ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 1
2014

Д. М. Ермилов (Москва, ТВП). **Полиномиальные подстановки над кольцом Галуа, содержащие цикл максимальной длины.**

Рассмотрим кольцо Галуа $R = GR(q^n, p^n)$ мощности q^n и характеристики p^n. Пусть $f(x) \in R[x]$ — биективный полином над кольцом Галуа R. Будем понимать под *цикловой структурой биективного полинома* $f(x)$ над кольцом R цикловую структуру подстановки, которую задает $f(x)$ над R. Напомним, что цикловая структура подстановки — это таблица $[l_1^{k_1}, \ldots, l_t^{k_t}]$, указывающая, что подстановка состоит из k_1 циклов длины $l_1, \ldots, k_t$ циклов длины l_t. В работе [1] показано, что цикловая структура произвольного полинома над кольцом Галуа R не может содержать цикл, длина которого больше $q(q-1)p^{n-2}$.

В данной работе рассматривается класс полиномов над кольцом Галуа R, цикловая структура которых содержит цикл максимальной длины $q(q-1)p^{n-2}$. Назовем такие полиномы МДЦ-полиномами.

Обозначим через J множество pR делителей нуля кольца Галуа R, $J^k = p^k R$ и $R_k = R/J^k$ — факторкольцо кольца R по идеалу J^k. Сформулируем критерий быть МДЦ-полиномом.

Теорема. *Пусть* $f(x) \in R[x]$ *и* $\alpha = (f^{[q]}(x))'_{x=a}$, *где* $a \in R_1$ *и* $f^{[q]}(x)$ — *q-я композиционная степень полинома* $f(x)$. *Тогда* $f(x)$ *является МДЦ-полиномом в том и только том случае, если*:

a) *в цикловой структуре полинома* $f(x)$ *над кольцом* R_3 *содержится цикл длины* $q(q-1)p$, *при* $p > 2$;

b) *в цикловой структуре полинома* $f(x)$ *над кольцом* R_3 *содержится цикл длины* $q(q-1)p$, *при* $p = 2$ *и* $\alpha \equiv e \pmod{J}$;

c) *в цикловой структуре полинома* $f(x)$ *над кольцом* R_4 *содержится цикл длины* $q(q-1)p^2$, *при* $p = 2$ *и* $\alpha \equiv 3e \pmod{J}$.

Следующие примеры показывают, что результаты теоремы усилить нельзя.

Пример 1. Рассмотрим кольцо Галуа $R = GR(15625, 125)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_{125}[y]_{/y^2+y+1}$. Элементами кольца R' являются многочлены над кольцом $\mathbb{Z}_{125}$ первой и нулевой степени, которые будем обозначать через векторы длины 2. Например, $2y + 1 \in R'$ будем обозначать $(2, 1)$. Элементы кольца R отождествим с элементами кольца R'. Возьмем полином, удовлетворяющий условиям a) теоремы:

$$f(x) = (0,3)x^{23} + (0,2)x^{22} + (4,0)x^{20} + (0,3)x^{19} + (0,2)x^{18} + (0,2)x^{16} +$$
$$+(1,0)x^{15} + (0,2)x^{14} + (1,1)x^{12} + (2,1)x^{11} + (0,4)x^{10} + (4,0)x^8 + (4,0)x^7 +$$
$$+(1,2)x^6 + (2,3)x^5 + (0,2)x^4 + (4,1)x^3 + (3,0)x^2 + (4,3)x + (0,2)$$

из кольца $R[x]$. Полином $f(x)$ над кольцом R_2 имеет цикловую структуру $[600^1, 25^1]$, но он не является МДЦ-полиномом, так как над кольцом R его цикловая структура равна $[600^{26}, 25^1]$.

П р и м е р 2. Рассмотрим кольцо Галуа $R = GR(64, 8)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_8[y]_{/y^2+y+1}$. Возьмем полином удовлетворяющий условиям b) теоремы:

$$f(x) = (0,1)x^6 + (1,0)x^5 + (0,1)x^4 + (0,1)x^3 + (0,1)x^2 + (0,1)x + (0,1)$$

из кольца $R[x]$. Полином $f(x)$ над кольцом R_2 имеет цикловую структуру $[12^1, 4^1]$, т. е. в цикловой структуре содержится цикл длины $q(q-1)$. Но над кольцом R его цикловая структура равна $[12^5, 4^1]$. Это означает, что $f(x)$ не является МДЦ-полиномом.

П р и м е р 3. Рассмотрим кольцо Галуа $R = GR(256, 16)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_{16}[y]_{/y^2+y+1}$. Возьмем полином удовлетворяющий условиям c) теоремы:

$$f(x) = (1,1)x^7 + (1,0)x^6 + (0,1)x^5 + (1,0)x^4 + (1,0)x^3 + (1,0)x^2 + (0,1)x + (0,1)$$

из кольца $R[x]$. Полином $f(x)$ над кольцом R_3 имеет цикловую структуру $[24^2, 12^1, 4^1]$, т. е. в цикловой структуре содержится цикл длины $q(q-1)p$. Но над кольцом R его цикловая структура равна $[24^{10}, 12^1, 4^1]$, следовательно, $f(x)$ не является МДЦ-полиномом.

СПИСОК ЛИТЕРАТУРЫ

1. *Ермилов Д. М.*, *Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа. — Математические вопросы криптографии, 2013, т. 4, в. 1, с. 27–57.