Определение 1. Пусть i — формальный символ, для которого выполняется условие $i^2 = -1$ (*мнимая единица).* Множество $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ с естественными операциями сложения и умножения называется *кольцом гауссовых чисел.*

Определение 2. Пусть $z = a + bi \in \mathbb{Z}[i]$. Число $\overline{z} = a - bi \in \mathbb{Z}[i]$ называется *сопряжённым* к числу z. Числа $\mathrm{Re}(z) = a \in \mathbb{Z}$, $\mathrm{Im}(z) = b \in \mathbb{Z}$ и $N(z) = a^2 + b^2 \in \mathbb{N} \cup \{0\}$ называются *действительной* частью, *мнимой* частью и *нормой* числа z соответственно.

Определение 3. Пусть $z, w \in \mathbb{Z}[i]$, причём $w \neq 0$. Говорят, что z *делится на* w, если существует такое $u \in \mathbb{Z}[i]$, что $z = wu$. В этом случае также говорят, что число z *кратно* числу w; число w называется *делителем* числа z, а число u называется *частным* от деления z на w.

Задача 1. Пусть $z, w \in \mathbb{Z}[i]$. Докажите, что:
а) $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$; **б)** если $z \vdots w$, то $\overline{z} \vdots \overline{w}$; **в)** $N(z) = z \cdot \overline{z}$; **г)** $N(zw) = N(z)N(w)$.

Определение 4. Число $z \in \mathbb{Z}[i]$ называется *обратимым* (или *гауссовой единицей),* если существует такое $w \in \mathbb{Z}[i]$, что $zw = 1$. В этом случае w называется *обратным* к числу z и обозначается z^{-1}.

Задача 2. **а)** Перечислите все обратимые гауссовы числа.
б) Найдите все делители гауссова числа 6.

Задача 3. Будем изображать гауссовы числа на координатной плоскости таким образом, чтобы числу $a + bi \in \mathbb{Z}[i]$ соответствует точка плоскости с координатами (a, b).
а) Каким преобразованиям плоскости соответствуют отображения $z \mapsto -z$, $z \mapsto \overline{z}$ и $z \mapsto i \cdot z$?
б) Нарисуйте на плоскости все числа, кратные гауссовому числу $z = 1 + 2i$.
в) Как изменится картинка, если в пункте **б** заменить $(1 + 2i)$ на произвольное гауссово число?

Задача 4. (*Деление с остатком*) Пусть $z, w \in \mathbb{Z}[i]$, причём $w \neq 0$.
а) Докажите, что существуют $q, r \in \mathbb{Z}[i]$ такие, что $z = w \cdot q + r$ и $N(r) < N(w)$.
б) Сколькими способами можно выбрать такую пару гауссовых чисел?

Задача 5. **а)** Дайте определение для наибольшего общего делителя (НОД) двух ненулевых гауссовых чисел. Докажите, что он определён однозначно с точностью до умножения на гауссовы единицы.
б) Докажите, что алгоритм Евклида работает для гауссовых чисел, приводя к НОД.
в) Найдите НОД$(7 + 9i, 10 + 2i)$.
г) Найдите НОД$(z, \overline{z})$ для произвольного $z \in \mathbb{Z}[i]$.

Определение 5. Необратимое гауссово число $z \neq 0$ называется *неприводимым*, если его нельзя представить в виде произведения двух необратимых гауссовых чисел.

Задача 6. **а)** Являются ли неприводимыми гауссовы числа $(7 + i)$, $-i$, $(2 + 3i)$, 5, $7i$?
б) Докажите, что если $N(z)$ — простое целое число, то z — неприводимое гауссово число.

Задача 7. Докажите, что если z и w — произвольные гауссовы числа, а u — такое неприводимое гауссово число, что zw делится на u, то либо z делится на u, либо w делится на u.

Задача 8. (*Основная теорема арифметики для гауссовых чисел.*) Докажите, что каждое ненулевое необратимое гауссово число раскладывается в произведение неприводимых гауссовых чисел, причём такое разложение единственно с точностью до порядка сомножителей и умножения их на обратимые числа.
Указание. Вспомните, как доказывалась основная теорема арифметики для целых чисел и многочленов.

Задача 9. **а)** Пусть $m, n \in \mathbb{Z}$, $z \in \mathbb{Z}[i]$, причём z неприводимо. Докажите, что если $m \vdots z^n$, то $m \vdots \overline{z}^n$.
б) Пусть $m \in \mathbb{Z}$. Докажите, что можно выбрать такое разложение числа m на неприводимые гауссовы числа, что каждое нецелое неприводимое число будет входить в это разложение вместе со своим сопряжённым, причём в той же степени.

1 а	1 б	1 в	1 г	2 а	2 б	3 а	3 б	3 в	4 а	4 б	5 а	5 б	5 в	5 г	6 а	6 б	7	8	9 а	9 б

Задача 10. (*Описание неприводимых гауссовых чисел*)
Пусть $z \in \mathbb{Z}[i]$, q — простое целое число. Докажите следующие утверждения.

а) Если z не является неприводимым и $\operatorname{Im} z = 0$, то либо число $\operatorname{Re} z$ составное, либо найдётся такое $w \in \mathbb{Z}[i]$, что $z = w\overline{w}$.

б) Если z неприводимо, то $\overline{z}$ тоже неприводимо.

в) Если z неприводимо, то существует ровно одно простое целое число p, делящееся на z.

г) Если z неприводимо, то существует простое целое число p такое, что $N(z) = p$ или $N(z) = p^2$.

д) Если $q = (4k + 3)$ при некотором $k \in \mathbb{N}$, то q является неприводимым гауссовым числом.

е) (*Лемма Вильсона*) Число $((q-1)! + 1)$ делится на q.

ж) Если $q = (4k + 1)$ при некотором $k \in \mathbb{N}$, то число $((2k)!^2 + 1)$ делится на q.

з) Если $q = (4k + 1)$ при некотором $k \in \mathbb{N}$, то q не является неприводимым гауссовым числом.

и) Если $q = 2$ или $q = (4k + 1)$ при некотором $k \in \mathbb{N}$, то найдётся единственное с точностью до сопряжения и умножения на гауссовы единицы неприводимое число $w \in \mathbb{Z}[i]$ такое, что $p = w\overline{w}$.

к) Любое неприводимое гауссово число получается из одного из упомянутых в пунктах **д** и **и** неприводимых гауссовых чисел умножением на некоторую гауссову единицу.

Задача 11. (*Представление числа в виде суммы двух квадратов*) Рассмотрим диофантово уравнение $n = x^2 + y^2 = (x + yi)\overline{(x + yi)}$. Обозначим число его целочисленных решений через $T(n)$.

а) Найдите все решения и нарисуйте их на плоскости для $n = 2$, 13, 25, 43 65.

б) Докажите, что при $n \equiv 3 \pmod 4$ решений нет.

в) Пусть $p \equiv 1 \pmod 4$ — простое целое число. Чему равно $T(p)$?

г) Пусть p — простое целое число. Найдите $T(p^k)$.

д) Пусть $m, n \in \mathbb{Z}$, причём $(n, m) = 1$. Докажите, что $T(nm) = 4T(n)T(m)$.

е) Пусть $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ — каноническое разложение целого числа n на простые множители. Выразите $T(n)$ через $p_1, \ldots, p_k$ и $\alpha_1, \ldots, \alpha_k$.

ж) Докажите, что $T(n)$ есть учетверённая разность между количеством натуральных делителей числа n, имеющих вид $(4k+1)$, и количеством натуральных делителей числа n, имеющих вид $(4k+3)$.

з)* Найдите натуральное число, которое представимо в виде суммы двух квадратов натуральных чисел ровно 57-ю способами.

и)* Найдите наименьшее число, удовлетворяющее условию пункта **з.**

Задача 12. Упорядоченная по возрастанию тройка натуральных чисел (a, b, c) называется *пифагоровой,* если она удовлетворяет равенству $c^2 = a^2 + b^2 = (a + bi)(a - bi)$. Применив основную теорему арифметики к этому равенству, получите явное описание всех пифагоровых троек.

Задача 13. Решите в целых числах уравнение $y^3 = x^2 + 1$.

Задача 14. (*Диофант*) Докажите, что число 15 не представимо в виде суммы квадратов двух рациональных чисел.

10 а	10 б	10 в	10 г	10 д	10 е	10 ж	10 з	10 и	10 к	11 а	11 б	11 в	11 г	11 д	11 е	11 ж	11 з	11 и	12	13	14

Примечание. Упоминания о задаче представления целого числа в виде суммы квадратов двух целых чисел встречаются с древнейших времен. В частности, уже две с лишним тысячи лет назад было известно, что если два числа представимы в виде суммы двух квадратов, то представимо и их произведение — это следует из тождеств Брахмагу́пты (598-670 гг.), известных еще Диофа́нту Александри́йскому (III век до н.э.): $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2$. Общий ответ на вопрос, какие числа представимы в виде суммы двух квадратов (теорема Ферма-Эйлера) без доказательства упоминается в 1632 году в сочинениях Альбе́ра Жира́ра (1595-1632 гг.). Пьер Ферма́ (1601-1665 гг.) утверждал, что метод решения ему известен, однако документальных свидетельств этому не осталось. Первое известное нам доказательство дал в 1749 году Леона́рд Э́йлер (1707-1783 гг.) — оно использует метод спуска и тождества Брахмагупты. Два доказательства через гауссовы числа предложил в 1877 году Ри́хард Дедеки́нд (1831-1916 гг.). Одно из них описано выше в задаче 11. Что же касается самих гауссовых чисел, то их впервые ввёл Карл Фри́дрих Га́усс (1777-1855 гг.) в 1832 году для исследования уравнения $x^4 \equiv a \pmod p$.