Рождественская теорема Ферма

Определение 1. *Гауссовы целые числа* $\mathbb{Z}[i]$ — это комплексные числа с целыми действительной и мнимой частями.

Пример 1. Числа $5+3i, 0, 7$ — гауссовы.

Определение 2. Гауссово число называется *простым*, если оно не может быть представлено в виде произведения двух необратимых в этом кольце элементов.

Задача 1. Какие элементы обратимы в кольце $\mathbb{Z}[i]$?

Обратимые элементы в $\mathbb{Z}[i]$ играют ту же роль, что ± 1 в целых числах.

Пример 2. Число 2 не является простым в гауссовых числах, поскольку $2 = (1+i)(1-i)$, а числа $1+i$ и $1-i$ уже являются простыми, поскольку они и только они имеют наименьшую норму, равную 2. Заметим также, что числа $1+i$ и $1-i$ отличаются друг от друга умножением на i — один из обратимых элементов кольца $\mathbb{Z}[i]$, в такой ситуации говорят, что числа $1+i$ и $1-i$ *ассоциированны*, т. е. отличаются умножением на обратимый элемент.

Чтобы делить с остатком в гауссовых числах, необходимо ввести некоторую числовую характеристику каждого числа — норму — иначе мы не сможем понять, когда деление с остатком закончено. Например, у целых чисел ей служил модуль, а у многочленов — степень. Введём норму гауссова числа $a+bi$:

$$N(a+bi) = a^2 + b^2.$$

Задача 2. Докажите, что для любых гауссовых чисел a и b

$$N(ab) = N(a)N(b).$$

Задача 3. Какие из данных гауссовых чисел простые: $1+i, 3, 5, 3+i$?

Задача 4. Докажите, что $N(ab) \geqslant N(a)$, и равенство выполняется только в случае, если b обратим.

Задача 5. Докажите возможность деления с остатком в $\mathbb{Z}[i]$, т. е. что для любых $a, b \in \mathbb{Z}[i]$, где $b \neq 0$, существуют такие q и r из $\mathbb{Z}[i]$, что $a = qb + r$, и либо $r = 0$, либо $N(r) < N(b)$. *Указание.* Привлеките геометрическую интуицию.

Определение 3. И вообще, абстрактное кольцо R без делителей нуля, не являющееся полем, называется *евклидовым*, если существует функциия $N : R\backslash\{0\} \to \mathbb{Z}_+$ — норма, удовлетворяющая условиям:

1) $N(ab) \geqslant N(a)$, причём равенство имеет место только тогда, когда элемент b обратим;

2) для любых $a,\ b \in R$, где $b \neq 0$, существуют такие q и r из R, что $a = bq + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Т. е. евклидовы кольца — это кольца, в которых можно делить с остатком.

Пример 3. Целые числа $\mathbb{Z}$ — евклидово кольцо.

Пример 4. Евклидовыми кольцами являются кольца многочленов над любым полем (например, $\mathbb{R}[x]$).

Пример 5. Из задач **4** и **5** следует, что $\mathbb{Z}[i]$ — евклидово кольцо.

Теорема 1. *В евклидовом кольце для любых двух элементов a и b существует наибольший общий делитель d, и он может быть представлен в виде $d = au + bv$ для некоторых u, v из кольца.*

Задача 6. Докажите теорему.

Определение 4. Необратимый элемент кольца без делителей нуля называется *простым*, если он не может быть представлен в виде произведения двух необратимых в этом кольце элементов.

Пример 6. В кольце $\mathbb{Z}$ простыми элементами служат простые числа с точностью до знака.

Пример 7. В кольце многочленов $\mathbb{R}[x]$ простыми элементами служат неприводимые многочлены.

Теорема 2. *В евклидовом целостном кольце всякий необратимый ненулевой элемент может быть разложен на простые множители, причём это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы.*

Определение 5. Кольца, в которых любой необратимый элемент единственным способом (с точностью до порядка сомножителей и домножения на обратимые элементы) представляется в виде произведения необратимых, называются *факториальными*.

Следствие 3. *Кольца $\mathbb{Z}$, $\mathbb{R}[x]$, $\mathbb{Z}[i]$ — факториальные.*

Задача 7. Осознайте следствие.

Но есть кольца, в которых это не так:

Задача 8. Докажите, что евклидово кольцо $\mathbb{Z}[\sqrt{-5}]$ с нормой $N(a + b\sqrt{-5}) = a^2 + 5b^2$ не факториально.
Указание. Рассмотрите число 6.

Задача 9. При каких простых p уравнение $x^2 + 1 = 0$ имеет решение в поле $\mathbb{Z}_p$?
Указание. Загуглите символ Лежандра.

Задача 10. Найдите все простые в $\mathbb{Z}$ числа p, которые просты также в $\mathbb{Z}[i]$.
Указание. $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[x]/(x^2+1)$ и примените результат ваших размышлений над последней задачей прошлого листка.

Задача 11. Докажите, что простые элементы $\mathbb{Z}[i]$ суть (с точностью до ассоциированности) простые натуральные числа вида $4k+3$; числа вида $a+bi$, где a^2+b^2 — простое (в $\mathbb{Z}$) и число $1+i$.
Указание. Во втором случае срабатывает простое рассуждение с нормами.

Задача 12 (Собственно, рождественская теорема Ферма)**.** Докажите, что простое натуральное число p представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда $p = 4k + 1$.

Задача 13 (Обобщение)**.** Докажите, что натуральное число n представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда в его разложение на простые множители в $\mathbb{Z}$ все множители вида $4k+3$ входят в чётной степени.

Задача 14. В зависимости от простых чисел $p_i,\ i = 1, ..., s$ найдите количество представлений числа $p_1 ... p_s$ в виде суммы двух квадратов.