Глава I

Простые числа

Натуральные числа — видимо, первый математический объект, который был принят человеком на самой заре нашей цивилизации, многие тысячи лет тому назад, с вполне понятной целью пересчёта предметов. Натуральные числа можно складывать, перемножать, и, казалось бы, нет ничего проще. Однако не будем торопиться с выводами. В математике часто бывает так, что объекты, которые появляются из вполне «приземлённых» соображений, таят в себе неожиданную глубину.

§ 1. Простые числа и неприводимые многочлены

Числа называют *составными*, если их можно разложить на два меньших сомножителя. Например, число $6 = 2 \cdot 3$ является составным. А вот число 7 нельзя разложить подобным образом. Поэтому число 7 называют *простым* числом. Итак, дадим определение.

Определение. *Составным числом* называется натуральное число, которое может быть разложено в произведение двух натуральных чисел, отличных от него самого.

Простым числом называется натуральное число, большее 1 и не являющееся составным.

Замечание. Часто в качестве определения простых чисел даётся следующее их свойство: у простого числа есть *ровно два* делителя — 1 и оно само. В дальнейшем (рассматривая, скажем, примеры Яглома и Гильберта) мы увидим, насколько важно давать верные определения.

Замечание. Как следует из определения, 1 не является ни простым, ни составным числом. Почему — мы подробно обсудим в § III.2.

Давайте выпишем все простые числа, меньшие 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,
47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Возникает естественный вопрос: как искать простые числа? Опишем старинный способ, придуманный ещё в III в. до н. э. Эратосфеном Киренским, хранителем Александрийской библиотеки.

Выпишем натуральные числа, начиная с 2. Двойку обведём, а остальные числа, которые делятся на 2, зачеркнём. Ближайшим незачёркнутым числом будет 3. Обведём и его, а все остальные числа, кратные 3, зачеркнём. Следующее наименьшее незачёркнутое число — это 5. Обводим пятёрку, а остальные числа, кратные 5, зачёркиваем. Повторяя эту процедуру снова и снова, мы в конце концов добьёмся того, что незачёркнутыми останутся лишь простые числа — они словно просеялись сквозь решето.

Замечание. Такой способ не позволяет достаточно быстро находить большие простые числа и тем более определять, является ли данное число простым или нет, поскольку нужно выписать все числа до него.

Казалось бы, какие сложности можем мы испытать при изучении простых чисел? Ещё какие! Чтобы продемонстрировать, о чём идёт речь, рассмотрим, например, среди простых чисел пары таких, разность между которыми минимальна. Как легко видеть, эта разность, кроме одного исключительного случая 2 и 3, равна 2:

2, **3**, **5**, **7**, **11**, **13**, **17**, **19**, 23, **29**, **31**, 37, **41**, **43**, 47, 53, **59**, **61**,
67, **71**, **73**, 79, 83, 89, 97, **101**, **103**, **107**, **109**, 113, 127, 131, ...

Такие пары простых чисел называются близнецами. Как устроено множество чисел-близнецов? Можно ли хотя бы утверждать, что это множество бесконечно? До сих пор ответы на эти вопросы неизвестны.

Прежде чем двигаться дальше, отметим одно ключевое соображение для всего нашего курса. В математике первостепенную роль играет *установление аналогий* между, казалось бы, совершенно различными структурами.

Рассмотрим, на первый взгляд, неожиданный в данном контексте пример: множество многочленов от одной переменной. Странно было бы ожидать, что множество многочленов имеет нечто общее с множеством натуральных чисел. Однако заметим, что многочлены можно складывать и перемножать и даже раскладывать на множители. Не правда ли, очень похоже на натуральные числа? Возникает естественный вопрос: *существуют ли в множестве многочленов аналоги простых чисел*? Да, существуют! Они называются *неприводимыми многочленами*.

Определение. *Приводимым многочленом* называется многочлен, который может быть разложен в произведение двух многочленов меньшей положительной степени.

Неприводимым многочленом называется многочлен положительной степени, не являющийся приводимым.

Замечание. Обратите внимание на то, что в этом определении существенную роль играет степень многочлена.

Замечание. Как следует из определения, многочлены нулевой степени (т. е. ненулевые числа) не является ни приводимыми, ни неприводимыми. Причины этому те же, по которым 1 не является ни простым, ни составным числом (вновь аналогия!).

Замечание. В большинстве школьных учебников и пособий многочленом называют «выражение вида…». Вообще говоря, эта фраза определением не является. Здесь просто одно слово — «многочлен», заменено другим — «выражение». А что такое выражение?.. В главе VII мы дадим строгое определение многочлена.

Рассмотрим несколько примеров. Начнём с приводимых многочленов. Таковыми являются, например, следующие:

$$
\begin{aligned}
&x^2 = x \cdot x,\\
&x^2 - 1 = (x-1)\cdot(x+1),\\
&x^2 - \frac{1}{4} = \Big(x - \frac{1}{2}\Big)\cdot\Big(x + \frac{1}{2}\Big),\\
&x^3 - x = x\cdot(x^2-1) = x\cdot(x-1)\cdot(x+1),\\
&x^3 + x = x\cdot(x^2+1).
\end{aligned}
$$

Приведём несколько примеров неприводимых многочленов.

$$x,\ x+c\ (c \text{ — произвольное число}),\ x^2+1,\ x^2+x+1.$$

Необходимо заметить, что вопрос о неприводимости того или иного многочлена зависит от множества, которому принадлежат его коэффициенты. Начнём с многочленов, коэффициенты которых являются произвольными действительными числами (это множество обозначается через $\mathbb{R}[x]$). Оказывается, существует критерий, который позволяет явно описать все неприводимые многочлены в $\mathbb{R}[x]$! Ими являются

1) все многочлены первой степени;
2) многочлены второй степени с отрицательным дискриминантом.

А именно, рассмотрим многочлен ax^2+bx+c. Используя процедуру выделения полного квадрата (смотрите, как эта процедура заработала!), получаем

$$ax^2+bx+c=a\Big(x^2+\frac{b}{a}x\Big)+c=a\Big(x^2+2\frac{b}{2a}x+\frac{b^2}{4a^2}-\frac{b^2}{4a^2}\Big)+c=$$
$$=a\Big(x^2+2\frac{b}{2a}x+\frac{b^2}{4a^2}\Big)-\frac{b^2}{4a}+\frac{ac}{a}=a\Big(x+\frac{b}{2a}\Big)^2-\frac{b^2-4ac}{4a}.$$

Выражение $D=b^2-4ac$ играет ключевую роль при рассмотрении многочленов второй степени и называется *дискриминантом* многочлена ax^2+bx+c. Рассмотрим три случая.

- $D<0$. В таком случае, как видно из полученного нами представления, многочлен не имеет корней и всегда принимает значения одного знака: положительные, если $a>0$, и отрицательные, если $a<0$. Именно в этом случае многочлен ax^2+bx+c является неприводимым. Приведём соответствующие примеры:

$$x^2+1>0,\quad x^2+x+1=\Big(x+\frac{1}{2}\Big)^2+\frac{3}{4}>0,$$
$$-x^2-1<0,\quad -2x^2+3x-2=-2\Big(x-\frac{3}{4}\Big)^2-\frac{7}{8}<0.$$

- $D=0$. В таком случае

$$ax^2+bx+c=a\Big(x+\frac{b}{2a}\Big)^2,$$

откуда очевидно следует приводимость исходного многочлена.

- $D>0$. В этом случае оказывается, что у исходного многочлена обязательно будут корни x_1, x_2 и разложение будет иметь вид

$$ax^2+bx+c=a\Big(x+\frac{b}{2a}\Big)^2-\frac{b^2-4ac}{4a}=a(x-x_1)\cdot(x-x_2).$$

Например,

$$x^2-1=(x-1)\cdot(x+1),$$
$$x^2-x-2=(x-2)\cdot(x+1),$$
$$3x^2-5x-2=(3x+1)\cdot(x-2)=3\Big(x+\frac{1}{3}\Big)\cdot(x-2),$$
$$-2x^2+7x-3=-(2x-1)\cdot(x-3)=-2\Big(x-\frac{1}{2}\Big)\cdot(x-3),$$
$$x^2-2=(x-\sqrt{2})(x+\sqrt{2}).$$

В множестве $\mathbb{R}[x]$ все многочлены третьей степени и выше приводимы, т. е. их можно разложить на множители! Например,

$$x^4+4=(x^2-2x+2)\cdot(x^2+2x+2).$$

Замечание. Множество $\mathbb{R}[x]$ *похоже* на множество $\mathbb{N}$. Но, как мы ранее сказали, не существует эффективного алгоритма, который позволяет определить, является ли данное натуральное число простым. Даже с использованием самых современных компьютеров это потребует значительного времени. Однако в случае многочленов с действительными коэффициентами вопрос решается много проще.

Если рассматривать многочлены, коэффициенты которых являются произвольными рациональными числами (это множество обозначается через $\mathbb{Q}[x]$), то ситуация становится намного сложнее. Не существует явного описания неприводимых многочленов в $\mathbb{Q}[x]$. Приведём несколько примеров многочленов, которые приводимы как элементы множества $\mathbb{R}[x]$, но неприводимы как элементы множества $\mathbb{Q}[x]$:

$$x^2-2, \quad x^4+1, \quad x^4+x^3+x^2+x+1,$$
$$x^5-3, \quad x^6+x^5+x^4+x^3+x^2+x+1.$$

Замечание. В множестве $\mathbb{Q}[x]$ существуют неприводимые многочлены любой степени. Например, x^n-p, где p — простое число.

При повседневном знакомстве с теми или иными объектами, например с натуральными числами, вы вырабатываете соответствующую интуицию, приобретаете знание поведения этих объектов. Устанавливаемые аналогии наподобие той, что мы отметили между числами и многочленами, позволяют *перебрасывать интуицию* на новые структуры.

Вернёмся к рассмотрению простых чисел и докажем следующее утверждение, которое понадобится нам в дальнейшем.

Лемма (о простом делителе). *У любого натурального числа, большего* 1, *существует простой делитель.*

Доказательство. Пусть n — произвольное натуральное число, большее 1. Рассмотрим *наименьший* натуральный делитель p числа n, больший 1.

Почему такой делитель p существует?

Действительно, предположим, что наименьшего делителя не существует. В таком случае для любого делителя q найдётся такой делитель q', что $q > q'$. Если наименьшего делителя нет, то эту цепочку можно продолжать: $q > q' > q'' > \ldots$ Но она обязательно оборвётся, поскольку рано или поздно мы получим 1.

Докажем, что число p простое. Предположим противное: пусть число p составное. Тогда по определение составного числа найдутся два натуральных числа a и b, отличные от p и такие, что $p = ab$. Но тогда $a < p$ и n делится на a. В самом деле, если $n = p \cdot n_1$, то, подставляя в это равенство $p = ab$, получаем $n = a \cdot (bn_1)$. Значит, n делится на a и p — не наименьший делитель числа n. Противоречие. □

Замечание. Обратите внимание на то, что утверждения о простых числах отнюдь не просты, если доказывать их в общем виде. Например, утверждение о возможности разложения натурального числа на простые множители единственным образом является на самом деле теоремой! Теоремой, требующей доказательства (совсем не простого), которое мы дадим в главе IX.

Замечание. После того как мы установили аналогию между числами и многочленами, имеет смысл спросить, а существует ли для многочленов аналог утверждения, которое мы только что доказали для чисел. Как правило, такой аналог существует. В качестве примера приведём следующее утверждение.

Лемма (о неприводимом делителе). *У любого многочлена положительной степени существует неприводимый делитель.*

Введём для удобства общепринятое обозначение для степени многочлена: deg.

Доказательство. Пусть f — произвольный многочлен, $\deg f > 0$. Рассмотрим многочлен p *наименьшей* положительной степени, который делит f.

Почему такой многочлен p существует?

Действительно, предположим, что такого многочлена не существует. В таком случае для любого делителя q найдётся такой делитель q', что $\deg q > \deg q'$. Если нет делителя наименьшей степени, то эту цепочку можно продолжать: $\deg q > \deg q' > \deg q'' > \ldots$ Но она обязательно оборвётся, поскольку рано или поздно мы получим 1.

Докажем, что многочлен p неприводим. Предположим противное: пусть p — приводимый многочлен. Тогда по определение приводимого многочлена найдутся такие многочлены g и h положительной степени, что $p = gh$. Но тогда $\deg g < \deg p$ и f делится на g. В самом деле, если $f = p \cdot f_1$, то, подставляя в это равенство $p = gh$, получаем $f = g \cdot (hf_1)$. Значит, f делится на g и p — делитель многочлена f не наименьшей степени — противоречие. □