

## О круговых многочленах

А. Я. Белов

Как известно, любой многочлен с целыми коэффициентами однозначно разлагается в произведение неприводимых множителей. Хорошо известна также следующая

**ТЕОРЕМА 1.** *Многочлен  $x^n - 1$  разлагается в произведение неприводимых над  $\mathbb{Q}$  многочленов  $\Phi_d$ :*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

*При этом корнями  $\Phi_d$  являются неприводимые корни  $d$ -й степени из единицы и  $\deg(\Phi_d) = \varphi(d)$ .*

Здесь  $\varphi(d)$  есть *функция Эйлера*, выражающая количество различных остатков от деления на  $d$ , взаимно простых с  $d$ . Корень  $d$ -й степени из единицы называется *неприводимым*, если он не является корнем из единицы, степени меньшей чем  $d$ .

Этой теоремой довольно часто пользуются (см., например решение задачи 2.7 из задачника «Математического просвещения», №6, с. 140–142). С ее доказательством можно ознакомиться по книгам [1, 2]. Мы приводим здесь другое доказательство, которое довольно красиво и содержательно. (Автор благодарит А. В. Шаповалова, рассказавшего ему это доказательство.)

Если число  $d$  — простое, то  $\Phi_d(x) = x^{d-1} + x^{d-2} + \dots + 1$  и доказательство неприводимости многочлена  $\Phi_d(x)$  получается путем применения критерия Эйзенштейна к многочлену  $\Phi_d(x+1)$  (неприводимость которого равносильна неприводимости  $\Phi_d(x)$ ). Напомним соответствующее утверждение:

**Предложение 1 (КРИТЕРИЙ ЭЙЗЕНШТЕЙНА).** *Пусть*

$$P(x) = x^n + a_1x^{n-1} + \dots + a_n,$$

*причем все коэффициенты  $a_1, \dots, a_n$  делятся на некоторое простое  $p$  и  $a_n$  не делится на  $p^2$ . Тогда многочлен  $P$  неприводим над множеством рациональных чисел.*

Доказательство этого критерия получается от противного сравнением коэффициентов  $P(x)$  и  $P_1(x)P_2(x)$  и применения леммы Гаусса, которая утверждает, что неприводимость над  $\mathbb{Z}$  влечет неприводимость над  $\mathbb{Q}$ . Мы предоставляем читателю провести доказательства самому, либо обратиться к любому ВУЗовскому учебнику по алгебре.

Бытует мнение (в том числе среди алгебраистов), что теорема 1 стандартным образом выводится из этого своего частного случая ( $d$  — простое) с помощью теории Галуа. Однако такое доказательство теоремы 1 нам неизвестно.

### НЕСКОЛЬКО ПОЛЕЗНЫХ ФАКТОВ

Прежде всего отметим, что

$$\Phi_d(x) = \frac{x^d - 1}{\prod_{s|d; s < d} \Phi_s(x)}. \quad (1)$$

Если частное двух многочленов с целыми коэффициентами и со старшим коэффициентом 1 является многочленом, то этот многочлен также имеет целые коэффициенты и старший коэффициент 1. Применяя это наблюдение к равенству (1), получаем по индукции, что все коэффициенты многочленов  $\Phi_d$  — целые.

**КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ.** Пусть  $z_1, \dots, z_k$  — конечный набор попарно взаимно простых целых чисел,  $a_1, \dots, a_k$  — произвольные целые числа. Тогда найдется такое число  $x$ , что  $x \equiv a_i \pmod{z_i}$ ,  $1 \leq i \leq k$ .

**ТЕОРЕМА ВЬЕТА.** Коэффициенты  $a_k$  многочлена  $x^n + a_1x^{n-1} + \dots + a_n$  выражаются через его корни  $x_i$  следующим образом:

$$a_k = (-1)^k \sum_{i_1 < \dots < i_k} x_{i_1} \cdot \dots \cdot x_{i_k}.$$

*Симметрический многочлен* — это многочлен, значение которого не зависит от перестановки переменных. *Элементарными симметрическими многочленами* называются многочлены

$$s_k = \sum_{i_1 < \dots < i_k} x_{i_1} \cdot \dots \cdot x_{i_k}.$$

**ОСНОВНАЯ ТЕОРЕМА О СИММЕТРИЧЕСКИХ МНОГОЧЛЕНАХ.** Любой симметрический многочлен от  $x_1, \dots, x_n$  с целыми коэффициентами можно представить в виде многочлена с целыми коэффициентами от элементарных симметрических многочленов  $s_k$ ,  $1 \leq k \leq n$ .

Следствием этих двух утверждений является

ЛЕММА 1. Пусть  $Q(x) = (x - x_1) \cdot \dots \cdot (x - x_n)$  — многочлен с целыми коэффициентами. Тогда при всех  $k \in \mathbb{N}$  коэффициенты многочлена  $\tilde{Q}_k(x) = (x - x_1^k) \cdot \dots \cdot (x - x_n^k)$  также целые.

Пусть  $\bar{Q}(x)$ ,  $\bar{\bar{Q}}$  — покоэффициентные редукции многочленов  $Q(x)$ ,  $\tilde{Q}_k(x)$  по модулю простого числа  $p$ ;  $\xi_1, \dots, \xi_n$  — корни  $\bar{Q}$  в подходящем алгебраическом расширении  $\mathbb{Z}_p$ . Тогда  $\xi_1^k, \dots, \xi_n^k$  — корни  $\bar{\bar{Q}}$ .

Следующая лемма является ослаблением теоремы Дирихле о простых числах в арифметической прогрессии, разность которой взаимно проста с начальным членом. Через  $\mathbb{Z}_q^*$  обозначается группа по умножению остатков от деления на  $q$  чисел, взаимно простых с  $q$ .

ЛЕММА 2. Пусть  $G \neq \mathbb{Z}_q^*$  — подгруппа группы  $\mathbb{Z}_q^*$ . Тогда множество простых чисел, остатки от деления которых на  $q$  не принадлежит группе  $G$ , бесконечно.

В частности, количество простых чисел, не представимых в виде  $qk + 1$ , (например  $6k - 1$  или  $4k - 1$ ) бесконечно.

ДОКАЗАТЕЛЬСТВО. Предположим противное. Пусть  $\mathcal{P}$  — множество всех  $p$ , остатки от которых по модулю  $q$  не лежат в  $G$ , а  $x \notin G$ . В силу китайской теоремы об остатках можно найти такое  $y$ , что  $y \equiv x \pmod{q}$ ,  $y \equiv 1 \pmod{p_i}$  для любого  $p_i \in \mathcal{P}$ .

Тогда произведение  $q \prod_{p_i \in \mathcal{P}} p_i + y$  содержит простой делитель, не сравнимый с элементами  $G$  по модулю  $q$ , и не принадлежащий  $\mathcal{P}$ . Противоречие.

И еще одно полезное наблюдение:

ЛЕММА 3. Пусть  $p$  — простое. В любом кольце имеют место следующие сравнения по модулю  $p$ : а)  $(a + b)^p \equiv a^p + b^p$ , б)  $(ab)^p = a^p b^p$ , в) для любого многочлена  $Q$  с целыми коэффициентами  $Q(\xi)^p \equiv Q(\xi^p)$ .

Пп. а) и б) проверяются непосредственно, в) из них следует.

#### ДОКАЗАТЕЛЬСТВО НЕПРИВОДИМОСТИ $\Phi_d(x)$

Предположим, что  $\Phi_d$  разлагается в произведение неприводимых многочленов  $Q_i$ , отличных от константы:  $\Phi_d(x) = \prod_{i=1}^s Q_i(x)$  и  $s > 1$ . Пусть  $m = \min \deg Q_i$ , без ограничения общности считаем, что  $\deg(Q_1) = m$ .

Пусть  $x_1, \dots, x_m$  — корни  $Q_1$ . Тогда для любого  $k$ , взаимно простого с  $d$ , числа  $x_i^k$  будут неприводимыми корнями  $d$ -й степени из единицы, а многочлен  $\tilde{Q}_k = \prod_i (x - x_i^k)$  по лемме 1 будет иметь целые коэффициенты. Поскольку НОД двух многочленов с целыми коэффициентами есть снова многочлен с целыми коэффициентами, а  $Q_i$  — неприводимый и

$\deg Q_i \geq \deg \tilde{Q}_k = m$ , то многочлены  $Q_i$  и  $\tilde{Q}_k$  либо не имеют общих делителей, либо совпадают.

Любой неприводимый корень  $d$ -й степени из единицы имеет вид  $x_1^r$ , где  $\text{НОД}(d, r) = 1$  и, следовательно, является корнем  $\tilde{Q}_r$ . Значит, любой многочлен разложения  $Q_i$  имеет нетривиальный общий делитель с некоторым  $\tilde{Q}_r$ . Поэтому, в силу вышесказанного,  $Q_i$  должен совпадать с каким-то  $\tilde{Q}_r$ . Итак, разложение  $\Phi_d$  на неприводимые компоненты должно иметь вид  $\Phi_d = \prod \tilde{Q}_k$ .

Заметим также, что поскольку все корни рассматриваемых многочленов суть корни  $d$ -й степени из единицы, многочлен  $\tilde{Q}_k$  зависит только от остатка  $k$  по модулю  $d$ . Если при этом  $\text{НОД}(k, d) = 1$ , то все корни многочлена  $\tilde{Q}_k$  суть *неприводимые корни  $d$ -й степени из единицы*.

Рассмотрим множество таких остатков  $k$  по модулю  $d$ , что  $\tilde{Q}_k = Q_1 = \tilde{Q}_1$ . Оно образует подгруппу  $G$  в группе  $\mathbb{Z}_d^*$ . В силу нашего предположения о приводимости  $\Phi_d$  группа  $G$  не совпадает со всей группой  $\mathbb{Z}_d^*$ .

При всех достаточно больших  $p$  редукции по модулю  $p$  для различных  $Q_i$  будут различны и, кроме того, редукция многочлена  $x^d - 1$  (а, значит, и  $\Phi_d$ ) не будет иметь кратных корней (ибо будет взаимно проста со своей производной  $dx^{d-1}$  если  $p > d$ ).

Из леммы 2 следует наличие такого  $k$ :  $\tilde{Q}_k \neq Q_1$ , что для бесконечного набора простых  $p$  выполняется сравнение  $p \equiv k \pmod{d}$ .

Но тогда, с одной стороны, в силу леммы 3 и равенства  $\forall i: x_i^d = 1$  все корни редукции по модулю  $p$  многочлена  $\tilde{Q}_k$  совпадут с корнями  $Q_1$  а коэффициенты редукции, в силу леммы 1 будут равны редукции по модулю  $p$  коэффициентов исходного  $\tilde{Q}_k$ .

С другой стороны,  $Q_1 \neq \tilde{Q}_k$  и, следовательно, при всех достаточно больших  $p$  сравнение  $Q_1 \equiv \tilde{Q}_k$  по модулю  $p$  место не имеет. Полученное противоречие доказывает теорему.

**УПРАЖНЕНИЕ.** а) Воспользовавшись теоремой Лагранжа, утверждающей, что порядок элемента делит порядок группы, докажите что любой простой делитель значения многочлена  $\Phi_d(n)$  при целом  $n$  имеет вид  $kd + 1$ .

б) По аналогии с доказательством леммы 2 докажите, что имеется бесконечно много простых делителей значений многочлена с целыми коэффициентами в целых точках, если этот многочлен отличен от константы. Выведите отсюда бесконечность множества простых чисел вида  $dk + 1$ .

#### СПИСОК ЛИТЕРАТУРЫ

- [1] Б. Л. ван дер Варден. *Алгебра*. М.: Наука, 1976. Гл. 8, §60.
- [2] В. Прасолов. *Многочлены*. М.: МЦНМО, 2000. П. 13.3.