Math-Net.Ru

Общероссийский математический портал

А. В. Акишин, Об одном классе подстановочных многочленов над кольцами вычетов по модулю 2^n , *Матем. вопр. криптогр.*, 2013, том 4, выпуск 2, 5–15

DOI: <https://doi.org/10.4213/mvk78>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.149

26 апреля 2023 г., 13:19:05

**Об одном классе подстановочных
многочленов над кольцами вычетов
по модулю 2^n**

А. В. Акишин

Московский государственный технический университет радиотехники,
электроники и автоматики, Москва

Получено 30.VII.2012

В работе рассматриваются преобразования колец вычетов по модулю 2^n , имеющие вид многочленов с рациональными коэффициентами. Определяются условия, при которых такие многочлены определяют подстановки на кольцо вычетов.

Ключевые слова: несовместимые многочлены, кольца вычетов, генераторы псевдослучайных последовательностей

On a class of permutation polynomials over rings of residues modulo 2^n

A. V. Akishin

*Moscow State Technical University of Radio Engineering, Electronics and Automatics,
Moscow*

Abstract. We consider mappings of the residue rings modulo 2^n representable as polynomials with rational coefficients. Conditions ensuring that such a polynomial define a permutation of a ring are described.

Key words: incompatible polynomials, residue rings, pseudo-random number generators

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 2, pp. 5–15 (Russian).

1. Введение

Преобразования колец вычетов $\mathbb{Z}_n$ широко используются в криптографии. Например, достаточно широко распространены так называемые конгруэнтные генераторы псевдослучайных последовательностей, то есть генераторы, формирующие псевдослучайные последовательности вида

$$u_{i+1} \equiv f(u_i) \pmod{n},$$

где $f(x) \in \mathbb{Z}[x]$ — некоторый многочлен с целочисленными коэффициентами. Наиболее широко известен линейный конгруэнтный генератор [5], входящий в стандартные библиотеки большинства современных компиляторов. Не удовлетворяя криптографическим требованиям, такие генераторы, однако, достаточно успешно проходят статистические тесты. Это позволяет использовать их в криптографических алгоритмах в качестве генераторов исходных последовательностей.

Как правило, для конгруэнтных генераторов выбирают многочлен $f(x)$ таким образом, чтобы он был подстановкой на кольце $\mathbb{Z}_n$. Условия, при которых многочлен $f(x) \in \mathbb{Z}[x]$ с целочисленными коэффициентами задает некоторую подстановку на кольце $\mathbb{Z}_{2^n}$, получены в работе [8].

С другой стороны, для обеспечения максимального периода важной является задача описания многочленов, дающих максимальный период. Для линейного конгруэнтного генератора эта задача решается в [5], а в общем случае — в работе [6].

Однако класс преобразований, задаваемых многочленами с целочисленными коэффициентами, уже класса всех преобразований кольца вычетов. В настоящей работе мы рассмотрим класс многочленов, позволяющий получать более широкий класс преобразований колец вычетов и имеющий достаточно простую реализацию, тем самым интересный с прикладной точки зрения.

2. Определения и обозначения

Многочлен $f(x) \in \mathbb{Z}[x]$ с целочисленными коэффициентами обладает тем свойством, что для любых $a, b \in \mathbb{Z}$ из

$$a \equiv b \pmod{n}$$

следует, что

$$f(a) \equiv f(b) \pmod{n}.$$

В работах [2, 3] такие преобразования были названы совместимыми с эпиморфизмом $\mathbb{Z} \rightarrow \mathbb{Z}_n$. В работе [1] было введено понятие несовместимого преобразования. Напомним некоторые определения и обозначения.

Пусть

$$\alpha_n: \mathbb{Z} \rightarrow \mathbb{Z}_{2^n}$$

— эпиморфизм колец. Для удобства будем считать, что

$$\mathbb{Z}_{2^n} = \{0, 1, \dots, 2^n - 1\}.$$

Пусть, далее,

$$\Psi_n = \{\psi: \mathbb{Z}_{2^n} \rightarrow \mathbb{Z} \mid \psi(k) \in k + 2^n\mathbb{Z}\}$$

— множество *функций выбора*. Каждая функция выбора $\psi \in \Psi_n$ выбирает по одному представителю в каждом классе вычетов и тем самым задает некоторую полную систему вычетов.

Пусть $f: \mathbb{Z} \rightarrow \mathbb{Z}$ — некоторое отображение кольца целых чисел в себя. При заданном эпиморфизме α_n каждая функция выбора $\psi \in \Psi_n$ определяет отображение

$$f \rightarrow f_\psi = \alpha_n f \psi.$$

Будем говорить, что отображение f *реализует* отображение $f_\psi: \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^n}$ в системе вычетов ψ . Через

$$F_n(f) = \{f_\psi \mid \psi \in \Psi_n\}$$

обозначим множество всех отображений $\mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^n}$, реализуемых отображением f в различных системах вычетов. В частности, если отображение f является совместимым с эпиморфизмом α_n , например задается некоторым многочленом с целыми коэффициентами, то $|F_n(f)| = 1$. Если же отображение f не совместимо с эпиморфизмом α_n , то $|F_n(f)| > 1$. Отметим, что может оказаться так, что множество $F_n(f)$ содержит все функции на кольце $\mathbb{Z}_{2^n}$. В работе [1] преобразования с таким свойством были названы максимально несовместимыми.

В данной работе мы рассмотрим один класс несовместимых с эпиморфизмом α_n отображений, а именно будем рассматривать отображения, задаваемые многочленами вида

$$f(x) = a_0 h(x)^m + a_1 h(x)^{m-1} + \dots + a_m, \quad (1)$$

где $a_i \in \mathbb{Z}$, а многочлен $h(x)$ имеет вид

$$h(x) = \frac{x(x+1)}{2} \in \mathbb{Q}[x].$$

Как показано в работе [1], максимально несовместимые с эпиморфизмом α_n многочлены указанного вида существуют только при $n = 1$. Там же получено описание всех таких многочленов. В данной работе рассмотрим случай $n > 1$.

3. Эквивалентность функций выбора

Пусть $\varphi, \psi \in \Psi_n$ — две функции выбора. Будем говорить, что функции φ и ψ являются *эквивалентными* относительно многочлена f вида (1), если выполняется равенство $f_\varphi = f_\psi$.

Лемма 1. *Две эквивалентные относительно многочлена $h(x)$ функции выбора $\varphi, \psi \in \Psi_n$ эквивалентны и относительно любого многочлена $f(x)$ вида (1).*

Доказательство. В самом деле, предположим, что $h_\varphi = h_\psi$. Тогда из (1) легко получаем

$$\begin{aligned} f_\varphi(k) &= \alpha_n f(\varphi(k)) = \alpha_n \left(\sum_{j=0}^m a_j h(\varphi k)^{m-j} \right) = \\ &= \alpha_n \left(\sum_{j=0}^m a_j h(\psi k)^{m-j} \right) = \alpha_n f(\psi(k)) = f_\psi(k). \end{aligned}$$

Таким образом, $f_\varphi = f_\psi$. □

Отметим, что обращение этого утверждения в общем случае не верно.

Выясним, когда функции выбора являются эквивалентными относительно многочлена $h(x)$. Для этого нам понадобится следующее предложение, которое проверяется непосредственным вычислением.

Предложение 1. *Для любых $x, y \in \mathbb{Z}$ имеет место равенство*

$$h(x + y) = h(x) + xy + h(y).$$

Условие эквивалентности двух функций выбора дается следующей леммой.

Лемма 2. Две функции выбора $\varphi, \psi \in \Psi_n$ эквивалентны относительно многочлена $h(x)$ тогда и только тогда, когда

$$\varphi(k) \equiv \psi(k) \pmod{2^{n+1}}$$

для любого $k \in \mathbb{Z}_{2^n}$.

Доказательство. Положим $\varphi(k) = a_k$, $\psi(k) = a_k + 2^n t_k$, где $t_k \in \mathbb{Z}$, $k = 0, 1, \dots, 2^n - 1$. Тогда по определению эквивалентности функций выбора и с учетом предложения 1 для каждого $k \in \mathbb{Z}_{2^n}$ выполняется сравнение

$$h(a_k + 2^n t_k) \equiv h(a_k) + h(2^n t_k) \equiv h(a_k) \pmod{2^n}.$$

Отсюда следует, что

$$h(2^n t_k) = 2^{n-1} t_k (2^n t_k + 1) \equiv 0 \pmod{2^n}.$$

Следовательно, $t_k = 2s_k$ для каждого $k = 0, 1, \dots, 2^n - 1$. Таким образом, действительно,

$$\psi(k) \equiv \varphi(k) \pmod{2^{n+1}}$$

для каждого $k = 0, 1, \dots, 2^n - 1$. Этим доказана необходимость указанного в лемме условия.

Докажем теперь его достаточность. Если

$$\psi(k) = a_k + 2^{n+1} t_k, \quad k = 0, 1, \dots, 2^n - 1,$$

где $a_k = \varphi(k)$, $t_k \in \mathbb{Z}$, то для любого $k = 0, 1, \dots, 2^n - 1$ получаем

$$h(a_k + 2^{n+1} t_k) = h(a_k) + h(2^{n+1} t_k) \equiv h(a_k) \pmod{2^n}.$$

Следовательно, $h_\varphi = h_\psi$. Этим доказательство леммы завершено. $\square$

На основе леммы 2 можно предложить следующий способ описания всех классов эквивалентности функций выбора. Для этого определим отображение $\beta_n: \Psi_n \rightarrow \mathbb{Z}_2^{2^n}$, положив

$$\beta_n(\psi) = \{\psi_0, \psi_1, \dots, \psi_{2^n-1}\},$$

где

$$\psi_i = \begin{cases} 0, & \text{если } \psi(i) \equiv i \pmod{2^{n+1}}, \\ 1 & \text{в противном случае, то есть при } \psi(i) \equiv i + 2^n \pmod{2^{n+1}}. \end{cases}$$

Тогда из леммы 2 легко получаем следующее утверждение.

Лемма 3. *Функции выбора $\varphi, \psi \in \Psi_n$ эквивалентны относительно многочлена $h(x)$ тогда и только тогда, когда $\beta_n(\varphi) = \beta_n(\psi)$. Отображение β_n сюръективно.*

Следствие 1. *Многочлен $h(x)$ реализует на кольце вычетов $\mathbb{Z}_{2^n}$ точно 2^{2^n} различных отображений.*

Наличие сюръективного отображения β_n дает возможность задавать функции выбора в виде векторов пространства $\mathbb{F}_2^{2^n}$. При этом каждому вектору $\mathbf{x} \in \mathbb{F}_2^{2^n}$ сопоставляется некоторая (любая) функция $\psi \in \Psi_n$, для которой $\beta_n(\psi) = \mathbf{x}$. Эту возможность мы будем использовать в дальнейшем, не различая эквивалентные функции выбора. Соответственно, через $h_{\mathbf{x}}$ обозначим то отображение, которое реализует в кольце $\mathbb{Z}_{2^n}$ многочлен $h(x)$ в системе вычетов, задаваемой функцией выбора $\psi \in \Psi_n$ с $\beta_n(\psi) = \mathbf{x}$. Например, для $n = 2$ вектор $(0, 0, 0, 0)$ задает систему вычетов $\{0, 1, 2, 3\}$, а вектор $(1, 0, 0, 1)$ задает систему вычетов $\{4, 1, 2, 7\}$.

Пусть теперь

$$f(x) = a_0 h(x)^m + a_1 h(x)^{m-1} + \dots + a_m,$$

причем $a_i \in \mathbb{Z}$ — целые числа, $i = 0, 1, \dots, m$. Рассмотрим многочлен

$$\bar{f}(y) = a_0 y^m + a_1 y^{m-1} + \dots + a_m \in \mathbb{Z}[y].$$

Очевидно, что многочлен $\bar{f}(y)$ совместим с эпиморфизмом α_n . Если $\bar{f}(y)$ реализует некоторое отображение π на кольце $\mathbb{Z}_{2^n}$, то выполняется равенство

$$f_{\psi} = \pi h_{\psi}$$

для любой функции выбора $\psi \in \Psi$, то есть каждому отображению h_{ψ} сопоставляется некоторое отображение f_{ψ} . Если отображение π является подстановкой на $\mathbb{Z}_{2^n}$, то это сопоставление является взаимно однозначным, что обосновывает следующее утверждение.

Лемма 4. *Если многочлен $\bar{f}(y)$ реализует подстановку на кольце вычетов $\mathbb{Z}_{2^n}$, то многочлен $f(x)$ реализует точно 2^{2^n} различных отображений на $\mathbb{Z}_{2^n}$.*

Если же многочлен $\bar{f}(y)$ реализует отображение π , не являющееся подстановкой на $\mathbb{Z}_{2^n}$, то может случиться так, что

$$\pi h_{\psi} = \pi h_{\varphi}$$

для некоторых функций выбора $\varphi, \psi \in \Psi_n$. Однако с прикладной точки зрения наиболее важным является случай, когда отображение π является подстановкой. Поэтому везде далее считаем, что многочлен $\bar{f}(y)$ реализует подстановку на $\mathbb{Z}_{2^n}$. Отметим, что критерии того, определяет ли многочлен $\bar{f}(y)$ подстановку на кольце $\mathbb{Z}_{2^n}$, описаны, например, в [6–8].

4. Подстановочные функции выбора

Функцию выбора $\psi \in \Psi_n$, для которой отображение f_ψ является подстановкой на кольце вычетов $\mathbb{Z}_{2^n}$, будем называть *подстановочной*.

Начнем со следующей, достаточно очевидной, леммы.

Лемма 5. *Если $\bar{f}(x)$ — несовместимый с эпиморфизмом α_n многочлен вида (1) и многочлен $\bar{f}(y)$ задает подстановку на $\mathbb{Z}_{2^n}$, то преобразование f_ψ является подстановкой на кольце $\mathbb{Z}_{2^n}$ тогда и только тогда, когда h_ψ — подстановка.*

Поэтому задачу описания подстановочных функций выбора достаточно рассмотреть только для многочлена $h(x)$. При этом будет удобнее задавать функции выбора в виде векторов пространства $\mathbb{F}_2^{2^n}$.

Пусть $\mathbf{0}$ обозначает нулевой вектор пространства $\mathbb{F}_2^{2^n}$.

Предложение 2. *Преобразование $h_{\mathbf{0}}$ является подстановкой.*

Доказательство. Предположим, что для некоторых x, y выполняется равенство

$$h(x) \equiv h(y) \pmod{2^n}$$

при условии, что $0 \leq x, y < 2^n$. Тогда

$$\frac{x(x+1)}{2} \equiv \frac{y(y+1)}{2} \pmod{2^n}.$$

Легко показать, что это соотношение эквивалентно сравнению

$$(x-y)(x+y+1) \equiv 0 \pmod{2^{n+1}}.$$

В произведении слева одна скобка всегда четная, а другая — нечетная, следовательно, возможны два варианта:

- 1) $x \equiv y \pmod{2^{n+1}}$,
- 2) $x+y+1 \equiv 0 \pmod{2^{n+1}}$.

В первом случае, учитывая условие $0 \leq x, y < 2^n$, получаем $x = y$.

Во втором случае имеем

$$x+y+1 \leq (2^n-1) + (2^n-1) + 1 = 2^{n+1} - 1 < 2^{n+1},$$

так что при наложенных ограничениях на x и y это сравнение решений не имеет.

Таким образом, мы получили, что из условий

$$h(x) \equiv h(y) \pmod{2^n}, \quad 0 \leq x, y < 2^n,$$

следует, что $x = y$, т. е. преобразование h_0 инъективно. Но так как кольцо $\mathbb{Z}_{2^n}$ конечно, то из инъективности следует биективность, значит, преобразование h_0 является подстановкой. $\square$

Из предложения 1 следует, что

$$h(x + 2^n) \equiv h(x) + h(2^n) \equiv h(x) + 2^{n-1} \pmod{2^n}$$

для любого $x \in \mathbb{Z}$. Это означает, что если h_x — отображение, которое многочлен $h(x)$ реализует в полной системе вычетов, заданной вектором $\mathbf{x} = (x_0, x_1, \dots, x_{2^n-1}) \in \mathbb{F}_2^{2^n}$, и $\mathbf{y} = (y_0, y_1, \dots, y_{2^n-1}) \in \mathbb{F}_2^{2^n}$ — другой вектор, то имеет место равенство

$$h_y(k) = \begin{cases} h_x(k), & \text{если } y_k = x_k, \\ h_x(k) + 2^{n-1}, & \text{если } y_k \neq x_k. \end{cases}$$

Используем это в доказательстве следующей леммы.

Лемма 6. *Отображение h_x является подстановкой на $\mathbb{Z}_{2^n}$ тогда и только тогда, когда вектор $\mathbf{x} = (x_0, x_1, \dots, x_{2^n-1})$ является симметричным, то есть $x_i = x_{2^n-1-i}$ для любого $i = 0, 1, \dots, 2^{n-1}$.*

Доказательство. Решим сравнение

$$h(b) \equiv h(a) + 2^{n-1} \pmod{2^n}$$

при фиксированном a , $0 \leq a < 2^n$. Оно эквивалентно сравнению

$$(b - a)(b + a + 1) \equiv 0 \pmod{2^n}.$$

Так как в произведении слева одна скобка четная, а другая — нечетная, то должно выполняться одно из условий:

$$b - a \equiv 0 \pmod{2^n} \text{ или } b + a + 1 \equiv 0 \pmod{2^n}.$$

Нас интересуют значения b , удовлетворяющие неравенствам $0 \leq b < 2^n$. При этом в первом случае получим $b = a$. Во втором случае $b = 2^n - 1 - a$. В частности,

$$h(2^n - 1 - a) \equiv h(a) + 2^{n-1} \pmod{2^n}.$$

Предположим теперь, что h_x — подстановка на $\mathbb{Z}_{2^n}$ в системе вычетов $x = (x_0, x_1, \dots, x_{2^n-1}) \in \mathbb{F}_2^{2^n}$. Предположим, что для некоторого $k, 0 \leq k < 2^n$, имеет место неравенство $x_k \neq x_{2^n-1-k}$, то есть $x_{2^n-1-k} = 1 - x_k$. Тогда

$$h_x(k) \equiv h(k) + 2^{n-1}x_k \pmod{2^n},$$

а в силу равенства $a + 2^{n-1} \equiv a - 2^{n-1} \pmod{2^n}$ для любого a

$$h_x(2^n - 1 - k) \equiv h(k) + 2^{n-1} + 2^{n-1}(1 - x_k) \equiv h(k) + 2^{n-1}x_k \pmod{2^n}.$$

Следовательно, $h_x(k) = h_x(2^n - 1 - k)$, что невозможно, так как по предположению h_x — подстановка. Значит, условие леммы является необходимым.

Докажем его достаточность. Пусть для каждого $k = 0, 1, \dots, 2^n - 1$ имеет место равенство $x_k = x_{2^n-1-k}$. Предположив, что для некоторых k, s выполняется равенство $h_x(k) = h_x(s)$, мы видим, что должно выполняться одно из равенств:

$$k = s \text{ или } s = 2^n - 1 - k.$$

Первый случай очевиден. Во втором случае получаем

$$h_x(s) \equiv h(k + 2^n x_k) \equiv h(k) + 2^{n-1} + 2^{n-1}x_k \equiv h_x(k) + 2^{n-1},$$

что противоречит предположению. Таким образом, действительно, h_x — подстановка на $\mathbb{Z}_{2^n}$. $\square$

Теперь, используя лемму 6, легко доказать следующую теорему.

Теорема 1. Пусть $f(x)$ — многочлен вида (1), несовместимый с эпиморфизмом α_n , и многочлен $\bar{f}(y)$ задает подстановку на $\mathbb{Z}_{2^n}$. Тогда отображение $\hat{f}_x$ является подстановкой на $\mathbb{Z}_{2^n}$ тогда и только тогда, когда вектор $x = (x_0, x_1, \dots, x_{2^n-1})$ является симметричным.

Так как симметричные векторы образуют подпространство размерности 2^{n-1} в векторном пространстве $\mathbb{F}_2^{2^n}$, то справедливо следующее утверждение.

Следствие 2. Многочлен вида (1) реализует на $\mathbb{Z}_{2^n}$ точно $2^{2^{n-1}}$ различных подстановок.

В качестве примера в следующей таблице для случая $n = 1$ приведены: а) векторы, задающие различные системы вычетов (в первом столбце),

б) полная система вычетов кольца $\mathbb{Z}_2$ (во втором столбце) и в) нижняя строка отображения h_x в данной системе вычетов (в третьем столбце).

x	Система вычетов	h_x
00	01	01
01	03	00
10	21	11
11	23	10

Как видно из примера, преобразование $h(x)$ реализует на $\mathbb{Z}_2$ ровно $2^{2^1} = 4$ различных отображений, из которых $2^{2^{1-1}} = 2$ являются подстановками. Подстановки задаются симметричными векторами $(0, 0)$ и $(1, 1)$.

В следующей таблице приведен аналогичный пример для случая $n = 2$.

x	Система вычетов	h_x
0000	0123	0132
0001	0127	0130
0010	0163	0112
0011	0167	0110
0100	0523	0332
0101	0527	0330
0110	0563	0312
0111	0567	0310
1000	4123	2132
1001	4127	2130
1010	4163	2112
1011	4167	2110
1100	4523	2332
1101	4527	2330
1110	4563	2312
1111	4567	2310

Как видно, многочлен $h(x)$ реализует на кольце $\mathbb{Z}_4$ ровно $2^{2^2} = 16$ различных отображений, из которых $2^{2^{2-1}} = 4$ являются подстановками. Эти подстановки задаются симметричными векторами $(0, 0, 0, 0)$, $(0, 1, 1, 0)$, $(1, 0, 0, 1)$ и $(1, 1, 1, 1)$.

Список литературы

1. Акишин А. В. Несовместимые преобразования колец главных идеалов // Дискретная математика. — 2007. — Т. 19. Вып. 1. — С. 50–59.

2. Анашин В.С. Равномерно распределенные последовательности целых p -адических чисел // Математические заметки. — 1994. — Т. 55. Вып. 2. — С. 3–46.
3. Анашин В.С. Равномерно распределенные последовательности целых p -адических чисел // Дискретная математика. — 2004. — Т. 14. Вып. 4. — С. 3–64.
4. Глухов М.М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // Труды по дискретной математике. — 1997. — Т. 1. — С. 43–66.
5. Кнут Д. Искусство программирования. Основные алгоритмы. — 3-е изд. — М.: Вильямс, 2001. — Т. 1. — 720 с.
6. Ларин М.В. Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. — 2002. — Т. 14. Вып. 2. — С. 20–32.
7. Mullen G.L., Stevens H. Polynomial functions (mod m) // Acta Math. Hungarica. — 1984. — V. 44. No. 3–4. — P. 237–241.
8. Rivest R.R. Permutation polynomials modulo 2^w // Finite Fields and Their Appl. — 2001. — V. 7. No. 2. — P. 287–292.