Основная теорема арифметики

Возможность разложения натурального числа на простые множители единственным образом является ключевым фактом в теории чисел. Фактом, который вам прекрасно знаком и которым вы (явно или неявно) почти всегда пользуетесь при работе с натуральными числами. Более того, этот факт кажется совершенно очевидным и воспринимается так же естественно, как восход солнца утром. Тем не менее, это не просто само собой разумеющийся факт, а следующая теорема.

Теорема (основная теорема арифметики). *Каждое натуральное число n, большее 1, может быть разложено в произведение простых чисел: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, где $\alpha_1, \ldots, \alpha_k \geqslant 1$. Это разложение единственно с точностью до порядка простых сомножителей.*

Замечание. Если бы 1 считалась простым числом, то нельзя было бы утверждать, что разложение на простые единственно. Действительно, $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3 = \ldots$

Замечание. Основная теорема арифметики отсутствует в «Началах» Евклида. Впервые её точная формулировка и доказательство появились в книге «Арифметические исследования» (1801 г.) Гаусса, имя которого мы уже упоминали.

Причина, по которой строгое доказательство этой теоремы появилось только у Гаусса, по всей видимости, заключалась в том, что он был первым, кто систематически исследовал множества, похожие на целые числа, но не всегда обладающие всеми свойствами целых чисел. Например, мы познакомимся и с такими множествами, для которых не справедлива основная теорема арифметики!

§ 1. Примеры Яглома и Гильберта

Сама по себе основная теорема арифметики не кажется чем-то удивительным. Ведь совершенно очевидно, что любое число расклады-

вается в произведение простых, разложение это единственно (например, $36 = 2^2 \cdot 3^2$), и что вообще можно извлечь интересного из такого тривиального факта?

Оказывается, всё далеко не так просто. Основная теорема арифметики отражает одно из важнейших свойств натуральных чисел. Это свойство называется *факториальностью*.

Рассмотрим несколько примеров, показывающих, как возникают сложности в таких вопросах.

Пример Яглома

Этот пример был предложен советским математиком Исааком Ягломом.

Давайте рассмотрим множество чётных чисел: $2, 4, 6, 8, 10, \ldots$ Выясним, как будут выглядеть, так сказать, простые и составные числа в этом множестве.

По нашему определению *составным* называется число, которое может быть разложено в произведение двух чисел, отличных от него самого, а все остальные числа (кроме 1, которой у нас и так нет) называются *простыми*.

Число 2, очевидно, является простым. Число $4 = 2 \cdot 2$ представимо в виде произведения двух двоек и потому является составным.

Каким будет число 6 — простым или составным? Казалось бы, $6 = 2 \cdot 3$. Но ведь числа 3 нет в нашем множестве! Значит, число 6 *не может быть разложено в произведение двух чисел из нашего множества* и потому *является простым*!

Предложение. *Все чётные числа, кратные* 4, *являются составными, а все не кратные* 4 — *простыми.*

Доказательство. Рассмотрим чётное натуральное число n.

Если n делится на 4, то $n = 4k$ и $n = 2 \cdot (2k)$. Таким образом, число n разложено в произведение двух чётных отличных от него чисел, а значит, n — *составное* число по определению.

Если n не делится на 4, оно не может быть разложено в произведение двух чётных чисел, а значит, является *простым* числом по определению. □

Теперь давайте проверим, работает ли основная теорема арифметики в таком множестве чисел. Рассмотрим число 36. Имеем

$$36 = 2 \cdot 18 = 6 \cdot 6.$$

Но и 2, и 6, и 18 являются простыми числами! Значит, число 36 можно разложить на простые множители *двумя различными способами*!

Пример Гильберта

В примере Яглома мы рассмотрели множество чётных чисел и выяснили, что основная теорема арифметики для него неверна. Можно ли подобный пример построить для нечётных чисел? Оказывается, можно. Следующий пример был предложен Давидом Гильбертом.

Рассмотрим следующее множество чисел вида $4k+1$:

$$1,\ 5,\ 9,\ 13,\ 17,\ 21,\ \ldots$$

Опять попробуем найти простые и составные числа в этом множестве.

Легко видеть, что числа 5, 9, 13, 17, 21 в начале ряда являются простыми. Приведём несколько примеров составных чисел в этом множестве (напомним, что число 1 не является ни простым, ни составным):

$$45 = 5 \cdot 9, \quad 65 = 5 \cdot 13, \quad 117 = 9 \cdot 13.$$

Попробуем построить контрпример к основной теореме арифметики. Для этого заметим, что произведение двух чисел вида $4k+3$ является числом вида $4k+1$. Например, $3 \cdot 7 = 21$. Хотя числа 3 и 7 не принадлежат рассматриваемому нами множеству, ему принадлежит 21 (именно поэтому в примере Гильберта число 21 является простым). Поскольку мы ищем число, имеющее два разложения на простые, попробуем сконструировать его с использованием чисел 3 и 7. Рассмотрим число $441 = 3^2 \cdot 7^2$. Имеем

$$441 = 21 \cdot 21 = 9 \cdot 49.$$

И 9, и 21, и 49 являются простыми числами.

Попробуйте самостоятельно отыскать число, имеющее три различных разложения на простые множители в примерах Яглома и Гильберта.

§ 2. $\mathbb{Z}[\sqrt{-k}]$ и Великая теорема Ферма

Обратимся теперь к более содержательным и сложным примерам. Что такое $\mathbb{Z}[\sqrt{-k}]$, наверняка спрашиваете вы. Рассмотрим «числа» вида $a + b\sqrt{-k}$, где k — фиксированное *натуральное* число, а a и b — произвольные *целые* числа. Во-первых, отметим, что обычные целые числа содержатся среди рассматриваемых (достаточно положить $b = 0$).

Таким образом, только что определённое нами множество «чисел» представляет собой лишь расширение множества $\mathbb{Z}$ целых чисел. Во-вторых, разберёмся с тем, как понимать, что такое $\sqrt{-k}$? Очень просто: $\sqrt{-k}$ — это «число», квадрат которого равен $-k$:

$$(\sqrt{-k})^2 = \sqrt{-k}\cdot\sqrt{-k} = -k.$$

Замечание. Пока $\sqrt{-k}$ — это не более чем символ. О строгом определении $\mathbb{Z}[\sqrt{-k}]$ мы будем говорить в § X.6.

Оперировать с новыми числами так же легко, как и с обычными целыми числами. Сложение определяется очевидным образом:

$$(a+b\sqrt{-k})+(c+d\sqrt{-k}) = (a+c)+(b+d)\sqrt{-k}.$$

Чтобы определить умножение, используем правила обычной арифметики и не забудем про равенство $(\sqrt{-k})^2 = \sqrt{-k}\cdot\sqrt{-k} = -k$:

$$\begin{aligned}(a+b\sqrt{-k})\cdot(c+d\sqrt{-k}) &= \\ &= (a+b\sqrt{-k})\cdot c + (a+b\sqrt{-k})\cdot d\sqrt{-k} = \\ &= ac + bc\sqrt{-k} + ad\sqrt{-k} + bd\sqrt{-k}\cdot\sqrt{-k} = \\ &= (ac-bdk) + (bc+ad)\cdot\sqrt{-k}\end{aligned}$$

Таким образом, множество чисел вида $a+b\sqrt{-k}$ выдерживает сложение и умножение (что делает его похожим на множество $\mathbb{Z}$ целых чисел). Это множество и обозначается через $\mathbb{Z}[\sqrt{-k}]$. Обратимся теперь к конкретным примерам.

Как ошибся Эйлер

Рассмотрим множество $\mathbb{Z}[\sqrt{-3}]$ чисел вида

$$a+b\sqrt{-3}, \quad \text{где} \quad a,b\in\mathbb{Z}.$$

Попробуем отыскать несколько простых и составных чисел в этом множестве. Начнём с целых чисел (которые являются элементами множества $\mathbb{Z}[\sqrt{-3}]$). Составные целые числа являются, очевидно, и составными числами в $\mathbb{Z}[\sqrt{-3}]$. А что можно сказать про простые целые числа? Будут ли они обязательно простыми в $\mathbb{Z}[\sqrt{-3}]$? Следующий пример показывает, что нет:

$$7 = (2+\sqrt{-3})\cdot(2-\sqrt{-3}).$$

Вообще говоря, совершенно непонятно, как выяснить, является ли данное число $a+b\sqrt{-3}$ простым. Чтобы ответить на этот вопрос, введём вспомогательное понятие.

Определение. *Нормой* числа $a+b\sqrt{-k}$ называется число

$$N(a+b\sqrt{-k}) = (a+b\sqrt{-k})\cdot(a-b\sqrt{-k}) = \\ = a^2 - b^2\cdot\sqrt{-k}\cdot\sqrt{-k} = a^2+kb^2.$$

Замечание. Число $a-b\sqrt{-k}$ называется *сопряжённым* с числом $a+b\sqrt{-k}$.

Предложение. *Пусть $z, w \in \mathbb{Z}[\sqrt{-k}]$. Тогда*

$$N(z\cdot w) = N(z)\cdot N(w).$$

Доказательство. Пусть $z = a+b\sqrt{-k}$, $w = c+d\sqrt{-k}$. Тогда

$$N\big((a+b\sqrt{-k})\cdot(c+d\sqrt{-k})\big) = \\ = N\big((ac-kbd)+(bc+ad)\cdot\sqrt{-k}\big) = \\ = (ac-kbd)^2 + k(bc+ad)^2 = (a^2+kb^2)\cdot(c^2+kd^2) = \\ = N(a+b\sqrt{-k})\cdot N(c+d\sqrt{-k}).$$

□

Замечание. Тождество Эйлера

$$(ac-kbd)^2 + k(bc+ad)^2 = (a^2+kb^2)\cdot(c^2+kd^2)$$

означает, что норма N обладает свойством мультипликативности:

$$N(z\cdot w) = N(z)\cdot N(w).$$

Иными словами, произведение чисел вида a^2+kb^2 является числом такого вида. Если $k=1$, то мы приходим к рассмотрению чисел, представимых в виде суммы двух квадратов. Подробнее о них мы будем говорить в § VIII.1.

Замечание. Норма числа $a+b\sqrt{-k}$ — целое *неотрицательное* число. С каждым целым числом можно также связать величину, называемую нормой. В таком случае она будет просто модулем целого числа. Понятие нормы можно ввести и для многочленов: нормой многочлена будет его степень.

Оказывается, существование нормы позволяет провести более глубокое исследование вышеперечисленных (и не только) множеств. Об этом мы будем говорить в § IX.3.

Докажем теперь, что, скажем, число 2 является простым в $\mathbb{Z}[\sqrt{-3}]$. Действительно, предположим, что

$$2 = (a+b\sqrt{-3})\cdot(c+d\sqrt{-3}).$$

Используя утверждение о норме произведения, получаем

$$N(2) = N\big((a + b\sqrt{-3}) \cdot (c + d\sqrt{-3})\big) = N(a + b\sqrt{-3}) \cdot N(c + d\sqrt{-3}),$$

что равносильно равенству

$$4 = (a^2 + 3b^2) \cdot (c^2 + 3d^2).$$

В нём каждый из сомножителей является натуральным числом, поэтому либо оба сомножителя в правой части равны 2, либо один из них равен 1, а другой 4. Первое невозможно, поскольку уравнение $a^2 + 3b^2 = 2$, очевидно, не имеет решений в целых числах. Во втором случае получаем уравнения

$$a^2 + 3b^2 = 1 \quad \text{и} \quad c^2 + 3d^2 = 4,$$

первое из которых имеет следующее решение: $a = \pm 1$, $b = 0$. Тогда в исходном разложении числа 2 на множители один из них равен 1 (или -1), т. е. разложение тривиально и имеет вид $2 = 1 \cdot 2$ (или $2 = (-1) \cdot (-2)$). Значит, число 2 действительно простое.

Разберём, на первый взгляд, более замысловатый пример и докажем простоту числа $1 + \sqrt{-3}$. Предположим обратное: пусть

$$1 + \sqrt{-3} = (a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}).$$

Используя утверждение о норме произведения, получаем

$$N(1 + \sqrt{-3}) = N((a + b\sqrt{-3}) \cdot (c + d\sqrt{-3})) = N(a + b\sqrt{-3}) \cdot N(c + d\sqrt{-3}),$$

что, как несложно видеть, равносильно равенству

$$4 = (a^2 + 3b^2) \cdot (c^2 + 3d^2),$$

которое мы только что рассмотрели, доказывая простоту числа 2. Таким образом, число $1 + \sqrt{-3}$ также является простым.

Замечание. Совершенно ясно, что абсолютно так же доказывается простота числа $1 - \sqrt{-3}$. Более того, если число $a + b\sqrt{-3}$ оказывается простым, то таковым будет и сопряжённое ему число $a - b\sqrt{-3}$.

Замечание. Из доказанного утверждения следует, что если норма $N(z)$ — простое натуральное число, то и число z будет простым в $\mathbb{Z}[\sqrt{-k}]$. Возникает естественный вопрос: верно ли обратное? Обязательно ли у простого в $\mathbb{Z}[\sqrt{-k}]$ числа норма будет простым натуральным числом? Попробуйте найти ответ на этот вопрос.

Вернёмся к вопросу, которому посвящена данная глава. Выполнена ли основная теорема арифметики для $\mathbb{Z}[\sqrt{-3}]$? Оказывается, нет! Например,

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}).$$

Но постойте! Всё не так просто… Где гарантия, что перед нами два различных разложения на простые множители? В примерах Яглома и Гильберта ответ на этот вопрос был очевиден. Теперь это не так. Поясним, что имеется в виду, на примере целых чисел. Имеем

$$4 = 2 \cdot 2 = (-2) \cdot (-2).$$

Мы, конечно, понимаем, что эти разложения не следует отличать, потому что

$$(-2) \cdot (-2) = (-1) \cdot (-1) \cdot 2 \cdot 2.$$

Иными словами, с точки зрения разложения целых чисел на множители (-1) аналогична 1. Что понимать под аналогом 1? Когда у нас появилось понятие простого числа, мы отмечали, что 1 не является ни простым, ни составным. Ведь если считать 1 простым, то в таком случае нельзя утверждать, что существует единственное разложение на простые множители. В случае натуральных чисел это замечание не кажется содержательным, однако рассматриваемые нами сейчас примеры показывают, что не всё так просто.

Определение. Элемент q данного множества называется *обратимым* (или *делителем единицы*), если существует такой элемент s, принадлежащий данному множеству, что $q \cdot s = 1$.

Элемент s принято обозначать через q^{-1}.

Если вернуться к целым числам, то, как легко видеть, $1^{-1} = 1$ и $(-1)^{-1} = -1$. Других делителей единицы в $\mathbb{Z}$ нет. Покажем теперь, как наличие именно делителей единицы может «испортить» теорему о разложении на простые множители. Пусть q — делитель единицы и имеется разложение элемента n на простые множители:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k.$$

Тогда имеет также место такое разложение:

$$n = q \cdot q^{-1} \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k.$$

Например, как отмечено выше,

$$(-2) \cdot (-2) = (-1) \cdot (-1) \cdot 2 \cdot 2 = (-1) \cdot (-1)^{-1} \cdot 2 \cdot 2.$$

Продемонстрируем это явление также на примере многочленов:

$$x^2-1=(x-1)\cdot(x+1)=2(x-1)\cdot\frac{1}{2}(x+1)=3(x-1)\cdot\frac{1}{3}(x+1)=\ldots$$

Замечание. В множестве многочленов от одной переменной $\mathbb{R}[x]$ обратимыми элементами будут в точности многочлены нулевой степени (числа).

Имея это в виду, несколько подкорректируем определение простого и составного элементов.

Определение. *Составным* называется *необратимый* элемент, который может быть разложен в произведение двух *необратимых* элементов.

Простым называется *необратимый* элемент, не являющийся составным.

Делители единицы (обратимые элементы) не являются ни простыми, ни составными.

Разложение на простые множители следует понимать с точностью до умножения на делители единицы (обратимые элементы). Точно так же, как мы не различаем разложения натурального числа 36:

$$36=2\cdot2\cdot3\cdot3=1\cdot2\cdot2\cdot3\cdot3=1\cdot1\cdot2\cdot2\cdot3\cdot3=\ldots,$$

не отличают разложения

$$x^2-1=(x-1)\cdot(x+1)=2(x-1)\cdot\frac{1}{2}(x+1)=3(x-1)\cdot\frac{1}{3}(x+1)=\ldots,$$

или, более общим образом,

$$n=p_1\cdot\ldots\cdot p_k=q_1\cdot q_1^{-1}\cdot p_1\cdot\ldots\cdot p_k=q_1\cdot q_1^{-1}\cdot q_2\cdot q_2^{-1}\cdot p_1\cdot\ldots\cdot p_k=\ldots,$$

где $q_1, q_2, \ldots$ — делители единицы.

Замечание. Данное определение является универсальным. В частности, оно охватывает и случай натуральных чисел, и случай многочленов.

Найдём все делители единицы в множествах $\mathbb{Z}[\sqrt{-k}]$. В этом нам поможет уже известное понятие нормы.

Теорема. *В $\mathbb{Z}[\sqrt{-k}]$ при $k>1$ делителями единицы являются в точности* $1, -1$.

В $\mathbb{Z}[\sqrt{-1}]$ делителями единицы являются в точности следующие числа: $1, -1, \sqrt{-1}, -\sqrt{-1}$.

Доказательство. Пусть $q = a + b\sqrt{-k}$ — делитель единицы. Тогда существует $q^{-1} = c + d\sqrt{-k} \in \mathbb{Z}[\sqrt{-k}]$. Имеем

$$\begin{aligned} q \cdot q^{-1} = 1 \;\Rightarrow\; & N(q) \cdot N(q^{-1}) = N(q \cdot q^{-1}) = 1 \;\Leftrightarrow \\ \Leftrightarrow\; & N(a + b\sqrt{-k}) \cdot N(c + d\sqrt{-k}) = 1 \;\Leftrightarrow \\ \Leftrightarrow\; & (a^2 + kb^2) \cdot (c^2 + kd^2) = 1 \;\Leftrightarrow \\ \Leftrightarrow\; & a^2 + kb^2 = 1, \quad c^2 + kd^2 = 1. \end{aligned}$$

Поскольку $k > 1$, получаем, что $b = 0$, $d = 0$.

Представленная цепочка равенств имеет место для любого натурального k. В случае $k > 1$ получаем, что делители единицы содержатся среди чисел ± 1. Очевидно, что 1 и -1 будут обратимыми.

В случае $k = 1$ из цепочки равенств следует, что делители единицы содержатся среди чисел ± 1, $\pm\sqrt{-1}$. Простая проверка показывает, что все эти числа являются обратимыми. Действительно,

$$\begin{aligned} 1 \cdot 1 = 1, \quad &\text{т. е.} \quad 1^{-1} = 1, \\ (-1) \cdot (-1) = 1, \quad &\text{т. е.} \quad (-1)^{-1} = -1, \\ \sqrt{-1} \cdot (-\sqrt{-1}) = 1, \quad &\text{т. е.} \quad (\sqrt{-1})^{-1} = -\sqrt{-1}, \\ (-\sqrt{-1}) \cdot \sqrt{-1} = 1, \quad &\text{т. е.} \quad (-\sqrt{-1})^{-1} = \sqrt{-1}. \end{aligned}$$

□

Из данной теоремы следует, что разложение

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}).$$

действительно является разложением числа 4 на простые множители двумя различными способами!

Теперь давайте разберёмся, при чём здесь Эйлер и какую же ошибку он допустил. С этим связана крайне интересная история, которая берёт своё начало в III веке до н. э. в исследованиях древнегреческого математика Диофанта. Его имя нам известно благодаря его многотомной «Арифметике» из 13 книг. Основная тема «Арифметики» — решение уравнений в целых числах. К этой теме мы вернёмся в дальнейшем, а сейчас нас будет интересовать одна из задач, упомянутых Диофантом, которая связана с описанием так называемых пифагоровых троек, т. е. целочисленных решений уравнения

$$x^2 + y^2 = z^2.$$

В главе V мы подробно поговорим об этой задаче.

Замечание. Вы наверняка не в первый раз сталкиваетесь с уравнением $x^2 + y^2 = z^2$. Впервые оно появилось несколько тысяч лет назад,

когда люди открыли теорему Пифагора (а произошло это задолго до Пифагора). Удивительно, какую заметную роль это уравнение сыграло в истории науки, а значит, и всей нашей цивилизации. Оно связано не только с геометрией, но привело также и к открытию иррациональных чисел (об этом подробнее в главе X), и к знаменитой проблеме Ферма, о которой пойдёт речь ниже.

Сочинения Диофанта долгое время оставались неизвестны европейским математикам. Только в XVI веке одна из его рукописей была случайно обнаружена в библиотеке Ватикана. Первый перевод «Арифметики» на латинский язык был издан в 1621 году, и владельцем одного из экземпляров стал французский математик Пьер Ферма. Значительная часть его наследия в области теории чисел — мысли, идеи, формулировки теорем, гипотезы — дошла до нас в форме записей и замечаний на полях этого экземпляра «Арифметики». Напротив восьмой задачи второй книги Диофанта «разбить квадратное число на два других квадратных числа» (это и есть упомянутая выше задача) Ферма сделал самую знаменитую свою запись: «Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duas eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet», в которой утверждалось, что при $n > 2$ *не существует отличных от нуля целых чисел, являющихся решением уравнения*

$$x^n + y^n = z^n.$$

Так формулируется Великая теорема Ферма.

В математике бывает так, что задача, имеющая простую формулировку, требует крайне нетривиального решения. Великая теорема Ферма, пожалуй, самый знаменитый тому пример. На протяжении более чем трёх сотен лет предпринимались попытки найти её доказательство. Наконец оно было получено в 1995 году английским математиком Эндрю Уайлсом после 8 лет работы. Его более чем 100-страничное доказательство отнюдь не элементарно [1]. Единственный случай, для которого известно элементарное доказательство, — это случай $n = 4$. Указанное доказательство дано самим Ферма и опирается на упомянутые формулы для пифагоровых троек.

[1] Это доказательство выходит далеко за рамки теории чисел и использует методы алгебраической геометрии — науки, объединяющей алгебру и геометрию и исследующей множества решений систем алгебраических уравнений.

Следующий после Ферма шаг делает Эйлер (век спустя) — он доказывает теорему для случая $n = 3$, т. е. показывает, что уравнение $x^3 + y^3 = z^3$ не имеет нетривиальных решений в целых числах. Совершенно поразительным и принципиально новым в доказательстве Эйлера было привлечение чисел вида $a + b\sqrt{-3}$!

Замечание. С Великой теоремой Ферма связана одна важная нить исторического развития алгебры. Хотя в формулировке теоремы участвуют только целые числа, в ходе её доказательства потребовалось обратиться к числам более общего вида (например, $\mathbb{Z}[\sqrt{-k}]$). Глубокое проникновение в арифметику этих чисел потребовало введения новых понятий и придало импульс развитию всей алгебры, теории чисел и других математических наук.

В своём доказательстве Эйлер использует следующее рассуждение: он рассматривает равенство

$$a^2 + 3b^2 = (a + b\sqrt{-3}) \cdot (a - b\sqrt{-3})$$

и утверждает, что, *поскольку левая его часть является кубом, то же справедливо и для обоих сомножителей правой части*. В частности,

$$a + b\sqrt{-3} = (s + t\sqrt{-3})^3.$$

По всей видимости, Эйлер полагал очевидным, что из взаимной простоты чисел a и b следует взаимная простота чисел $(a + b\sqrt{-3})$ и $(a - b\sqrt{-3})$ и тем самым утверждение о том, что множители в правой части также являются кубами. Вообще говоря, это нуждается в доказательстве. Более того, учитывая, что для $\mathbb{Z}[\sqrt{-3}]$ не выполнена основная теорема арифметики, нельзя быть уверенным, что это вообще так[1]! Действительно, обратимся к примеру Яглома. Имеем $216 = 12 \cdot 18$. Числа 12 и 18 не имеют общих делителей (число 18 вообще простое!) и не являются кубами.

§ 3. Гауссовы числа

Множество $\mathbb{Z}[\sqrt{-1}]$ чисел вида $a + b\sqrt{-1}$, $a, b \in \mathbb{Z}$, впервые появилось в работах Гаусса в 1832 году. Именно Гауссом было открыто, что арифметические понятия и теоремы, которые всегда связывались

[1] В данном случае это утверждение действительно верно, хотя для его доказательства необходимо привлечь дополнительные соображения. Доподлинно неизвестно, владел ли ими Эйлер.

с натуральными и целыми числами, можно переносить на другие объекты [1]. Мы уже отмечали это на примере множества многочленов от одной переменной. Гаусс в своих исследованиях пришёл к необходимости перенести известные теоремы на множество $\mathbb{Z}[\sqrt{-1}]$.

Выше мы описали делители единицы в $\mathbb{Z}[\sqrt{-1}]$. Теперь найдём несколько простых и составных чисел в $\mathbb{Z}[\sqrt{-1}]$. Число 2 является простым в целых числах и простым в $\mathbb{Z}[\sqrt{-3}]$. Однако в $\mathbb{Z}[\sqrt{-1}]$ имеем

$$2 = (1+\sqrt{-1})\cdot(1-\sqrt{-1}),$$

а значит, число 2 составное в $\mathbb{Z}[\sqrt{-1}]$! А что можно сказать о числах $(1\pm\sqrt{-1})$? Являются ли они простыми? Докажем, что они действительно простые. Предположим, что

$$1+\sqrt{-1} = (a+b\sqrt{-1})\cdot(c+d\sqrt{-1}).$$

Тогда получаем

$$N(1+\sqrt{-1}) = N\big((a+b\sqrt{-1})\cdot(c+d\sqrt{-1})\big) = N(a+b\sqrt{-1})\cdot N(c+d\sqrt{-1}),$$

что равносильно равенству $2=(a^2+b^2)\cdot(c^2+d^2)$. Из него вытекает, что либо $a^2+b^2=1$, либо $c^2+d^2=1$. В обоих случаях один из сомножителей в разложении

$$1+\sqrt{-1} = (a+b\sqrt{-1})\cdot(c+d\sqrt{-1})$$

является делителем единицы. Итак, число $1+\sqrt{-1}$ (и $1-\sqrt{-1}$) действительно простое.

Разумеется, возникает вопрос: верна ли основная теорема арифметики для гауссовых чисел? Рассмотрим следующий пример:

$$5 = (1+2\sqrt{-1})\cdot(1-2\sqrt{-1}) = (2+\sqrt{-1})\cdot(2-\sqrt{-1}).$$

Легко убедиться, что числа, участвующие в данных разложениях, простые. Кажется, мы нашли пример, который показывает, что основная теорема арифметики не выполнена. Однако не будем торопиться, ведь мы уже отмечали, что разложение на простые множители следует понимать с точностью до умножения на делители единицы. Если в случае натуральных чисел или многочленов сразу видно, какие разложения следует считать одинаковыми, то в случае гауссовых чисел

[1] Не просто переносить, но и строго доказывать! Такие аналогии были замечены ещё Эйлером, но строгие доказательства появились, по всей видимости, именно в работах Гаусса.

это не столь очевидно. Обратимся к разложению числа 5:

$$\begin{aligned} 5 &= (1+2\sqrt{-1})\cdot(1-2\sqrt{-1}) = \\ &= \sqrt{-1}\cdot(2-\sqrt{-1})\cdot(-\sqrt{-1})\cdot(2+\sqrt{-1}) = \\ &= \sqrt{-1}\cdot(-\sqrt{-1})\cdot(2-\sqrt{-1})\cdot(2+\sqrt{-1}) = \\ &= \sqrt{-1}\cdot(\sqrt{-1})^{-1}\cdot(2-\sqrt{-1})\cdot(2+\sqrt{-1}). \end{aligned}$$

Так что полученные нами разложения на самом деле суть одно! Всё равно что $2\cdot 3$ и $1\cdot 1\cdot 2\cdot 3$.

Совершенно удивительно, но основная теорема арифметики выполнена для множества гауссовых чисел! Правда, если для доказательства того, что теорема *не выполнена*, достаточно было всего лишь привести пример, то совершенно непонятно, как доказать, что теорема верна. Мы знакомы с несколькими примерами множеств, для которых имеет место основная теорема арифметики. Среди них множество $\mathbb{N}$ натуральных чисел, множество $\mathbb{Z}$ целых чисел, множества $\mathbb{R}[x]$ и $\mathbb{Q}[x]$ многочленов, теперь появился пример множества $\mathbb{Z}[\sqrt{-1}]$ гауссовых чисел. Позже мы дадим доказательство, которое будет универсальным и будет включать в себя все вышеперечисленные случаи.

§ 4. Десять следствий

Примеры, разобранные нами в предыдущих параграфах, показывают, что основная теорема арифметики — не очевидный факт, а глубокое свойство, которым обладают не только множества натуральных и целых чисел, но и множества многочленов и гауссовых чисел, как будет доказано в главе IX.

Естественно ожидать, что из этой теоремы следует много важных фактов. Для нас будут существенны следующие десять утверждений — следствий из основной теоремы арифметики.

Замечание. Эти следствия будут иметь место всегда, когда выполнена основная теорема.

Следствие 1. *Пусть*

$$a = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_n^{k_n},\quad b = p_1^{l_1}\cdot p_2^{l_2}\cdot\ldots\cdot p_n^{l_n}$$

— разложения чисел a и b на простые сомножители, причём $k_i \geqslant 0$, $l_i \geqslant 0$, но $k_i + l_i > 0$. Тогда

$$\text{НОД}(a,b) = p_1^{\min(k_1,l_1)}\cdot p_2^{\min(k_2,l_2)}\cdot\ldots\cdot p_n^{\min(k_n,l_n)}.$$

Следствие 2. *В обозначениях предыдущего следствия*

$$\text{НОК}(a,b) = p_1^{\max(k_1,l_1)} \cdot p_2^{\max(k_2,l_2)} \cdot \ldots \cdot p_n^{\max(k_n,l_n)}.$$

Следствие 3. *Имеет место формула*

$$\text{НОД}(a,b) \cdot \text{НОК}(a,b) = ab.$$

Замечание. Именно это следствие применяется для вычисления наименьшего общего кратного.

Следствие 4. *Если* $(ab) \vdots c$ *и* $\text{НОД}(a,c) = 1$, *то* $b \vdots c$.

Следствие 5 (лемма Евклида о простом делителе)**.** *Если* p *— простое число и* $(ab) \vdots p$, *то либо* $a \vdots p$, *либо* $b \vdots p$.

Следствие 6. *Если* $\text{НОД}(b,c) = 1$ *и* $a \vdots b$, $a \vdots c$, *то* $a \vdots (bc)$.

Следствие 7. *Если* c *— общее кратное чисел* a *и* b, *то* $c \vdots \text{НОК}(a,b)$.

Следствие 8. *Если* d *— общий делитель чисел* a *и* b, *то* $\text{НОД}(a,b) \vdots d$.

Следствие 9. *Имеют место следующие формулы*:

$$\text{НОД}(ma,mb) = m \cdot \text{НОД}(a,b), \quad \text{НОД}\Big(\frac{a}{m},\frac{b}{m}\Big) = \frac{\text{НОД}(a,b)}{m},$$

$$\text{НОК}(ma,mb) = m \cdot \text{НОК}(a,b), \quad \text{НОК}\Big(\frac{a}{m},\frac{b}{m}\Big) = \frac{\text{НОК}(a,b)}{m}.$$

Следствие 10. *Если* $\text{НОД}(a,b) = 1$ *и* $c^n = ab$, *то* $a = a_1^n$, $b = b_1^n$.

Замечание. Именно это следствие использовал Эйлер, ошибочно полагая, что основная теорема арифметики выполнена для чисел $\mathbb{Z}[\sqrt{-3}]$.

Доказательства всех следствий напрямую следуют из основной теоремы арифметики.