О многочленах, значения которых кратны m

Н. Н. Осипов
e-mail: nnosipov@rambler.ru

§ 1. Постановка задачи

Пусть $\mathbb{Z}[x]$ — *кольцо многочленов* от переменной x с целыми коэффициентами. Фиксируем натуральное число m. Скажем, что многочлен $f(x) \in \mathbb{Z}[x]$ обладает *m-свойством*, если

$$f(a) \equiv 0 \pmod{m}$$

при любом $a \in \mathbb{Z}$. Очевидно, множество всех многочленов $f(x)$ с m-свойством образует *идеал* кольца $\mathbb{Z}[x]$, который мы обозначим через I_m.

Задача. Для произвольного натурального числа m дать описание идеала I_m.

Под описанием произвольного идеала I кольца $\mathbb{Z}[x]$ мы будем понимать указание конкретной *системы порождающих* этот идеал многочленов:

$$I = (g_1(x), \ldots, g_r(x)) = \{g_1(x)f_1(x) + \ldots + g_r(x)f_r(x) : f_i(x) \in \mathbb{Z}[x]\}.$$

Такое описание всегда возможно, поскольку по *теореме Гильберта о базисе* (см., например, [1], стр. 373) всякий идеал кольца $\mathbb{Z}[x]$ является конечно порождённым.

Ясно, что $(m) \subset I_m$, но m-свойством обладают не только многочлены, все коэффициенты которых делятся на m.

Пример 1. Пусть $m = p$ — простое число. Из *малой теоремы Ферма* непосредственно следует, что многочлен $x^p - x$ обладает p-свойством. □

Этот пример допускает следующее обобщение.

Пример 2. Пусть $m = p_1 \ldots p_t$ — *число Кармайкла*. Это значит, что $p_1, \ldots, p_t$ — различные простые числа, для которых выполнены сравнения

$$m - 1 \equiv 0 \pmod{p_i - 1}, \quad i = 1, \ldots, t. \tag{1}$$

Тогда многочлен $x^m - x$ обладает m-свойством. Действительно, достаточно обнаружить, что этот многочлен обладает p_i-свойством для каждого простого делителя p_i числа m, что вытекает из разложения

$$x^m - x = x(x^{m-1} - 1),$$

сравнений (1) и малой теоремы Ферма. □

Отметим, что многочлены в примерах 1 и 2 являются *нормированными*, т. е. имеют единичный старший коэффициент. Для произвольного m легко привести пример нормированного многочлена с m-свойством — таковым будет многочлен

$$x(x-1)\ldots(x-m+1).$$

Однако, вообще говоря, его степень m не является минимально возможной.

§ 2. Предварительные факты

Пусть R — произвольное коммутативное кольцо с единицей 1. *Суммой* идеалов I и J этого кольца называется идеал

$$I + J = \{x + y : x \in I, y \in J\}.$$

Произведением идеалов I и J называется идеал

$$IJ = \{x_1y_1 + \ldots + x_ky_k : x_i \in I, y_i \in J\,(i = 1, \ldots, k) \text{ и } k = 1, 2, \ldots\}.$$

Из этих определений непосредственно вытекает, что если идеалы I и J порождаются конечными системами $\{a_1, \ldots, a_r\}$ и $\{b_1, \ldots, b_s\}$ своих элементов, то идеалы $I + J$ и IJ будут порождаться системами

$$\{a_1, \ldots, a_r, b_1, \ldots, b_s\}, \quad \{a_1b_1, \ldots, a_1b_s, \ldots, a_rb_1, \ldots, a_rb_s\}$$

соответственно. Очевидно также, что всегда $IJ \subset I \cap J$.

Лемма. Если $I + J = R$, то $IJ = I \cap J$.

Доказательство. Пусть $a \in I$ и $b \in J$ таковы, что $a + b = 1$. Тогда для произвольного элемента $x \in I \cap J$ имеем

$$x = xa + xb.$$

Поскольку $xa \in IJ$ и $xb \in IJ$, получим $x \in IJ$. □

Далее пусть $R = \mathbb{Z}[x]$. Если числа m_1 и m_2 взаимно просты, то из *расширенного алгоритма Евклида* следует существование таких целых чисел a_1, a_2, что

$$m_1a_1 + m_2a_2 = 1.$$

Тогда $(m_1) + (m_2) = \mathbb{Z}[x]$. Действительно, для любого $f(x) \in \mathbb{Z}[x]$ имеем

$$m_1(a_1f(x)) + m_2(a_2f(x)) = f(x).$$

Тем более $I_{m_1} + I_{m_2} = \mathbb{Z}[x]$, поэтому по лемме

$$I_{m_1m_2} = I_{m_1}I_{m_2}.$$

По индукции это равенство распространяется на любое количество попарно взаимно простых чисел $m_1, \ldots, m_t$. В частности, если $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ — *каноническое разложение* числа m, то, взяв $m_i = p_i^{\alpha_i}$, $i = 1, \ldots, t$, получим

$$I_m = \prod_{i=1}^{t} I_{p_i^{\alpha_i}}.$$

Впрочем, есть и иное представление идеала I_m. Положим

$$m_i^* = \frac{m}{p_i^{\alpha_i}}, \quad i = 1, \ldots, t.$$

Тогда справедливо равенство

$$I_m = \sum_{i=1}^{t} (m_i^*) I_{p_i^{\alpha_i}}. \tag{2}$$

В самом деле, поскольку числа $m_1^*, \ldots, m_t^*$ взаимно просты в совокупности, имеем

$$m_1^* a_1 + \ldots + m_t^* a_t = 1$$

для некоторых целых чисел $a_1, \ldots, a_t$. Значит, для любого $f(x) \in I_m$ верно представление

$$f(x) = (m_1^* f(x))a_1 + \ldots + (m_t^* f(x))a_t,$$

при этом $m_i^* f(x) \in (m_i^*) I_{p_i^{\alpha_i}}$. Теперь равенство (2) очевидно.

Таким образом, для решения поставленной задачи достаточно найти описание идеала I_{p^α} для произвольного простого p и натурального α.

§ 3. Решение задачи в случае $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, где $\alpha_i \leqslant p_i$

Пусть сначала $m = p$ — простое число.

Теорема 1. Для любого простого числа p имеем

$$I_p = (x^p - x, p).$$

Доказательство. Пусть $f(x) \in I_p$. Разделим $f(x)$ на $x^p - x$ с остатком:

$$f(x) = (x^p - x) f_1(x) + r(x),$$

где $f_1(x)$, $r(x) \in \mathbb{Z}[x]$ и $k = \deg r(x) < p$. Ясно, что $r(x) \in I_p$. Но тогда $\Delta^l r(x) \in I_p$ при любом $l = 1, 2, \ldots$, где Δ — *разностный оператор*:

$$\Delta g(x) = g(x) - g(x-1).$$

Так как $\Delta^k r(x) = k! c_k$, где c_k — старший коэффициент $r(x)$, то c_k делится на p. Рассмотрев

$$r_1(x) = r(x) - c_k x^k \in I_p,$$

аналогично докажем, что старший коэффициент $r_1(x)$ тоже делится на p. И так далее. В итоге все коэффициенты $r(x)$ окажутся кратными p, т. е. $r(x) = p f_2(x)$, где $f_2(x) \in \mathbb{Z}[x]$. □

Теорема 2. Для любого простого числа p и натурального числа $\alpha \leqslant p$ имеем

$$I_{p^\alpha} = I_p^\alpha = ((x^p - x)^\alpha, p(x^p - x)^{\alpha-1}, \ldots, p^{\alpha-1}(x^p - x), p^\alpha).$$

Доказательство. Достаточно доказать для каждого $\beta = 1, 2, \ldots, p$ следующее утверждение: если многочлен

$$f(x) = \sum_{k=0}^{\beta-1} p^{\beta-1-k}(x^p - x)^k f_k(x)$$

обладает p^β-свойством, то все многочлены $f_k(x)$ обладают p-свойством.

При $\beta = 1$ доказывать нечего. Сделаем шаг $\beta \to \beta + 1$, где $\beta < p$. Пусть многочлен

$$f(x) = \sum_{k=0}^{\beta} p^{\beta-k}(x^p - x)^k f_k(x)$$

обладает $p^{\beta+1}$-свойством. Тогда

$$f(a+p) - f(a) \equiv 0 \pmod{p^{\beta+1}} \tag{3}$$

для любого $a \in \mathbb{Z}$. При $k = 0, 1, \ldots, \beta$ имеет место сравнение

$$p^{\beta-k}((a+p)^p - a - p)^k \equiv \sum_{l=0}^{k} (-1)^{k-l} C_k^l p^{\beta-l} (a^p - a)^l \pmod{p^{\beta+1}},$$

которое легко получить, воспользовавшись *биномом Ньютона*. Следовательно,

$$f(a+p) \equiv \sum_{k=0}^{\beta} \sum_{l=0}^{k} (-1)^{k-l} C_k^l p^{\beta-l} (a^p - a)^l f_k(a) \pmod{p^{\beta+1}}.$$

Поменяв порядок суммирования, правую часть этого сравнения можно привести к виду

$$\sum_{l=0}^{\beta} p^{\beta-l} (a^p - a)^l \sum_{k=l}^{\beta} (-1)^{k-l} C_k^l f_k(a) =$$

$$= f(a) + \sum_{l=0}^{\beta-1} p^{\beta-l} (a^p - a)^l \sum_{k=l+1}^{\beta} (-1)^{k-l} C_k^l f_k(a) = f(a) + \sum_{l=0}^{\beta-1} p^{\beta-l} (a^p - a)^l g_l(a),$$

где многочлены $g_l(x)$ имеют вид

$$g_l(x) = \sum_{k=l+1}^{\beta} (-1)^{k-l} C_k^l f_k(x), \quad l = 0, 1, \ldots, \beta - 1. \tag{4}$$

Таким образом, сравнение (3) равносильно сравнению

$$\sum_{l=0}^{\beta-1} p^{\beta-l} (a^p - a)^l g_l(a) \equiv 0 \pmod{p^{\beta+1}},$$

сократив которое на p, получим

$$\sum_{l=0}^{\beta-1} p^{\beta-1-l} (a^p - a)^l g_l(a) \equiv 0 \pmod{p^{\beta}}.$$

По индукции многочлены $g_0(x), \ldots, g_{\beta-1}(x)$ обладают p-свойством. Из равенств (4) теперь следует, что многочлены $f_1(x), \ldots, f_\beta(x)$ также обладают p-свойством. Но тогда и $f_0(x)$ обладает p-свойством. □

При $\alpha > p$ равенство

$$I_{p^\alpha} = I_p^\alpha$$

уже не выполняется. Например, идеал $I_{2^3} = I_8$ содержит многочлен

$$(x^2 - x)^2 + 2(x^2 - x),$$

который не принадлежит идеалу $I_2^3 = ((x^2-x)^3, 2(x^2-x)^2, 4(x^2-x), 8)$. Действительно, если

$$(x^2-x)^2 + 2(x^2-x) = (x^2-x)^3 f_1(x) + 2(x^2-x)^2 f_2(x) + 4(x^2-x) f_3(x) + 8 f_4(x)$$

для некоторых $f_i(x) \in \mathbb{Z}[x]$, то $f_4(x) = (x^2-x) f_5(x)$, где $f_5(x) \in \mathbb{Z}[x]$. Но тогда после сокращения на x^2-x и подстановки $x = 0$ получим противоречивое равенство:

$$2 = 4 f_3(0) + 8 f_5(0).$$

Основной результат этого параграфа — следующая

Теорема 3. Пусть каноническое разложение числа m таково, что

$$\alpha_i \leqslant p_i, \quad i = 1, \ldots, t.$$

Тогда имеет место равенство

$$I_m = (m) + \sum_{i=1}^{t} (m_i^*(x^{p_i} - x)^{\alpha_i}, m_i^* p_i (x^{p_i} - x)^{\alpha_i - 1}, \ldots, m_i^* p_i^{\alpha_i - 1}(x^{p_i} - x)).$$

В частности, идеал I_m порождается $1 + \alpha_1 + \ldots + \alpha_t$ многочленами.

Доказательство. Это непосредственное следствие равенства (2) и теоремы 2. □

В следующем параграфе мы укажем простой способ найти порождающую систему многочленов для идеала I_m в общем случае.

§ 4. Решение задачи для произвольного m

Пусть $g^*(x)$ — какой-нибудь конкретный нормированный многочлен с m-свойством. Разделим произвольный многочлен $f(x) \in I_m$ на $g^*(x)$ с остатком:

$$f(x) = g^*(x) f_1(x) + r(x),$$

где $\deg r(x) < n = \deg g^*(x)$ и $r(x) \in I_m$. Оказывается, каждый такой многочлен $r(x)$ допускает представление в виде

$$r(x) = a_0 g_0(x) + \ldots + a_{n-1} g_{n-1}(x),$$

где все $a_i \in \mathbb{Z}$, а система многочленов $g_0(x), \ldots, g_{n-1}(x)$ не зависит от $r(x)$. Найти эту систему многочленов можно, решив систему сравнений

$$r(a) \equiv 0 \pmod{m}, \quad a = 0, 1, \ldots, m-1, \tag{5}$$

относительно неизвестных коэффициентов многочлена

$$r(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}. \tag{6}$$

После этого можно было бы записать

$$I_m = (g^*(x), g_0(x), \ldots, g_{n-1}(x)).$$

Ясно, что в качестве $g^*(x)$ лучше выбирать многочлен с наименьшей возможной степенью.

Пример 3. Как уже отмечалось, идеал I_8 содержит многочлен

$$g^*(x) = (x^2 - x)^2 + 2(x^2 - x)$$

степени $n = 4$. Найдём все многочлены (6) с 8-свойством. Система сравнений (5) принимает вид

$$\begin{cases} c_0 \equiv 0 \pmod 8, \\ c_0 + c_1 + c_2 + c_3 \equiv 0 \pmod 8, \\ c_0 + 2c_1 + 4c_2 \equiv 0 \pmod 8, \\ c_0 + 3c_1 + c_2 + 3c_3 \equiv 0 \pmod 8, \\ c_0 + 4c_1 \equiv 0 \pmod 8, \\ c_0 - 3c_1 + c_2 - 3c_3 \equiv 0 \pmod 8, \\ c_0 - 2c_1 + 4c_2 \equiv 0 \pmod 8, \\ c_0 - c_1 + c_2 - c_3 \equiv 0 \pmod 8. \end{cases}$$

После *элементарных преобразований* получим равносильную систему сравнений

$$\begin{cases} c_0 \equiv 0 \pmod 8, \\ c_0 + c_1 + c_2 + c_3 \equiv 0 \pmod 8, \\ 2c_2 - 2c_3 \equiv 0 \pmod 8, \\ 2c_3 \equiv 0 \pmod 8, \end{cases}$$

откуда последовательно найдём

$$c_3 = 4a_3, \quad c_2 = 4a_2, \quad c_1 = 8a_1 - 4a_2 - 4a_3, \quad c_0 = 8a_0,$$

где все $a_i \in \mathbb{Z}$. Следовательно,

$$r(x) = a_0(8) + a_1(8x) + a_2(4x^2 - 4x) + a_3(4x^3 - 4x),$$

т. е. можно положить $g_0(x) = 8$, $g_1(x) = 8x$, $g_2(x) = 4x^2 - 4x$, $g_3(x) = 4x^3 - 4x$. □

Решение громоздкой системы сравнений (5) можно избежать, если перейти к рассмотрению так называемых целозначных многочленов.

§ 5. Целозначные многочлены

Многочлен $F(x)$ называется *целозначным*, если $F(a) \in \mathbb{Z}$ для любого $a \in \mathbb{Z}$. Из *интерполяционной формулы Лагранжа* следует, что любой целозначный многочлен $F(x)$ обязан иметь рациональные коэффициенты. Примером целозначного многочлена является многочлен вида

$$C_n(x) = \frac{x(x-1)\dots(x-n+1)}{n!},$$

где $n = \deg C_n(x)$ — любое натуральное число. Он имеет дробные коэффициенты, однако

$$C_n(a) = \begin{cases} (-1)^n C^n_{n-a-1}, & a < 0, \\ 0, & 0 \leqslant a < n, \\ C^n_a, & a \geqslant n, \end{cases}$$

т. е. $C_n(a) \in \mathbb{Z}$ при любом $a \in \mathbb{Z}$.

Основным фактом о целозначных многочленах является следующая теорема (см., например, [2], стр. 100).

Теорема 4. Многочлен $F(x)$ степени n является целозначным тогда и только тогда, когда он представим в виде

$$F(x) = b_0C_0(x) + b_1C_1(x) + b_2C_2(x) + \ldots + b_nC_n(x),$$

где все $b_i \in \mathbb{Z}$ и по определению $C_0(x) = 1$.

Доказательство. Очевидно, любой многочлен $F(x)$ указанного вида будет целозначным. Обратно, пусть $F(x)$ — некоторый целозначный многочлен степени n. Последовательно подберём целые числа b_0, b_1, b_2, …, b_n так, чтобы многочлен

$$G(x) = b_0C_0(x) + b_1C_1(x) + b_2C_2(x) + \ldots + b_nC_n(x)$$

обладал свойством: $G(a) = F(a)$ при $a = 0,\ 1,\ \ldots,\ n$. Для этого следует положить

$$b_0 = F(0), \quad b_1 = F(1) - b_0, \quad b_2 = F(2) - b_1C_1(2) - b_0$$

и т. д. Ясно, что такой многочлен $G(x)$ должен совпасть с многочленом $F(x)$, так как иначе многочлен $H(x) = F(x) - G(x)$ степени не выше n имел бы $n + 1$ корень. □

Как видно из доказательства, в действительности для целозначности многочлена $F(x)$ степени n достаточно, чтобы $F(a) \in \mathbb{Z}$ при $a = b,\ b + 1,\ \ldots,\ b + n$, где b — любое фиксированное целое число.

Теперь можно завершить решение поставленной задачи. Для данного m пусть n — наименьшее натуральное число, для которого $n!$ делится на m. Многочлен

$$g^*(x) = n!C_n(x) = x(x-1)\ldots(x-n+1)$$

обладает $n!$-свойством, а значит, и m-свойством. Из теоремы 4 следует, что всякий многочлен (6) с m-свойством представим в виде

$$r(x) = mb_0C_0(x) + mb_1C_1(x) + \ldots + mb_{n-1}C_{n-1}(x), \tag{7}$$

где все $b_i \in \mathbb{Z}$. Нужно выяснить, какими должны быть целые числа b_0, b_1, …, b_{n-1}, чтобы все коэффициенты многочлена (7) оказались целыми.

Пример 4. При $m = 8$ получим $n = 4$. Коэффициенты многочлена (7) имеют вид

$$c_0 = 8b_0, \quad c_1 = 8b_1 - 4b_2 + \frac{8b_3}{3}, \quad c_2 = 4b_2 - 4b_3, \quad c_3 = \frac{4b_3}{3}.$$

Сразу видно, что для целочисленности всех коэффициентов необходимо и достаточно, чтобы $b_3 = 3a_3$, где $a_3 \in \mathbb{Z}$. □

В общем случае можно рассуждать так. Коэффициент при x^{n-1} у многочлена (7) равен

$$\frac{mb_{n-1}}{(n-1)!}.$$

Это число должно быть целым, а так будет только если

$$b_{n-1} = \frac{(n-1)!a_{n-1}}{d_1}, \quad d_1 = \text{НОД}\,(m, (n-1)!),$$

где $a_{n-1} \in \mathbb{Z}$. В этом случае все коэффициенты многочлена

$$mb_{n-1}C_{n-1}(x) = a_{n-1}l_1C_{n-1}(x), \quad l_1 = \frac{m(n-1)!}{d_1} = \text{НОК}\,(m, (n-1)!),$$

также будут целыми числами. Аналогично, у многочлена

$$r(x) - a_{n-1}l_1C_{n-1}(x) = mb_0 + mb_1C_1(x) + \ldots + mb_{n-2}C_{n-2}(x)$$

коэффициент при x^{n-2} должен быть целым, поэтому

$$b_{n-2} = \frac{(n-1)!a_{n-2}}{d_2}, \quad d_2 = \text{НОД}\,(m, (n-2)!).$$

И так далее. В итоге получим

$$r(x) = a_0l_nC_0(x) + a_1l_{n-1}C_1(x) + \ldots + a_{n-1}l_1C_{n-1}(x), \tag{8}$$

где $l_k = \text{НОК}\,(m, (n-k)!)$, $k = 1, \ldots, n$. Таким образом, в качестве искомой системы многочленов $g_0(x), \ldots, g_{n-1}(x)$ можно взять

$$g_k(x) = l_{n-k}C_k(x), \quad k = 0, 1, \ldots, n-1.$$

Кроме того, из формулы (8) вытекает, что любой многочлен с m-свойством, имеющий степень меньше n, не может быть нормированным. Действительно, из определения числа n следует, что

$$l_{n-k} = \text{НОК}\,(m, k!) > k!, \quad k = 0, 1, \ldots, n-1,$$

поэтому старший коэффициент любого из многочленов $g_k(x)$ больше единицы.

Пример 5. Пусть $m = p^\alpha$, где $\alpha \leqslant p$. Тогда $n = p\alpha$, ибо при $n < p\alpha$ по *формуле Лежандра* мы получили бы

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots < \alpha,$$

т. е. $n!$ не делилось бы на p^α. Поэтому многочлен $(x^p - x)^\alpha$ является нормированным многочленом наименьшей степени, обладающим p^α-свойством.

Отметим кстати, что в случае $m = p^{p+1}$ получим $n = p^2$, поскольку

$$\nu_p(p^2!) = p + 1.$$

Одним из нормированных многочленов наименьшей степени, имеющих p^{p+1}-свойство, будет $x(x-1)\ldots(x-p^2+1)$. □

Список литературы

[1] *Винберг Э.Б.* Курс алгебры. М.: Изд-во «Факториал Пресс», 2001.

[2] *Прасолов В.В.* Многочлены. М.: МЦНМО, 2001.