УДК 519.113.6

ПОСТРОЕНИЕ ТРАНЗИТИВНЫХ ПОЛИНОМОВ НАД КОЛЬЦОМ $\mathbb{Z}_{p^2}$

А. О. Ковалевская

Разработан метод, позволяющий строить все транзитивные полиномы по модулю p^2. Метод работает в предположении, что заранее известны все полиномы, транзитивные по модулю p.

Ключевые слова: *полиномиальная функция над кольцом, рекуррентные последовательности, транзитивные полиномы.*

В работе рассматриваются рекуррентные последовательности вида

$$a \bmod p^n, \quad f(a) \bmod p^n, \quad f(f(a)) \bmod p^n, \quad \ldots, \tag{1}$$

где $f(x) \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Такие последовательности находят применение в различных областях математики. В частности, в криптографии они используются в качестве псевдослучайных последовательностей. Поэтому возникает проблема построения таких полиномов $f(x)$, для которых указанная последовательность имеет большой период.

Определение 1. Полином $f(x) \in \mathbb{Z}[x]$ будем называть транзитивным по модулю p^n, если последовательность (1) имеет период p^n, то есть максимальный.

Определение 2. Полином $f(x)$ будем называть тождеством по модулю p^n, если $f(a) \bmod p^n = 0$ для любого $a \in \mathbb{Z}$.

Транзитивные полиномиальные преобразования колец вычетов рассматриваются в [1]. В соответствии с этой работой, если $p \notin \{2, 3\}$, то полином, транзитивный по модулю p^2, транзитивен по модулю p^n для любого натурального n. Кроме того, транзитивные полиномы по модулю p^n могут быть получены из транзитивных по модулю p^2 путём добавления тождества. Таким образом, важным является случай $n = 2$. Рассмотрим задачу получения всех транзитивных полиномов по модулю p^2.

Известны различные формы представления полиномиальных функций. Любая полиномиальная функция над $\mathbb{Z}_{p^2}$, в соответствии с [2], может быть представлена многочленом

$$f(x) = f_0(x) + pf_1(x) + (x^p - x)f_2(x), \tag{2}$$

где $f_0(x)$, $f_1(x)$, $f_2(x)$ — полиномы над кольцом $\mathbb{Z}_p$ степени меньше p. Из формы (2) нетрудно получить другую, которая будет использована далее:

$$f(x) = f_0(x) + pf_1(x) + (x^p - x)(f_0^{'}(x) - f^{'}(x)), \tag{3}$$

где $f^{'}(x)$ и $f_0^{'}(x)$ — производные для $f(x)$ и $f_0(x)$ с коэффициентами, приведёнными по модулю p. Обозначим $f^p(x) = \underbrace{f(f \ldots (x) \ldots)}_{p \text{ раз}}$.

Метод построения транзитивного по модулю p^2 полинома $f(x)$ состоит из следующих шагов:

1) Выбирается полином $f_0(x) \in \mathbb{Z}_p[x]$, транзитивный по модулю p.
2) Выбирается такой $f^{'}(x) \in \mathbb{Z}_p[x]$, для которого выполняется $\prod\limits_{x \in \mathbb{Z}_p} f^{'}(x) \bmod p = 1$.
3) Выбирается $f_1(x) \in \mathbb{Z}_p[x]$ — произвольный полином степени меньше p.

4) Многочлен $f(x)$ строится по формуле (3).
5) Выполняется проверка $f(x)$ на транзитивность: если $f^p(a) \neq a$ для некоторого $a \in \mathbb{Z}$, то искомый полином получен, иначе вернуться на шаг 3 и выбрать в качестве $f_1(x)$ другой полином.

Корректность проверки на транзитивность в шаге 5 алгоритма следует из необходимого и достаточного условия транзитивности, сформулированного в [1], а также из выбора $f'(x)$ на шаге 2. Условие, выполнение которого требуется в шаге 2, следует из утверждений, сформулированных в [3]. Количество полиномов, удовлетворяющих данному условию, равно $(p-1)^{p-1}$.

Для того чтобы с помощью этого метода получить все транзитивные по модулю p^2 полиномы, на шаге 3 потребуется перебрать все возможные полиномы с коэффициентами из $\mathbb{Z}_p$, степень которых меньше p. Их количество равно p^p. С учётом того, что количество полиномов, транзитивных по модулю p, равно $(p-1)!$, получаем, что метод требует перебора $(p-2)!(p-1)^p p^p$ полиномов $f(x)$, из которых в соответствии с [1] транзитивными являются $(p-2)!(p-1)^{p+1}p^{p-1}$. Таким образом, доля нетранзитивных составляет $1/p$. При больших значениях p эта доля очень мала, что обеспечивает хорошую работу метода. При реализации алгоритма в системе компьютерной алгебры Sage все 15360000 транзитивных по модулю 25 полиномов были построены за 32 мин. Эксперименты проводились на компьютере с процессором Intel Core i7-3770 и оперативной памятью 15,4 Гб.

Если рассматривать задачу нахождения не всех, а какого-либо одного или нескольких транзитивных полиномов, то возможно улучшение этого метода. Оно заключается в следующем. Пусть выбранный случайным образом полином $f_1(x)$ не привёл к транзитивному $f(x)$. Тогда выберем такой полином $g(x)$, для которого $g(x) = 0$ при всех значениях x, кроме одного. Затем подставим в формулу (3) вместо $f_1(x)$ сумму $f_1(x)+g(x)$. Такое построение гарантирует получение транзитивного по модулю p^2 полинома $f(x)$. Пусть в результате этих действий получили многочлен $F(x) = f(x) + pg(x)$. Тогда $F^p(x)$ имеет следующий вид:

$$F^p(x) = f^p(x) + p\,[g(x)\ g(f(x))\ \ \ldots\ \ g(f^{p-1}(x))] \begin{bmatrix} f'(f(x))f'(f^2(x))\cdots f'(f^{p-1}(x)) \\ f'(f^2(x))\ldots f'(f^{p-1}(x)) \\ \vdots \\ f'(f^{p-1}(x)) \\ 1 \end{bmatrix}. \quad (4)$$

В силу того, что $f(x)$ транзитивен по модулю p, но не транзитивен по модулю p^2, имеем $f^p(x) \bmod p^2 = x$. Кроме того, $g(x), g(f(x)), \ldots, g(f^{p-1}(x))$ — значения полинома $g(x)$ во всех различных точках. Среди них есть только одно ненулевое. Тогда в формуле (4) второе слагаемое не равно нулю по модулю p^2, откуда следует, что $F(x)$ транзитивен по модулю p^2.

ЛИТЕРАТУРА

1. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. №14(2). С. 20–32.
2. *Frisch S. and Krenn D.* Sylow p-groups of polynomial permutations on the integers mod p^n // J. Number Th. 2013. No. 133. P. 4188–4199.
3. *Ермилов Д. М., Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа // Математические вопросы криптографии. 2013. № 4(1). С. 27–57.