: pereladova.ann@yandex.ru

Научный руководитель — Анашин Владимир Сергеевич

Основная идея настоящей работы заключается в построении генератора псевдослучайной последовательности в виде сплетения автоматов. Такая задача обусловлена тем, что при правильном построении сплетений можно получить равномерно распределенную последовательность с максимально возможным периодом равным произведению максимальных периодов последовательностей, вырабатываемых каждым из сплетаемых автоматов. В представленной работе в качестве одного из автоматов используется автомат, реализующий целочисленные операции.

В [1] рассматривается задача построения рекуррентной последовательности максимального периода $m2^n$ с помощью 2-адической арифметики. В данной работе приводятся достаточные условия, которым должно удовлетворять сплетение, чтобы порождать рекуррентную последовательность с длиной кратчайшего периода равной mp^n , в случае p -адической арифметики, где p — составное число.

В Теореме 1 приняты следующие обозначения:

- $\delta_r(z)$ — значение r -го разряда представления z в p -ичной системе счисления.
- $\psi_n^j(\delta_0(z), \dots, \delta_{n-1}(z)) : A^n \rightarrow A$, где $A = \{0, 1, \dots, p-1\}$ — функция «переноса единицы», соответствующая преобразованию g_j .

Теорема 1. Пусть p — некоторое составное число. Выберем m такое, что $(m, p) = 1$. Пусть c_0, \dots, c_{m-1} последовательность некоторых констант, пусть g_0, \dots, g_{m-1} конечная последовательность биективных по модулю p^n преобразований в \mathbb{Z}_p и эти последовательности удовлетворяют следующим условиям:

- $g_j(x) \equiv (x + c_j) \pmod{p}$ для всех $j = 0, 1, \dots, m-1$;
- $\sum_{j=0}^{m-1} c_j \equiv a \pmod{p}$, где $(a, p) = 1$;

- последовательность $(c_i \bmod m \bmod p)_{i=0}^{\infty}$ чисто периодическая, а m — длина её кратчайшего периода;
- $\delta_k(g_j(z)) \equiv \zeta_k + \psi_k^j(\zeta_0, \dots, \zeta_{k-1}) \pmod{p}$, $k = 1, 2, \dots$, где $\zeta_r = \delta_r(z)$, $r = 0, 1, 2, \dots$;
- $\sum_{j=0}^{m-1} \sum_{z \in \mathbb{Z}/p^n \mathbb{Z}} \psi_n^j(\delta_0(z), \dots, \delta_{n-1}(z)) \equiv b \pmod{p}$, где $(b, p) = 1$.

Тогда рекуррентная последовательность $X = (x_i)_{i=0}^{\infty}$, определяемая соотношением $x_{i+1} = g_i \bmod m(x_i)$, равномерно распределена над \mathbb{Z}_p (то есть на каждом периоде каждое слово встречается ровно m раз), а именно, последовательность $X \bmod p^k = (x_i \bmod p^k)_{i=0}^{\infty}$ чисто периодическая для всех $k = 1, 2, \dots$ и длина кратчайшего периода такой последовательности равна mp^k .

Литература

1. Anashin V., Khrennikov A. Applied algebraic dynamics. Berlin, New York: Walter de Gruyter, 2009