А. В. З я з и н, **А. Б. Ш и ш к о в** (Москва, МИРЭА (ТУ)). **О периодических свойствах координатных последовательностей одного типа представлений линейных рекуррентных последовательностей над простым конечным полем.**

При выработке псевдослучйных последовательностей в качестве одного из способов применяется усложнение линейных рекуррентных последовательностей (ЛРП) над кольцами и полями. Усложнение также имеет много разновидностей. В частности, используется метод представления ЛРП над разными алгебраическими структурами.

Пусть u — линейная рекуррентная последовательность над кольцом K, R — другое кольцо, σ — произвольное отображение из K в R. Последовательность v над кольцом R, знаки которой образованы по правилу $v(i) = \sigma(u(i))$, будем называть (σ, R)-*представлением последовательности* u, или просто *представлением*.

Рассмотрим следующий вариант представления. Пусть u — ЛРП максимального периода ранга m над конечным полем из p элементов (оно выступает в качестве кольца K), где p — простое число. В качестве кольца R рассмотрим кольцо $\mathbf{Z}_{2^n}$ ($2^n \leqslant p$). Пусть σ — отображение, ставящее в соответствие элементу поля K его двоичное представление (как целого числа) в кольце R.

Обозначим $v_0(i), v_1(i), \ldots, v_{n-1}(i)$ координаты двоичного представления знака последовательности $v(i)$. Поскольку ЛРП u имеет период $p^m - 1$, период любой из последовательностей v_j, $j = 0, 1, \ldots, n-1$, делит это число. В работе, представленной данным докладом, изучался вопрос, в каком случае этот период сокращается, т. е. становится меньше, чем $p^m - 1$.

Теорема. *Пусть во введенных выше обозначениях $p_0, p_1, \ldots, p_{n-1}$ — двоичные координаты числа p. Обозначим k минимальное число, для которого $p_k = 0$. Тогда период последовательности v_k равен $(p^m - 1)/2$. Период любой последовательности при v_j равен $j \neq k$, равен $p^m - 1$.*

В доказательстве теоремы использовался результат работы [1]. Методы доказательства — теоретико-числовые и комбинаторные.

Работа выполнена при поддержке гранта Президента РФ НШ 8.2010.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Куракин В. Л.* Представления над кольцом $\mathbf{Z}_{p^n}$ линейной рекуррентной последовательности максимального периода над полем $\mathbf{GF}(q)$. — Дискретн. матем., 1992, т. 4, в. 4, с. 96–116.