Р. В. Б о г о н а т о в (Москва, ТВП). **Ранг суммы двух рекуррент максимального периода над $\mathbf{Z}_{2^n}$.**

Для чисел $a \in \mathbf{Z}_{2^n}$ и $N \in \{0, 1, \ldots, 2^n - 1\}$, имеющих двоичные разложения $a = a_0 + 2a_1 + \cdots + 2^{n-1}a_{n-1}$ и $N = N_0 + 2N_1 + \cdots + 2^{n-1}N_{n-1}$, определим число $a^{[N]} = a_0^{N_0} a_1^{N_1} \cdots a_{n-1}^{N_{n-1}}$, где полагаем $0^0 = 1$.

Утверждение. *Пусть $a, b \in \mathbf{Z}_{2^n}$ и $c = a + b$. Тогда координаты c_s, $s \in \{0, 1, \ldots, n-1\}$, двоичного разложения числа c удовлетворяют соотношениям*

$$c_s \equiv \sum_{N=0}^{2^s} a^{[N]} b^{[2^s - N]} \pmod 2.$$

Пусть $F(x)$ и $G(x)$ — многочлены максимального периода над кольцом вычетов $\mathbf{Z}_{2^n}$, степеней, соответственно, M_1 и M_2. Пусть u, v — линейные рекуррентные последовательности (ЛРП) максимального периода над кольцом $\mathbf{Z}_{2^n}$ с минимальными многочленами, соответственно, $F(x)$ и $G(x)$. Тогда их периоды будут равны

$$T(u) = 2^{n-1}\Big(2^{M_1} - 1\Big), \quad T(v) = 2^{n-1}\Big(2^{M_2} - 1\Big).$$

Определим последовательность w как сумму последовательностей u и v в кольце $\mathbf{Z}_{2^n}$. Для ЛРП w определим s-е двоичные координатные последовательности, $s \in \{0, 1, \ldots, n-1\}$, из равенств $w(i) = w_0(i) + 2w_1(i) + \cdots + 2^{n-1}w_{n-1}(i)$, $i \geqslant 0$, где $w_s(i) \in \{0, 1\}$. Координатные последовательности w_s, $s \in \{0, 1, \ldots, n-1\}$, можно рассматривать как ЛРП над полем GF(2).

Для ранга (степени минимального многочлена) координатной последовательности w_s выполняются следующие соотношения.

Теорема. *Пусть $n \geqslant 2$, $s \in \{1, 2, \ldots, n-1$ и $(M_1, M_2) = 1$. Тогда справедливы оценки*:

a) $\operatorname{rank} w_s \geqslant \binom{M_1}{2^s} + \binom{M_2}{2^s} + (2^{s-1} + 1)(M_1 + M_2)$;

b) $\operatorname{rank} w_s \leqslant \binom{M_1}{2^s} + \binom{M_2}{2^s} + M_1 + M_2 + 2^{s-1} \sum\limits_{\substack{k,t=0 \\ k+t \leqslant 2^s}}^{2^s-1} \binom{M_1}{k}\binom{M_2}{t}$.

Работа поддержана грантами НШ–4.2008.10 и МК–24.2009.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Кузьмин А. С.*, *Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа. — Алгебра и логика, 1995, т. 3, № 2, с. 169–189.
2. *Kurakin V. L.*, *Kuzmin A. S.*, *Mikhalev A. V.*, *Nechaev A. A.* Linear recurring sequences over rings and modules. (Contemporary Math. and its Appl. Thematic surveys. V. 10. Algebra 2. Moscow, 1994.) — J. of Math. Sciences, 1995, v. 76, № 6, p. 2793–2915.