Д. М. Ермилов, **О. А. Козлитин** (Москва, ТВП). **О периодических свойствах полиномиального генератора над кольцом Галуа.**

Один из распространенных способов выработки псевдослучайных последовательностей состоит в использовании рекурренты с глубиной зависимости 1:

$$u_{i+1} = F(u_i) \quad \text{для всех} \quad i \geqslant 0, \tag{1}$$

где u_0 — начальное заполнение, а F — некоторая функция, не зависящая от i. При этом из соображений быстродействия функция F должна быть легко реализуемой. Например, если u — последовательность над кольцом R, то можно потребовать линейности или полиномиальности функции F. Далее мы будем считать, что функция F полиномиальна, и отождествлять функцию F с представляющим ее полиномом.

Первый естественный вопрос, возникающий в связи с генератором (1) — это вопрос о дефекте и периоде последовательности u. Его можно расширить до вопроса о строении графа преобразования F. В такой формулировке (для произвольного кольца R) рассматриваемая задача далека от решения, поэтому ограничимся наиболее исследованным классом колец — конечными локальными кольцами главных идеалов. К этому классу относятся, например, все конечные поля, все примарные кольца вычетов, а также целый ряд других коммутативных и некоммутативных колец [1].

Задача о строении графа преобразования F в случае, когда R — примарное кольцо вычетов, рассматривалась в работах ряда авторов, среди которых следует выделить В. С. Анашина [2] и М. В. Ларина [3]. Существует обширный класс коммутативных колец, занимающий промежуточное положение между примарными кольцами вычетов и произвольными конечными локальными кольцами главных идеалов — кольца Галуа. Полиномиальные преобразования колец Галуа описаны в [4]. Строение графа преобразования F над произвольным кольцом Галуа, насколько известно авторам, в литературе не обсуждалось.

Далее $R = \mathrm{GR}\,(q^n, p^n)$ — кольцо Галуа порядка q^n с характеристикой p^n. Для всякого $i \in \{1, 2, \ldots, n\}$ обозначим φ_i отображение, приводящее многочлены над кольцом R по модулю $p^i R$. Пусть элемент $a \in R$ лежит на цикле преобразования F. Длину цикла преобразования $\varphi_i(F)$, содержащего элемент $\varphi_i(a)$, обозначим $t_i(a)$. Таким образом, имеем последовательность натуральных чисел

$$t_1(a), t_2(a), \ldots, t_i(a), \ldots, t_n(a), \tag{2}$$

где $t_i(a) \,|\, t_{i+1}(a)$ для всякого $i \in \{1, 2, \ldots, n-1\}$. Очевидно, задача об описании циклов преобразования F сводится к изучению поведения последовательности (2).

Пусть «$\circ$» — операция композиции, $t \geqslant 1$ и $F^{[t]} = \underbrace{F \circ F \circ \cdots \circ F}_{t\,\text{раз}}$. Выберем и зафиксируем $a \in R$. Положим $f = F^{[t_1(a)]}$, $\nu = \|f(a) - a\|$, где $\|x\|$ есть наибольшее значение $k \in \{0, 1, \ldots, n\}$ со свойством $x \in p^k R$. Пусть f' и f'' — соответственно первая и вторая производная полинома f (см., например, [5]), e — единица кольца R.

Теорема. *Если* $f'(a) \equiv e \pmod{pR}$ *и* $p > 2$, *то справедливо неравенство*

$$t_n(a) \leqslant t_1(a)\, p^{n-\nu}. \tag{3}$$

Неравенство (3) *является строгим тогда и только тогда, когда* $p = 3$ *и* $e + yf''(a) \equiv 0 \pmod{pR}$, *где* y — *решение уравнения* $f(a) - a \equiv py \pmod{p^2 R}$.

Авторы выражают глубокую признательность профессору А. А. Нечаеву за постановку задачи и постоянное внимание к этой работе.

Работа выполнена при поддержке гранта Президента РФ НШ-4.2010.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Елизаров В. П.* Конечные кольца. М.: Гелиос–АРВ, 2006, 304 с.
2. *Анашин В. С.* О группах и кольцах, обладающих транзитивными полиномами. — В сб.: Тезисы XVI Всесоюзной алгебраической конференции. Ч. II. Л.: 1981, с. 4–5.
3. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов. — Дискретн. матем., 2002, т. 14, в. 2, с. 20–32.
4. *Нечаев А. А.* Полиномиальные преобразования конечных коммутативных колец главных идеалов. — Матем. заметки, 1980, т. 27, в. 6, с. 885–899.
5. *Глухов М. М.*, *Елизаров В. П.*, *Нечаев А. А.* Алгебра. М.: Гелиос–АРВ, 2003, 749 с.