

Гауссовы целые числа

Задача 3.1. Что из перечисленного является кольцом (со стандартными операциями)?

Какие из этих колец целостные? Какие из них являются полями? Перечислите все обратимые элементы в этих кольцах.

- а) $\mathbb{N}$; б) $\mathbb{Z}$; в) $\mathbb{Z}/m\mathbb{Z}$; г) $\mathbb{Z}[\sqrt{2}]$; д) $\mathbb{Z}[\sqrt[3]{2}]$; е) гауссовы целые $\mathbb{Z}[i]$;
ж) многочлены $\mathbb{R}[x]$;
з) $A[x]$, где A — произвольное кольцо;
и) формальные степенные ряды $\mathbb{R}[[x]]$;
к) гладкие функции на прямой $C^\infty(\mathbb{R})$.

▷ Напомним, что *нормой* гауссова целого числа $z = a + bi$ называется число $n(z) = a^2 + b^2$.

Задача 3.2. а) Докажите, что $n(zw) = n(z)n(w)$.

б) Опишите алгоритм деления с остатком в $\mathbb{Z}[i]$ и докажите, что это кольцо евклидово.

Задача 3.3. Поделите с остатком в $\mathbb{Z}[i]$:

- а) $14 + 8i$ на 3 ; б) 9 на $2 + i$; в) $15 - 7i$ на $3i - 2$.

Задача 3.4. Разложите $2, 3, 5$ на простые множители в $\mathbb{Z}[i]$.

Задача 3.5. а) Докажите, что никакое простое число $p \in \mathbb{Z}$ не представимо в виде произведения более двух необратимых сомножителей в $\mathbb{Z}[i]$.

б) Докажите, что целое простое число p либо остаётся простым в $\mathbb{Z}[i]$, либо представляется в виде произведения двух сопряженных простых: $p = (a + bi)(a - bi)$.

в) Докажите, что целое простое число p остаётся простым в $\mathbb{Z}[i]$, если $p = 4k + 3$.

Задача 3.6. Докажите, что никакое простое число нельзя представить в виде суммы двух квадратов двумя различными способами.

Задача 3.7. Покажите, что число 65 представимо в виде суммы двух квадратов двумя способами. Как это согласуется с основной теоремой арифметики в $\mathbb{Z}[i]$?

Задача 3.8. а) Докажите, что для простого числа p вида $4k + 1$ найдутся такие x и y , не делящиеся на p , для которых $x^2 + y^2$ делится на p . Более того, можно взять $y = 1$.

УКАЗАНИЕ. Можно воспользоваться теоремой Вильсона.

б*) Докажите, что $p \in \mathbb{Z}$ представляется в виде произведения двух сопряженных простых в $\mathbb{Z}[i]$, если $p = 4k + 1$.

УКАЗАНИЕ. Возьмите такое r , что $r^2 + 1$ делится на p . Для всех пар $0 \leq a, b \leq [\sqrt{p}]$ рассмотрите числа вида $a + br$; докажите, что некоторая разность чисел такого вида делится на p . Выведите отсюда существование ненулевого числа вида $A + Br$, где $|A| < \sqrt{p}$ и $|B| < \sqrt{p}$, делящегося на p .

Задача 3.9 (теорема Ферма–Эйлера). Докажите, что целое положительное число представимо в виде суммы двух квадратов тогда и только тогда, когда каждый входящий в него простой сомножитель вида $4k + 3$ входит в его разложение на простые в четной степени.