2013 Теоретические основы прикладной дискретной математики №4(22)

DOI 10.17223/20710410/22/2
УДК 512.714

ПЕРЕСТАНОВОЧНЫЕ МНОГОЧЛЕНЫ НАД ПРИМАРНЫМИ КОЛЬЦАМИ

А. В. Карпов

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: karpov@isc.tsu.ru

Изучаются вопросы обращения перестановочных многочленов над примарным кольцом $\mathbb{Z}_{p^k}$, где p — простое и $k > 1$. Устанавливаются необходимые и достаточные условия того, что два перестановочных многочлена являются взаимно обратными по модулю p^k. Доказывается рекуррентная формула для нахождения обратного перестановочного многочлена по модулю p^k на основе известного обращения по модулю p^2. Предлагается метод построения пар взаимно обратных многочленов по модулю p^k на основе одной такой пары.

Ключевые слова: *перестановочные многочлены, примарные кольца, полиномиальные перестановки.*

Введение

Рассматриваются многочлены с целыми коэффициентами от одной переменной. Каждый многочлен $f(x)$ индуцирует соответствующую функцию $\tilde{f} : \mathbb{Z} \to \mathbb{Z}$, значения которой можно рассматривать по разным модулям n, т. е. $\tilde{f}/n : \mathbb{Z}_n \to \mathbb{Z}_n$. Многочлен $f(x)$ называется *перестановочным* по модулю n (над $\mathbb{Z}_n$), если соответствующая ему функция $\tilde{f}/n : \mathbb{Z}_n \to \mathbb{Z}_n$ является биективной. Многочлен $g(x)$ называется *обратным* к $f(x)$ по модулю n, если для любого целого c выполняется $g(f(c)) = c \pmod n$. При этом многочлены $f(x)$ и $g(x)$ называются *взаимно обратными* по модулю n (над $\mathbb{Z}_n$).

Изучение перестановочных многочленов как таковых было начато в 1863 г. [1]. История развития этой области до 1922 г. освещена в [2]. Наиболее полный обзор современных и не только результатов, связанных с перестановочными многочленами над конечными полями, приведён в [3]. Вопросы, связанные с представимостью функций k-значной логики полиномами, в наиболее общем виде обсуждаются в [4]. В настоящее время появляются работы, связанные с перестановочными многочленами специального вида и их обращением [5 – 9], а также с различными прикладными вопросами, в том числе с применением перестановочных многочленов в криптографии и теории кодирования [10, 11]. Изучается строение группы перестановочных многочленов над конечным целочисленным кольцом [12].

В [13] приведен критерий перестановочности над произвольным кольцом классов вычетов целых чисел, из которого видно, что ключевым является случай примарных колец $\mathbb{Z}_{p^k}$, о котором и пойдёт речь далее.

1. Построение взаимно обратных многочленов

Исследование перестановочных многочленов над примарными кольцами начато в [14] для случая $p = 2$. Изучение некоторых частных случаев можно найти в [15]. В общем случае перестановочные многочлены над кольцами $\mathbb{Z}_{p^k}$ рассматриваются в [13], откуда известен следующий

Критерий перестановочности над $\mathbb{Z}_{p^k}$. Целочисленный многочлен является перестановочным над кольцом $\mathbb{Z}_{p^k}$ тогда и только тогда, когда он является перестановочным над полем $\mathbb{Z}_p$ и его производная не обращается в ноль в $\mathbb{Z}_p$.

Из приведённого критерия видно, что перестановочный над $\mathbb{Z}_{p^2}$ многочлен является перестановочным и по всем примарным модулям p^k и что задача построения перестановочных над $\mathbb{Z}_{p^k}$ многочленов сводится к построению перестановочных над полем $\mathbb{Z}_p$ многочленов $f_p(x)$ и многочленов $f_0(x)$, индуцирующих нулевую по модулю p функцию, таких, что $f_p'(x) + f_0'(x)$ не имеет корней в $\mathbb{Z}_p$.

Далее предлагается метод построения пар взаимно обратных многочленов по модулю p^k на основе одной такой пары.

Пусть $f_p(x)$ и $g_p(x)$ — взаимно обратные многочлены по модулю p^k. Следующая теорема позволяет обратить многочлен $f(x) = f_p(x) + f_0(x)$, используя известное обращение $g_p(x)$, при дополнительных ограничениях на $f_0(x)$.

Теорема 1. Пусть многочлены $f_p(x)$ и $g_p(x)$ — взаимно обратные по модулю p^k, а многочлены $f_0(x)$ и $f_0'(x)$ индуцируют нулевые функции по модулям $p^{\lceil k/2 \rceil}$ и $p^{\lfloor k/2 \rfloor}$ соответственно. Тогда обратным к $f(x)$ по модулю p^k является многочлен

$$g(x) = g_p(x) - f_0(g_p(x))g_p'(x).$$

Доказательство. Выберем произвольный $x \in \mathbb{Z}_{p^k}$ и рассмотрим суперпозицию

$$g(f(x)) = g_p(f(x)) - \underbrace{f_0(g_p(f(x)))}_{(*)} g_p'(f(x)). \tag{1}$$

Так как $f(x) = f_p(x) + f_0(x)$ и $f_0(x) = 0 \pmod{p^{\lceil k/2 \rceil}}$, то $g_p(f(x)) = g_p(f_p(x) + f_0(x)) = g_p(f_p(x)) + f_0(x)g_p'(f_p(x)) \pmod{p^k}$, $g_p(x)$ — обратный к $f_p(x)$ над $\mathbb{Z}_{p^k}$, следовательно,

$$g_p(f(x)) = x + f_0(x)g_p'(f_p(x)) \pmod{p^k}. \tag{2}$$

Подставляя (2) в (*) выражения (1), получаем

$$f_0(g_p(f(x))) = f_0(x + f_0(x)g_p'(f_p(x))) = f_0(x) + f_0'(x)f_0(x)g_p'(f_p(x)) \pmod{p^k}.$$

Так как $f_0'(x) = 0 \pmod{p^{\lfloor k/2 \rfloor}}$, то второе слагаемое в правой части последнего равенства равно нулю по модулю p^k и

$$f_0(g_p(f(x))) = f_0(x) \pmod{p^k}. \tag{3}$$

Далее заметим, что $g_p'(f(x)) = g_p'(f_p(x)) + f_0(x)g_p''(f_p(x)) \pmod{p^k}$, а значит, ввиду $f_0^2(x) = 0 \pmod{p^k}$, с учётом (3) получим

$$f_0(g_p(f(x)))g_p'(f(x)) = f_0(x)g_p'(f_p(x)) \pmod{p^k}. \tag{4}$$

Подставляя (2) и (4) в (1), получаем

$$g(f(x)) = x + f_0(x)g_p'(f_p(x)) - f_0(x)g_p'(f_p(x)) = x \pmod{p^k}.$$

Так как x — произвольный, то $g(x)$ является обратным к $f(x)$ над $\mathbb{Z}_{p^k}$. ■

Пример 1. Построим на основе теоремы 1 обратный многочлен к многочлену $f(x) = 2x + 2x^2 - x^4 + x^6 + 3x^8 + 3x^{10} + x^{12}$ по модулю 27. Многочлен $f_p(x) = 2x$ линеен, и обратный к нему над $\mathbb{Z}_{27}$ равен $g_p(x) = 14x$. В этом случае

$$f_0(x) = 2x^2 - x^4 + x^6 + 3x^8 + 3x^{10} + x^{12}$$

и вместе со своей производной он индуцирует нулевые функции по модулям 9 и 3 соответственно. Многочлен $f(x)$ удовлетворяет условиям теоремы 1, и обратный к нему найдём как

$$g(x) = g_p(x) - f_0(g_p(x))g_p'(x) = 14x + 20x^2 + 11x^4 + 4x^6 + 3x^8 + 21x^{10} + 22x^{12}.$$

Многочлен $g(x)$ индуцирует перестановку

$$(1, 14, 7, 26, 13, 20, 19, 23, 25, 8, 3, 2, 10, 5, 16, 19, 22, 11)(3, 6, 21, 15, 12, 24)(9, 18),$$

которая, как видно, является обратной к

$$(1, 11, 22, 17, 16, 5, 10, 2, 4, 8, 25, 23, 19, 20, 13, 26, 7, 14)(3, 24, 12, 15, 21, 6)(9, 18),$$

индуцированной $f(x)$.

Помимо порождения целого класса взаимно обратных по модулю p^k многочленов из одной пары взаимно обратных, теорема 1 позволяет свести задачу обращения $f(x)$ над $\mathbb{Z}_{p^k}$ к задаче обращения $f_p(x) = f(x) - f_0(x)$ над $\mathbb{Z}_{p^k}$, которая может оказаться проще. Так, в примере 1 многочлен $f_2(x)$ имеет достаточно сложную форму, но в силу того, что $f_p(x)$ линеен, обратить его оказывается несложно.

2. Условия на взаимно обратные многочлены, формула подъёма

Следующая теорема дает необходимые и достаточные условия того, что два многочлена являются взаимно обратными.

Теорема 2. Пусть многочлен $f(x)$ — перестановочный по модулю p^k. Тогда многочлен $g(x)$ является обратным к $f(x)$ по модулю p^k, если и только если выполняются следующие два условия:

1) для любого целого x выполняется

$$f'(x)g'(f(x)) = 1 \pmod{p^{\lfloor k/2 \rfloor}}; \tag{5}$$

2) $g(x)$ обращает $f(x)$ в $p^{\lceil k/2 \rceil}$ различных по модулю $p^{\lceil k/2 \rceil}$ точках.

Доказательство. Необходимость. Второе условие выполняется очевидным образом. Покажем, что выполняется условие 1. Для этого зафиксируем произвольный $x \in \mathbb{Z}_{p^k}$, придадим ему приращение $h = p^{\lceil k/2 \rceil}$. Тогда $h^2 = 0 \pmod{p^k}$ и разложение $g(f(x + h))$ по степеням h принимает вид

$$g(f(x + h)) = g(f(x)) + hf'(x)g'(f(x)) \pmod{p^k}. \tag{6}$$

Так как $g(x)$ является обратным к $f(x)$ над $\mathbb{Z}_{p^k}$, то (6) можно переписать в виде

$$h = hf'(x)g'(f(x)) \pmod{p^k},$$

откуда делением обеих частей на h получаем (5), и условие 1 выполняется в силу произвольности выбранного x.

Достаточность. Очевидно, что из $p^{\lceil k/2\rceil}$ различных по модулю $p^{\lceil k/2\rceil}$ точек путём прибавления к ним слагаемых $p^{\lceil k/2\rceil}l$, где $l \in \{0, 1, \ldots, p^{\lfloor k/2\rfloor} - 1\}$, можно получить все элементы $\mathbb{Z}_{p^k}$. Следовательно, так как выполняется условие 2, произвольный элемент кольца $\mathbb{Z}_{p^k}$ можно представить в виде $x + p^{\lceil k/2\rceil}l$, где x такой, что $g(f(x)) = x \pmod{p^k}$, а $l \in \{0, 1, \ldots, p^{\lfloor k/2\rfloor} - 1\}$. Тогда $g(f(x + p^{\lceil k/2\rceil}l)) = x + p^{\lceil k/2\rceil}lf'(x)g'(f(x)) \pmod{p^k}$, что, в силу условия 1, эквивалентно $g(f(x + p^{\lceil k/2\rceil}l)) = x + p^{\lceil k/2\rceil}l \pmod{p^k}$. Так как $x + p^{\lceil k/2\rceil}l$ — произвольный элемент кольца $\mathbb{Z}_{p^k}$, то $g(x)$ — обратный к $f(x)$ многочлен над $\mathbb{Z}_{p^k}$. ■

В ходе исследования было замечено, что многочлен $g(x)$, удовлетворяющий условию 1 теоремы 2, скорее всего, оказывается перестановочным. Можно также отметить, что, судя по примерам, перестановки, порождаемые взаимно обратными по модулю p^k многочленами, коммутируют по модулю p^{k+1}.

Далее излагается метод обращения целочисленного многочлена, перестановочного по всем примарным модулям p^n. Обращение осуществляется рекурсивно, начиная с известного обращения по модулю p^k при произвольном $k > 1$.

Понадобится

Следствие 1. Пусть многочлены $f(x)$ и $g(x)$ — взаимно обратные по модулю p^k. Тогда имеет место равенство

$$g(f(x)) = x + h_0(x), \tag{7}$$

где многочлены $h_0(x)$ и $h'_0(x)$ индуцируют нулевые функции по модулям p^k и $p^{\lfloor k/2\rfloor}$ соответственно.

Доказательство. Так как $g(x)$ является обратным к $f(x)$ над $\mathbb{Z}_{p^k}$, то их суперпозиция — тождественная функция, а значит, $g(f(x)) = x + h_0(x)$ и $h_0(x) = 0 \pmod{p^k}$ для всех $x \in \mathbb{Z}_{p^k}$. Из этого же следует, что выполняется условие 1 теоремы 2, а значит, $[g(f(x)]' = g'(f(x))f'(x) = 1 = 1 + h'_0(x) \pmod{p^{\lfloor k/2\rfloor}}$ для произвольного $x \in \mathbb{Z}_{p^k}$. ■

Следующая теорема позволяет «поднимать» обратный по модулю p^k многочлен до обратного по модулю $p^{k+\lfloor k/2\rfloor}$.

Теорема 3. Пусть многочлен $f(x)$ — перестановочный над $\mathbb{Z}_{p^k}$, $g_k(x)$ — обратный к $f(x)$ над $\mathbb{Z}_{p^k}$, $k > 1$. Тогда обратным к $f(x)$ по модулю $p^{k+\lfloor k/2\rfloor}$ является многочлен

$$g_{k+\lfloor k/2\rfloor}(x) = 2g_k(x) - g_k(f(g_k(x))). \tag{8}$$

Доказательство. Используя (7), равенство (8) можно переписать в виде $g_{k+\lfloor k/2\rfloor}(x) = g_k(x) - h_0(g_k(x))$. Выберем произвольный $x \in \mathbb{Z}_{p^k}$ и рассмотрим суперпозицию $g_{k+\lfloor k/2\rfloor}(f(x)) = g_k(f(x)) - h_0(g_k(f(x)))$. Так как $h_0(x) = g_k(f(x)) - x$, получаем $g_{k+\lfloor k/2\rfloor}(f(x)) = x + h_0(x) - h_0(x + h_0(x))$. Далее $h_0(x + h_0(x)) = h_0(x) + h_0(x)h'_0(x)$ и, в силу следствия 1, слагаемое $h_0(x)h'_0(x)$ обращается в ноль по модулю $p^{k+\lfloor k/2\rfloor}$ при любом $x \in \mathbb{Z}_{p^k}$. Окончательно получаем $g_{k+\lfloor k/2\rfloor}(f(x)) = x + h_0(x) - h_0(x) = x \pmod{p^{k+\lfloor k/2\rfloor}}$, что, в силу произвольности выбранного x, и доказывает теорему. ■

Пример 2. Рассмотрим многочлен $f(x) = x^3 + x$. Над $\mathbb{Z}_9$ он индуцирует перестановку $(1, 2)(4, 5)(7, 8)$ и, как видно, является обратным к самому себе. Над $\mathbb{Z}_{27}$ $f(x)$ индуцирует следующую перестановку:

$$(1, 2, 10, 11, 19, 20)(4, 14)(5, 22)(7, 26, 25, 17, 16, 8)(13, 23),$$

и над $\mathbb{Z}_{27}$ себя уже не обращает. По теореме 3 найдём обратный к $f(x)$ над $\mathbb{Z}_{27}$ многочлен. Используем (8), где $g_2(x) = f(x)$. Найдём $g_3(x) = 2f(x) - f(f(f(x)))$:

$$g_3(x) = x - x^3 + 18x^5 + 3x^7 + 6x^{11} + 6x^{13} + 24x^{15} + 15x^{19} + 21x^{21} + 18x^{23} + 18x^{25} - x^{27}.$$

Перестановка, индуцируемая полученным $g_3(x)$:

$$(1, 20, 19, 11, 10, 2)(4, 14)(5, 22)(7, 8, 16, 17, 25, 26)(13, 23),$$

обратна к перестановке, индуцированной $f(x)$.

Теорема 3 позволяет свести задачу обращения заданного перестановочного многочлена $f(x)$ по модулю p^k к задаче обращения $f(x)$ по модулю p^2. Таким образом, имея известное обращение по модулю p^2, по формуле (8) можно обратить заданный многочлен по модулю p^k для произвольного k.

Заключение

Рассмотрение вопросов перестановочности над конечным целочисленным кольцом сводится к случаю колец классов вычетов целых чисел по примарным модулям p^k.

Теорема 1 даёт метод построения пар взаимно обратных по модулю p^k перестановочных многочленов на основе одной такой пары, а также позволяет в некоторых случаях существенно упростить обращение. Формула (8) сводит задачу обращения по модулю p^k к обращению по модулю p^2 с последующим «подъёмом» решения, осуществляемым с модуля p^k на модуль $p^{k+\lfloor k/2 \rfloor}$. Получены необходимые и достаточные условия того, что два перестановочных многочлена являются взаимно обратными по модулю p^k (теорема 2).

Краткое изложение представленных результатов можно найти в [16].

ЛИТЕРАТУРА

1. *Hermite C.* Sur les fonctions de sept lettres // C. R. Acad. Sci. Paris. 1863. V. 57. P. 750–757.
2. *Dickson L. E.* History of the Theory of Numbers. Carnegie Institute, Washington, D. C., 1923. V. 3.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
4. *Мещанинов Д. Г.* Метод построения полиномов для функций k-значной логики // Дискретная математика. 1995. Т. 7. № 3. С. 48–60.
5. *Caceres A. and Colon-Reyes O.* Some criteria for permutation binomials. Preprint. University of Puerto Rico at Humacao, 1997.
6. *Akbary A. and Wang Q.* On some permutation polynomials over finite fields // Intern. J. Math. Math. Sci. 2005. V. 2005. Iss. 16. P. 2631–2640.
7. *Diaz-Vargas J., Rubio-Barrios C. J., Sozaya-Chan J. A., and Tapia-Recillas H.* Self-invertible permutation polynomials over $\mathbb{Z}_m$ // Intern. J. Algebra. 2011. V. 5. No. 23. P. 1135–1153.
8. *Ryu J. and Takeshita O. Y.* On quadratic inverses for quadratic permutation polynomials over integer rings // IEEE Trans. Inform. Theory. 2006. V. 52. Iss. 3. P. 1254–1260.
9. *Wu B. and Liu Z.* The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2 // `arxiv.org/abs/1301.0070`. January 2013.
10. *Varadharajan V.* Cryptosystems based on permutation polynomials // Intern. J. Computer Math. 1988. V. 23. Iss. 3–4. P. 237–250.
11. *Sun J. and Takeshita O. Y.* Interleavers for turbo codes using permutation polynomials over integer rings //IEEE Trans. Inform. Theory. 2005. V. 51. Iss. 1. P. 101–119.
12. *Frisch S. and Krenn D.* Sylow p-groups of polynomial permutations on the integers mod p^n // `arxiv.org/abs/1112.1228`. December 2011.

13. *Li S.* Permutation polynomials modulo m // `arxiv.org/pdf/math/0509523.pdf`. February 2008.
14. *Rivest R. L.* Permutation polynomials modulo 2^w // Finite Fields and Their Applications. 2001. No. 7. P. 287–292.
15. *Singh R. P. and Maity S.* Permutation polynomials modulo p^n // `eprint.iacr.org/2009/393.pdf`. 2009.
16. *Карпов А. В.* Обращение перестановочного многочлена над примарным кольцом // Междунар. конф. «Алгебра и логика: теория и приложения». Тез. докл. Красноярск: СФУ, 2013. С. 60–61.