

Алгебра. Глава 4. Многочлены и теория чисел.

Д. В. Карпов

2024

Показатель, к которому принадлежит вычет

Определение

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$, $d \in \mathbb{N}$. Вычет a *принадлежит к показателю* d , если $a^d = 1$, но $a^s \neq 1$ при $s \in \mathbb{N}$, $s < d$.

Обозначение: $a \in_p d$.

Лемма 1

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$. Тогда выполнены следующие утверждения.

1) Если $a^d = 1$ и $a \in_p s$, то $s \mid d$.

2) Если $a \in_p d$, то $d \mid p - 1$.

Доказательство. 1) • Предположим противное и поделим d на s с остатком: $d = sq + r$, $0 < r < s$.

• Тогда $1 = a^d = a^{sq+r} = (a^s)^q \cdot a^r = a^r$,

что противоречит минимальности s .

2) По теореме Эйлера $a^{p-1} = 1$. Тогда по пункту 1 имеем $d \mid p - 1$.

Лемма 2

Если $p \in \mathbb{P}$ и $d \mid p - 1$, то многочлен $t^d - 1 \in \mathbb{Z}_p[t]$ имеет ровно d корней, все они не 0.

Доказательство. • Многочлен $t^{p-1} - 1$ имеет в $\mathbb{Z}_p[t]$ ровно $p - 1$ корень (по теореме Эйлера, все ненулевые вычеты его корни).

• Пусть $p - 1 = qd$. Тогда

$$t^{p-1} - 1 = (t^d - 1)(t^{(q-1)d} + \dots + t^d + 1) =: (t^d - 1)f(t).$$

• Так как $\deg(f) = (q - 1)d$, этот многочлен по Теореме 3.7 имеет не более $(q - 1)d$ корней.

• Если $t^d - 1$ имеет менее d корней, то

$t^{p-1} - 1 = (t^d - 1)f(t)$ имеет менее $d + (q - 1)d = p - 1$ корней, противоречие. \square

Теорема 1

Если $p \in \mathbb{P}$ и $d \mid p - 1$, то к показателю d принадлежит ровно $\varphi(d)$ вычетов.

Доказательство. • Индукция по d . База $d = 1$ очевидна:
 $a \in_p 1 \iff a = 1$.

- Все вычеты, принадлежащие к показателю d , являются корнями многочлена $t^d - 1$.
- Если $s \mid d$ (скажем, $d = qs$) и $b \in_p s$, то $b^d = (b^s)^q = 1$, то есть, b — корень $t^d - 1$.
- Так как каждый ненулевой вычет принадлежит в точности одному показателю, вычеты, принадлежащие собственным делителям d дают нам

$$\sum_{s \mid d, s < d} \varphi(s) = \left(\sum_{s \mid d} \varphi(s) \right) - \varphi(d) = d - \varphi(d) \quad \text{различных}$$

корней многочлена $t^d - 1$ (последнее равенство верно по Теореме 2.17).

- Оставшиеся $d - (d - \varphi(d)) = \varphi(d)$ корней многочлена $t^d - 1$ принадлежат к d (по Лемме 1 они должны принадлежать к делителю d , а этим делителем может быть только само d). \square

Первообразный корень по модулю p

Определение

Пусть $p \in \mathbb{P}$. Вычет $a \in \mathbb{Z}_p$ — **первообразный корень по модулю p** , если $a \in_p p - 1$.

- По Теореме 1 существует в точности $\varphi(p - 1)$ первообразных корней по модулю p .

Теорема 2

Пусть $p \in \mathbb{P}$, a — первообразный корень по модулю p . Тогда $a, a^2, \dots, a^{p-1} = 1$ — ПрСВ $(\text{mod } p)$, то есть, в точности все ненулевые вычеты из \mathbb{Z}_p .

Доказательство. • Достаточно доказать, что $a^i \neq a^j$ при $1 \leq j < i \leq p - 1$.

- Предположим противное, пусть $a^i = a^j \iff a^j(a^{i-j} - 1) = 0$.
- Однако, $a^j \neq 0$ и $a^{i-j} \neq 1$, так как $0 < i - j < p - 1$.

Противоречие. □

- Если a — первообразный корень по модулю p , то любой ненулевой вычет $b \in \mathbb{Z}_p$ представляется в виде $b = a^k$, где $1 \leq k \leq p - 1$.

Определение

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$.

- Тогда a — **квадратичный вычет**, если существует такой $b \in \mathbb{Z}_p$, что $b^2 = a$.
- Если такого b не существует, то a — **квадратичный невычет**.
- Далее в этом разделе p — нечетное простое число.

Лемма 3

Пусть $p \in \mathbb{P}$ нечетно, $p_1 := \frac{p-1}{2}$. Тогда:

- 1) квадратичные вычеты в \mathbb{Z}_p — корни многочлена $t^{p_1} - 1$;
- 2) если $x^2 = y^2$, то $x = y$ или $x = -y$;
- 3) существует в точности $\frac{p-1}{2}$ квадратичных вычетов в \mathbb{Z}_p .

Доказательство. 1) • Если a — квадратичный вычет, то $a = b^2$ в \mathbb{Z}_p .

• По Теореме Эйлера $a^{p_1} - 1 = b^{2p_1} - 1 = b^{p-1} - 1 = 0$.

2)

$x^2 = y^2 \iff (x+y)(x-y) = 0 \iff x = y$ или $x = -y$.

3) Из пункта 2 следует, что ненулевые вычеты из \mathbb{Z}_p разбиваются на $\frac{p-1}{2}$ пар вида $\{x, -x\}$, дающих одинаковый квадрат. Значит, существует ровно $\frac{p-1}{2}$ квадратичных вычетов по модулю p . □

Лемма 4

Пусть $p \in \mathbb{P}$ нечетно, $p_1 := \frac{p-1}{2}$. Тогда выполнены следующие утверждения.

- 1) Квадратичные невычеты в \mathbb{Z}_p — корни многочлена $t^{p_1} + 1$.
- 2) Существует в точности $\frac{p-1}{2}$ квадратичных невычетов в \mathbb{Z}_p .

Доказательство. • По Теореме Эйлера многочлен $t^{p-1} - 1 = (t^{p_1} - 1)(t^{p_1} + 1)$ имеет в \mathbb{Z}_p ровно $p - 1$ корень — все ненулевые вычеты.

• Многочлен $t^{p_1} - 1$ имеет ровно p_1 корней, как мы знаем из Леммы 2. По Лемме 3 все эти корни — квадратичные вычеты.

• Все p_1 ненулевых вычетов, не являющиеся корнями $t^{p_1} - 1$, являются корнями многочлена $t^{p_1} + 1$.

• Значит, и многочлен $t^{p_1} + 1$ имеет ровно p_1 корней — в точности все квадратичные невычеты. □

Лемма 5

Пусть $p \in \mathbb{P}$ нечетно, $a, b \in \mathbb{Z}_p$, $a \neq 0$, $b \neq 0$. Тогда:

- 1) Если a, b — квадратичные вычеты, то ab — квадратичный вычет.
- 2) Если a — квадратичный вычет, а b — квадратичный невычет, то ab — квадратичный невычет.
- 3) Если a, b — квадратичные невычеты, то ab — квадратичный вычет.

Доказательство. 1) Существуют такие $x, y \in \mathbb{Z}_p$, что $a = x^2$ и $b = y^2$. Тогда $ab = (xy)^2$.

2) • Вычеты $a, 2a, \dots, (p-1)a$ — это в точности все ненулевые элементы \mathbb{Z}_p : среди них нет 0 и все они различны, так как $ai = aj \Rightarrow i = j$ (равенство можно домножить на a^{-1} .)

• Значит, среди $a, 2a, \dots, (p-1)a$ ровно по $\frac{p-1}{2}$ квадратичных вычетов и квадратичных невычетов.

• Так как при умножении a на квадратичные вычеты (на все $\frac{p-1}{2}$ штук) по пункту 1 получаются различные квадратичные вычеты (все $\frac{p-1}{2}$ штук), то при умножении a на квадратичные невычеты получаются квадратичные невычеты.

3) • И на этот раз $a, 2a, \dots, a(p-1)$ — это в точности все ненулевые элементы \mathbb{Z}_p , среди них ровно по $\frac{p-1}{2}$ квадратичных вычетов и квадратичных невычетов.

• Так как при умножении a на квадратичные вычеты (на все $\frac{p-1}{2}$ штук) по пункту 2 получаются различные квадратичные невычеты (все $\frac{p-1}{2}$ штук), то при умножении a на квадратичные невычеты получаются квадратичные вычеты. □

Решение квадратных уравнений в \mathbb{Z}_p

- Пусть $p \in \mathbb{P}$, $p \neq 2$, $a, b, c \in \mathbb{Z}_p$, $a \neq 0$, $D = b^2 - 4ac$.

$$ax^2 + bx + c = 0 \iff x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \iff$$
$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a} = \frac{b^2 - 4ac}{4a^2} \iff \left(x + \frac{b}{2a}\right)^2 = \frac{D}{4a^2}.$$

- Если D — квадратичный вычет, то $D = d^2$ для некоторого $d \in \mathbb{Z}_p$ и $\frac{D}{4a^2} = \left(\frac{\pm d}{2a}\right)^2$. Тогда уравнение имеет два решения:

$$x_1 = \frac{-b+d}{2a} \quad \text{и} \quad x_2 = \frac{-b-d}{2a}.$$

- Если $D = 0$, то уравнение имеет одно решение:

$$x_1 = \frac{-b}{2a}.$$

- Если D — квадратичный невычет, то $\frac{D}{4a^2}$ — также квадратичный невычет, а значит, решений нет (так как квадратичный невычет не может быть равен квадрату).

Квадратичные вычеты по модулю p . Символ Лежандра

Определение

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$.

- Тогда a — **квадратичный вычет** по модулю p , если вычет a в \mathbb{Z}_p — квадратичный вычет.
- Аналогично, a — **квадратичный невычет** по модулю p , если вычет a в \mathbb{Z}_p — квадратичный невычет.

Определение

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}$. Тогда **символ Лежандра**

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p; \\ 0, & \text{если } a \equiv 0 \pmod{p}. \end{cases}$$

Свойство 1

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Доказательство. • a — квадратичный вычет по модулю p

$$\iff \bar{a} \text{ — квадратичный вычет в } \mathbb{Z}_p \iff (\bar{a})^{\frac{p-1}{2}} = 1.$$

• a — квадратичный невычет по модулю p \iff

$$\bar{a} \text{ — квадратичный невычет в } \mathbb{Z}_p \iff (\bar{a})^{\frac{p-1}{2}} = -1.$$

• $a = 0 \iff a^{\frac{p-1}{2}} = 0.$ □

Свойство 2

(Первое дополнение к закону взаимности Гаусса.)

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Свойство 3

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Доказательство. • Следует из Леммы 5 и определения символа Лежандра. □

Лемма 6

Пусть $p \in \mathbb{P}$, $p_1 = \frac{p-1}{2}$, $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$. Тогда

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right]}.$$

Доказательство. • Пусть $M = \{1, 2, \dots, p_1\}$.

Утверждение 1

Для каждого $j \in M$ существует $s_j \in \{0, 1\}$ и $r_j \in M$ такие, что $ja \equiv (-1)^{s_j} r_j \pmod{p}$.

Доказательство. • Пусть r'_j — остаток от деления ja на p .

- Если $r'_j \in M$, то положим $r_j := r'_j$, $s_j = 0$.
- Если $r'_j \notin M$, то $r'_j \in \{p_1 + 1, \dots, p - 1\}$, тогда $p - r'_j \in \{1, \dots, p - 1 - p_1 = p_1\} = M$.
- В этом случае положим $r_j = p - r'_j$, $s_j = 1$. □

Утверждение 2

Если $i, j \in M$, $i \neq j$, то $r_i \neq r_j$.

Доказательство. • Предположим противное, пусть $r_i = r_j$.

- Если $s_i = s_j$, то $r'_i = r'_j$.
- Следовательно, $ia \equiv_p ja \iff a(i-j) \div p \Rightarrow i-j \div p$,
что не так (последний переход верен, так как $(a, p) = 1$).
- Если $s_i \neq s_j$, то $r'_i = p - r'_j$.
- Следовательно, $ia \equiv_p -ja \iff a(i+j) \div p \Rightarrow i+j \div p$,
что не так: $2 \leq i+j \leq 2p_1 = p-1$. □

Утверждение 3

$$s_j = 1 \iff \left[\frac{2aj}{p} \right] \not\equiv 2.$$

Доказательство. • Напомним, что

$$aj = pq + r'_j \iff 2aj = 2pq + 2r'_j, \text{ где } r'_j \in \{1, \dots, p-1\}.$$

$$\begin{aligned} s_j = 1 &\iff \frac{p+1}{2} = p_1 + 1 \leq r'_j \leq p-1 \iff \\ p+1 \leq 2r'_j \leq 2p-2 &\iff p+1+2pq \leq 2aj \leq 2p-2+2pq \iff \\ p+2pq < 2aj < 2p+2pq &\iff \\ 2q+1 < \frac{2aj}{p} < 2q+2 &\iff \left[\frac{2aj}{p} \right] = 2q+1 \not\equiv 2. \end{aligned}$$

• **Пояснение 1.** Так как разность целых чисел не менее 1,

$$p+1+2pq \leq 2aj \iff p+2pq < 2aj.$$

• **Пояснение 2.** Так как разность четных чисел не менее 2,

$$2aj \leq 2p-2+2pq \iff 2aj < 2p+2pq. \quad \square$$

- Вернемся к доказательству Леммы 6. По Утверждению 2, $\{r_1, \dots, r_{p_1}\} = M$ (так как все эти числа из M и различны, а $|M| = p_1$).
- Пусть $R = 1 \cdot 2 \cdot \dots \cdot p_1$. Тогда $r_1 r_2 \cdot \dots \cdot r_{p_1} = R$.
- Напишем цепочку сравнений:

$$(-1)^{\sum_{x=1}^{p_1} s_x} R \equiv (-1)^{\sum_{x=1}^{p_1} s_x} \cdot \prod_{x=1}^{p_1} r_x \equiv$$

$$\prod_{x=1}^{p_1} (-1)^{s_x} r_x \equiv \prod_{x=1}^{p_1} ax \pmod{p} \equiv a^{p_1} R \pmod{p} \quad (1).$$

- Сокращая (1) на R (можно, так как $(R, p) = 1$),

получаем $a^{p_1} \equiv (-1)^{\sum_{x=1}^{p_1} s_x} \equiv (-1)^{\sum_{x=1}^{p_1} [\frac{2ax}{p}]} \pmod{p}$
(последний переход верен по Утверждению 3). □

Лемма 7

Пусть $p \in \mathbb{P}$, $p_1 = \frac{p-1}{2}$.

1) (Второе дополнение к закону взаимности Гаусса.)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

2) Пусть $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$ и $a \not\equiv 2 \pmod{2}$. Тогда $\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]}$.

Доказательство. 1) • Тогда $\frac{p+a}{2} \in \mathbb{Z}$, применим Лемму 6:

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{p+a}{p}\right) = \left(\frac{2\frac{p+a}{2}}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{\frac{p+a}{2}}{p}\right) = \\ &= \left(\frac{2}{p}\right) \cdot (-1)^{\sum_{x=1}^{p_1} \left[\frac{2x\frac{p+a}{2}}{p}\right]} = \left(\frac{2}{p}\right) \cdot (-1)^{\sum_{x=1}^{p_1} (x + \left[\frac{ax}{p}\right])} = \\ &= \left(\frac{2}{p}\right) \cdot (-1)^{\sum_{x=1}^{p_1} x} \cdot (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]} = \left(\frac{2}{p}\right) \cdot (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]}. \quad (1) \end{aligned}$$

• Подставим $a = 1$ в (1) и учтем, что при $1 \leq x \leq p_1$ выполнено $\left[\frac{x}{p}\right] = 0$:

$$1 = \left(\frac{1}{p}\right) = \left(\frac{2}{p}\right) \cdot (-1)^{\frac{p^2-1}{8}}, \text{ откуда следует, что } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

2) Теперь (1) можно продолжить так:

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{2}{p}\right) \cdot (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]} = \\ &= \left((-1)^{\frac{p^2-1}{8}}\right)^2 \cdot (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]} = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]}. \quad \square \end{aligned}$$

Теорема 3

(Закон взаимности Гаусса.)

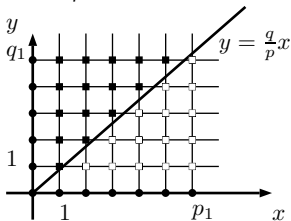
Пусть $p, q \in \mathbb{P}$ нечетны. Тогда $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Доказательство. • Пусть $p_1 := \frac{p-1}{2}$ и $q_1 := \frac{q-1}{2}$.

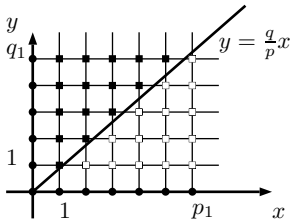
• По Лемме 7, $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{qx}{p}\right] + \sum_{y=1}^{q_1} \left[\frac{py}{q}\right]}$.

• Нам нужно доказать, что $\sum_{x=1}^{p_1} \left[\frac{qx}{p}\right] + \sum_{y=1}^{q_1} \left[\frac{py}{q}\right] = p_1 q_1$.

- Рассмотрим клетчатую решетку, проведем на ней прямую ℓ , заданную уравнением $y = \frac{q}{p}x$.
- Так как $(p, q) = 1$, при $x \leq p_1$ на этой прямой нет узлов — точек с целыми координатами. Аналогично, при $y \leq q_1$ на этой прямой нет узлов. (Ближайший к началу координат узел в 1 четверти на ℓ — это точка с координатами $x = p$, $y = q$.)
- На вертикалях с абсциссами $x \in \{1, 2, \dots, p_1\}$ отметим все узлы с положительными ординатами, лежащие под прямой ℓ (белые квадратики на рисунке). На вертикали с абсциссой x отмечено в точности $\lfloor \frac{qx}{p} \rfloor$ узлов.
- На горизонталях с ординатами $y \in \{1, 2, \dots, q_1\}$ отметим все узлы с положительными абсциссами, лежащие над прямой ℓ (черные квадратики на рисунке). На вертикали с ординатой y отмечено в точности $\lfloor \frac{py}{q} \rfloor$ узлов.



- В сумме мы отметили ровно $\sum_{x=1}^{p_1} \left[\frac{qx}{p} \right] + \sum_{y=1}^{q_1} \left[\frac{py}{q} \right]$ узлов.
- Так как прямая ℓ не проходит через узлы с рассматриваемыми абсциссами и ординатами, каждый узел с абсциссой от 1 до p_1 и с ординатой от 1 до q_1 отмечен ровно один раз (он либо над ℓ , либо под ℓ).
- Значит, отмечено ровно $p_1 q_1$ узлов. □



Кольцо многочленов $\mathbb{Z}[t]$. Содержание многочлена.

Определение

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$. Тогда его **содержание** $c(f) = (a_0, \dots, a_n)$ (НОД коэффициентов).

Лемма 8

(Лемма Гаусса.) Пусть $f, g \in \mathbb{Z}[x]$, $c(f) = c(g) = 1$. Тогда $c(fg) = 1$.

Доказательство. • Предположим противное и рассмотрим такое $p \in \mathbb{P}$, что $c(fg) \vdots p$. Однако, $c(f) \not\vdots p$ и $c(g) \not\vdots p$.

• Пусть $f(t) = a_n t^n + \dots + a_0$ и $g(t) = b_m t^m + \dots + b_0$. Рассмотрим такой наименьший индекс k , что $a_k \not\vdots p$ и такой наименьший индекс ℓ , что $b_\ell \not\vdots p$.

• Пусть $fg = d_{m+n} t^{n+m} + \dots + d_0$. Тогда

$$d_{k+\ell} = \left(\sum_{i=0}^{k-1} a_i b_{k+\ell-i} \right) + a_k b_\ell + \left(\sum_{i=k+1}^{k+\ell} a_i b_{k+\ell-i} \right) \not\vdots p,$$

так как первая сумма делится на p

($a_i \vdots p$ при $i \in \{0, \dots, k-1\}$) и вторая сумма делится на p

(при $i \in \{k+1, \dots, k+\ell\}$ мы имеем $k+\ell-i \in \{0, \dots, \ell-1\}$,

а значит, $b_{k+\ell-i} \vdots p$), а $a_k b_\ell \not\vdots p$.

• Значит, $c(fg) \not\vdots p$, противоречие.

Следствие 1

Для $f, g \in \mathbb{Z}[x]$ выполнено $c(fg) = c(f)c(g)$.

Доказательство. • Пусть $f(t) = c(f) \cdot f_1(t)$ и $g(t) = c(g) \cdot g_1(t)$.

• Тогда $f_1, g_1 \in \mathbb{Z}[t]$ и $c(f_1) = c(g_1) = 1$ и по Лемме Гаусса $c(f_1g_1) = 1$.

• Следовательно,

$c(fg) = c(c(f) \cdot f_1 \cdot c(g) \cdot g_1) = c(f)c(g) \cdot c(f_1g_1) = c(f)c(g)$
(мы воспользовались тем, что общий множитель $c(f)c(g)$ при вычислении НОД коэффициентов можно вынести). \square

Лемма 9

Пусть $f \in \mathbb{Z}[x]$, $q_1, \dots, q_n \in \mathbb{Q}[x]$, $f = q_1 \dots q_n$, $\deg(q_i) \geq 1$ для всех $i \in \{1, \dots, n\}$. Тогда существуют такие $p_1, \dots, p_n \in \mathbb{Z}[x]$ и $c_1, \dots, c_n \in \mathbb{Q}$, что $f = p_1 \dots p_n$ и $p_i = c_i q_i$ для всех $i \in \{1, \dots, n\}$.

Доказательство. • Для каждого $i \in \{1, \dots, n\}$ представим все коэффициенты q_i в виде несократимых дробей, пусть m_i — НОК знаменателей этих коэффициентов.

• Тогда $g_i = m_i q_i \in \mathbb{Z}[x]$ и $mf = g_1 \dots g_n$, где $m = m_1 \dots m_n \in \mathbb{N}$.

Утверждение

Пусть $mf = g_1 \dots g_n$, где $m \in \mathbb{N}$, $f, g_1, \dots, g_n \in \mathbb{Z}[x]$. Тогда существует разложение $f = p_1 \dots p_n$, где $p_i = d_i g_i \in \mathbb{Z}[x]$, $d_i \in \mathbb{Q}$ для всех $i \in \{1, \dots, n\}$.

Доказательство. Индукция по m .

База $m = 1$: построенное разложение $f = g_1 \dots g_n$ подходит.

Переход. • Пусть для меньших m утверждение доказано, $p \in \mathbb{P}$, $m \vdots p$.

• Тогда $c(g_1) \dots c(g_n) = c(g_1 \dots g_n) = c(m \cdot f) \vdots p$, значит, существует такое $i \in \{1, \dots, n\}$, что $c(g_i) \vdots p$.

• НУО $c(g_1) \vdots p$. Тогда $g_1 = p \cdot g_1^*$, где $g_1^* \in \mathbb{Z}[x]$.

• Пусть $m^* := \frac{m}{p}$. Тогда $m^* \in \mathbb{Z}$ и $m^* f = g_1^* g_2 \dots g_n$.

• Так как $m^* < m$, по индукционному предположению существует разложение $f = p_1 \dots p_n$, где $p_1 = d_1^* g_1^*$ и $p_i = d_i g_i$ при $i \in \{2, \dots, n\}$.

• Положим $d_1 := \frac{d_1^*}{p}$. Тогда $p_1 = d_1 g_1$, получено разложение для m . □

• Для завершения доказательства леммы остается положить $c_i := d_i m_i$.

Связь неприводимости в $\mathbb{Q}[x]$ и в $\mathbb{Z}[x]$

- Если многочлен $f \in \mathbb{Z}[x]$ неприводим в $\mathbb{Q}[x]$, то он, очевидно, неприводим и в $\mathbb{Z}[x]$.

Следствие 2

Многочлен $f \in \mathbb{Z}[x]$ неприводим в $\mathbb{Q}[x]$, если и только если он неприводим в $\mathbb{Z}[x]$.

Доказательство. \Rightarrow . Если многочлен $f \in \mathbb{Z}[x]$ приводим в $\mathbb{Z}[x]$, то он, очевидно, приводим и в $\mathbb{Q}[x]$.

\Leftarrow . • Предположим противное, пусть f приводим в $\mathbb{Q}[x]$.

• Тогда $f = g_1 g_2$, где $g_1, g_2 \in \mathbb{Q}[x]$, $1 \leq \deg(g_1) < \deg(f)$ и $1 \leq \deg(g_2) < \deg(f)$.

• По Лемме 9, существует разложение $f = h_1 h_2$, где $h_1, h_2 \in \mathbb{Z}[x]$, $h_1 = c g_1$ и $h_2 = c' g_2$, $c, c' \in \mathbb{Q}$.

• Тогда f приводим в $\mathbb{Z}[x]$, противоречие. □

Основная теорема арифметики в $\mathbb{Z}[t]$

Определение

Многочлен $f \in \mathbb{Z}[t]$ — *тривиальный*, если $c(f) = 1$.

Теорема 4

Любой многочлен $f \in \mathbb{Z}[x]$ с положительным старшим коэффициентом раскладывается в произведение $f = r_1 \dots r_k \cdot p_1 \dots p_n$, где $r_1, \dots, r_k \in \mathbb{P}$, а $p_1, \dots, p_n \in \mathbb{Z}[x]$ — тривиальные неприводимые многочлены с положительными старшими коэффициентами. Разложение единственно с точностью до перестановки сомножителей.

- Разумеется, многочлен $f \in \mathbb{Z}[x]$ с отрицательным старшим коэффициентом раскладывается в аналогичное произведение $f = -r_1 \dots r_k \cdot p_1 \dots p_n$.

Доказательство. \exists • Пусть $f = c(f) \cdot g$, тогда $g \in \mathbb{Z}[x]$ и $c(g) = 1$. По ОТА в \mathbb{Z} существует разложение на простые множители $c(f) = r_1 \dots r_k$.

- Пусть a — старший коэффициент g . Тогда $a > 0$.
- По ОТА в $\mathbb{Q}[x]$ существует разложение $g = aq'_1 q_2 \dots q_n$, где q'_1, q_2, \dots, q_n — неприводимые в $\mathbb{Q}[x]$ многочлены.
- Положим $q_1 := aq'_1$, тогда q_1 также неприводим в $\mathbb{Q}[x]$.
- Итак, $g = q_1 q_2 \dots q_n$.
- По Лемме 9 существует разложение $g = p_1 \dots p_n$, где $p_i \in \mathbb{Z}[x]$ и $p_i = c_i q_i$, $c_i \in \mathbb{Q}$.
- Можно считать, что старший коэффициент каждого p_i положителен: иначе заменим p_i на $-p_i$ и c_i на $-c_i$.
- Так как $p_i \sim q_i$ в $\mathbb{Q}[x]$, многочлены p_1, \dots, p_n неприводимы в $\mathbb{Q}[x]$, а значит, и в $\mathbb{Z}[x]$.
- Тогда $f = r_1 \dots r_k \cdot p_1 \dots p_n$.
- По Следствию 1 имеем $c(f) = c(r_1 \dots r_k \cdot p_1 \dots p_n) = r_1 \dots r_k \cdot c(p_1) \dots c(p_n) = c(f) \cdot c(p_1) \dots c(p_n)$, откуда $c(p_1) = \dots = c(p_n) = 1$.
- Значит, $f = r_1 \dots r_k \cdot p_1 \dots p_n$ — искомое разложение.

! • Предположим, что разложение не единственно:

$$f = r_1 \dots r_k p_1 \dots p_n = s_1 \dots s_\ell q_1 \dots q_m, \quad (1)$$

где $r_1, \dots, r_k, s_1, \dots, s_\ell \in \mathbb{P}$ и $p_1 \dots p_n, q_1 \dots q_m \in \mathbb{Z}[x]$ — неприводимые тривиальные многочлены с положительными старшими коэффициентами.

• По Лемме 8, тогда $c(p_1 \dots p_n) = c(p_1) \dots c(p_n) = 1$, откуда $c(f) = r_1 \dots r_k$ — разложение на простые множители.

Аналогично, $c(f) = s_1 \dots s_\ell$ — разложение на простые множители.

• По ОТА в \mathbb{Z} , эти разложения могут отличаться только порядком множителей, что нам и надо.

• Пусть $g := \frac{1}{c(f)} f \in \mathbb{Z}[x]$, тогда $g = p_1 \dots p_n = q_1 \dots q_m$ — два разложения g в произведение неприводимых в $\mathbb{Z}[x]$ тривиальных многочленов.

• По Следствию 2 это два разложения g в произведение неприводимых многочленов в $\mathbb{Q}[x]$.

- Пусть p_i^* — многочлен, полученный из p_i делением на старший коэффициент (для всех $i \in \{1, \dots, n\}$), а q_j^* — многочлен, полученный из q_j делением на старший коэффициент (для всех $j \in \{1, \dots, m\}$), а a — старший коэффициент f .
- Тогда $g = ap_1^* \dots p_n^* = aq_1^* \dots q_m^*$ — два разложения g в $\mathbb{Q}[x]$ в произведение неприводимых многочленов со старшим коэффициентом 1, а по ОТА в $\mathbb{Q}[x]$ (Теорема 3.5) такие разложения могут отличаться лишь порядком сомножителей.
- Значит, $m = n$ и можно считать, что $p_i^* = q_i^*$ для всех i .
- Тогда существует такое $c_i \in \mathbb{Q}$, что $p_i = c_i q_i$. Тогда $c_i > 0$ (так как c_i равно отношению положительных старших коэффициентов p_i и q_i).
- Нам остается доказать, что $c_1 = \dots = c_n = 1$. Пусть это не так. Из (1) ясно, что $c_1 c_2 \dots c_n = 1$. Значит, НУО $c_1 > 1$.
- Пусть $c_1 = \frac{a_1}{b_1}$ — представление в виде несократимой дроби. Тогда $(a_1, b_1) = 1$, $a_1 > 1$.
- Пусть $q_1(t) = d_w t^w + \dots + d_0$, тогда $p_1(t) = \frac{a_1 d_w}{b_1} t^w + \dots + \frac{a_1 d_0}{b_1}$.
- Так как $(a_1, b_1) = 1$, для всех $i \in \{1, \dots, w\}$ мы имеем $\frac{a_1 d_i}{b_1} \vdots a_1$. Значит, $1 = c(p_1) \vdots a_1$, противоречие.



Критерий Эйзенштейна

Теорема 5

Пусть $f(x) = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{Z}[t]$ и $p \in \mathbb{P}$ таковы, что $a_n \not\equiv p$, $a_{n-1}, \dots, a_0 \equiv p$ и $a_0 \not\equiv p^2$. Тогда f — неприводим в $\mathbb{Z}[t]$.

Доказательство. • Предположим противное. Пусть $f = gh$, где $\deg(g) > 0$ и $\deg(h) > 0$.

• Пусть $g(t) = b_m t^m + \dots + b_0$, $h(t) = c_k t^k + \dots + c_0$ (тогда $m + k = n$).

• Так как $c_0 b_0 = a_0 \equiv p$ и $c_0 b_0 \not\equiv p^2$, НУО $b_0 \equiv p$ и $c_0 \not\equiv p$.

• Так как $b_m c_k = a_n \not\equiv p$, мы имеем $b_m \not\equiv p$. Следовательно, можно выбрать наименьший такой индекс ℓ , что $b_\ell \not\equiv p$.

• Тогда $a_\ell = b_\ell c_0 + \sum_{i=0}^{\ell-1} b_i c_{\ell-i} \not\equiv p$, так как $b_\ell c_0 \not\equiv p$, а для всех $i \in \{0, \dots, \ell-1\}$ $b_i \equiv p$.

• Значит, $a_\ell \not\equiv p$. Но $\ell \leq m < n$, противоречие. □

Следствие 3

Пусть $f(x) = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{Z}[t]$ и $p \in \mathbb{P}$ таковы, что $a_0 \not\equiv p$, $a_1, \dots, a_n \equiv p$ и $a_n \not\equiv p^2$. Тогда f — неприводим в $\mathbb{Z}[t]$.

• Доказательство аналогично Теореме 5.

Значения в целых точках многочлена из $\mathbb{Z}[t]$

Лемма 10

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$, $x, y \in \mathbb{Z}$, $x \neq y$. Тогда $f(x) - f(y) \vdots x - y$.

Доказательство. • НУО $x - y > 0$. Так как $x \equiv_{x-y} y$, для всех $k \in \{0, \dots, n\}$ выполняется $x^k \equiv_{x-y} y^k$.

• Тогда $f(x) = \sum_{k=0}^n a_k x^k \equiv_{x-y} \sum_{k=0}^n a_k y^k = f(y)$. □

Рациональные корни многочлена из $\mathbb{Z}[t]$

Лемма 11

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$, $f(\frac{p}{q}) = 0$, где $p, q \in \mathbb{Z}$, $(p, q) = 1$. Тогда $a_n \dot{\vdots} q$ и $a_0 \dot{\vdots} p$.

Доказательство.

$$0 = q^n f\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n. \quad (1)$$

- Все слагаемые в правой части (1), кроме $a_n p^n$, делятся на q , значит, и $a_n p^n \dot{\vdots} q$. Так как $(p, q) = 1$, получаем $a_n \dot{\vdots} q$.
- Все слагаемые в правой части (1), кроме $a_0 q^n$, делятся на p , значит, и $a_0 q^n \dot{\vdots} p$. Так как $(p, q) = 1$, получаем $a_0 \dot{\vdots} p$. \square

Следствие 4

Пусть $f(t) = t^n + \dots + a_0 \in \mathbb{Z}[t]$, $\alpha \in \mathbb{Q}$, $f(\alpha) = 0$. Тогда $\alpha \in \mathbb{Z}$.

Доказательство. • Пусть $\alpha = \frac{p}{q}$, где $p, q \in \mathbb{Z}$, $(p, q) = 1$.

- По Лемме 11, $1 \dot{\vdots} q$, то есть $\alpha \in \mathbb{Z}$. \square

Лемма 12

Пусть $f(t) = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$, $f\left(\frac{p}{q}\right) = 0$, где $p, q \in \mathbb{Z}$, $(p, q) = 1$. Тогда $f(k) \vdots kq - p$ для любого $k \in \mathbb{Z}$.

Доказательство. •

$$q^n f(k) = q^n \left(f(k) - f\left(\frac{p}{q}\right) \right) =$$
$$\left(\sum_{i=0}^n q^n a_i k^i \right) - \left(\sum_{i=0}^n a_i p^i q^{n-i} \right) = \sum_{i=1}^n q^{n-i} a_i ((kq)^i - p^i) \vdots kq - p,$$

так для всех $i \in \{1, \dots, n\}$

$$(kq)^i - p^i \vdots kq - p \iff (kq)^i \equiv_{kq-p} p^i \iff kq \equiv_{kq-p} p.$$

• Так как $(q^n, kq - p) = (q, p) = 1$, из $q^n f(k) \vdots kq - p$ следует, что $f(k) \vdots kq - p$.



Разностный многочлен

Определение

Пусть $f \in K[x]$, где K — коммутативное кольцо с 1, причем $K \supset \mathbb{Z}$.

• **Разностный многочлен** задается формулой

$$\Delta f(x) := f(x+1) - f(x).$$

• Примеры подходящих колец K : $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Лемма 13

Пусть $f \in K[x]$, где K — коммутативное кольцо с 1, причем $K \supset \mathbb{Z}$. Тогда $\Delta f \in K[x]$, $\deg(\Delta f) = \deg(f) - 1$.

Доказательство. • Пусть $f(x) = a_n x^n + \dots + a_0$, где $n = \deg(f)$.

• По биному Ньютона, $a_k((x+1)^k - x^k) = \sum_{i=1}^k a_k C_k^i x^{k-i}$.

• Поэтому $\Delta f \in K[x]$.

• Одночлены с x^n в Δf сокращаются, а единственный одночлен с x^{n-1} — это $a_n C_n^1 x^{n-1}$ с коэффициентом $a_n C_n^1 \neq 0$.

Следовательно, $\deg(\Delta f) = n - 1$. □