ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 20 МАТЕМАТИКИ Выпуск 3
2013

Д. М. Ермилов (Москва, ТВП)**. О цикловой структуре биективных полиномиальных преобразований колец Галуа максимального периода.**

В настоящее время большую популярность получили полиномиальные генераторы, используемые для выработки псевдослучайных последовательностей. Различные свойства полиномиальных преобразований изучались в работах М. М. Глухова, А. А. Нечаева, В. С. Анашина, М. В. Ларина, В. Е. Викторенкова, Д. А. Пронькина и других авторов.

Широкое практическое применение имеют полиномиальные преобразования наибольшего периода. В работе [4] показано, что над кольцом Галуа $R = GR(q^n, p^n)$ биективное полиномиальное преобразование может иметь цикл длины не более, чем $(q-1)qp^{n-2}$. Возникает естественный вопрос об описании биективных полиномиальных преобразований $F(x) \in R[x]$, которые содержат цикл максимальной длины. Аналогичная задача решена М. В. Лариным в статье [3] для случая колец вычетов, в которой автор нашел критерии, описал вид и посчитал количество транзитивных (полноцикловых) полиномиальных преобразований колец вычетов.

В данной работе предлагаются первые результаты по описанию цикловой структуры биективных полиномиальных преобразований с максимальной длиной цикла над кольцами Галуа.

Теорема. *Пусть* $F(x) \in R[x]$ *— биективное полиномиальное преобразование, которое содержит цикл длины* $(q-1)qp^{n-2}$. *Тогда в цикловой структуре преобразования* $F(x)$ *содержится* $(\frac{q}{p})^{n-2}$ *циклов длины* $(q-1)qp^{n-2}$.

З а м е ч а н и е. Из теоремы [1] следует, что у биективного полиномиального преобразования с максимальной длиной цикла $F(x) \in R[x]$ ровно $(q-1)q^{n-1}$ элементов кольца R лежат на циклах максимальной длины. Цикловая структура множества элементов кольца R, не лежащих на циклах максимальной длины пока не известна.

Работа выполнена при поддержке гранта Президента РФ НШ-6260.2012.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Анашин В. С.* О группах и кольцах, обладающих транзитивными полиномами. — XVI Всесоюзная алгебраическая конференция. Тезисы. Часть II. Л.: 1981, с. 4–5.
2. *Елизаров В. П.* Конечные кольца. М.: 2006, Гелиос-АРВ.
3. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов. — Дискретн. матем., 2002, т. 14, в. 2, с. 20–32.
4. *Ермилов Д. М.*, *Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа. — Математические вопросы криптографии, 2013, т. 4, в. 1, с. 27–37.