Определение 1. Множество R называется *кольцом,* если на нём заданы операции *сложения* и *умножения* (отображения $+\colon R \times R \to R$ и $\cdot\colon R \times R \to R$ соответственно), удовлетворяющие следующим условиям (*аксиомам кольца):*

(A1) $\forall\, a, b \in R:\quad a + b = b + a$ (*коммутативность сложения*).

(A2) $\forall\, a, b, c \in R:\quad (a + b) + c = a + (b + c)$ (*ассоциативность сложения*).

(A3) В R существует такой элемент 0, что $\forall\, a \in R:\quad a + 0 = a$ (*существование нуля*).

(A4) $\forall\, a \in R\ \exists\, b \in R:\quad a + b = 0$ (*существование противоположного элемента*).
Элемент b называется *противоположным* к a и обозначается $-a$.

(M1) $\forall\, a, b, c \in C:\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*ассоциативность умножения*).

(AM) $\forall\, a, b, c \in R:\quad a \cdot (b + c) = a \cdot b + a \cdot c$
(*дистрибутивность умножения относительно сложения*).

Кольцо R называется *коммутативным,* если дополнительно выполнена аксиома

(M2) $\forall\, a, b \in R:\quad a \cdot b = b \cdot a$ (*коммутативность умножения*).

Кольцо R называется *кольцом с единицей,* если дополнительно выполнена аксиома

(M3) В $R \setminus \{0\}$ существует такой элемент 1, что $\forall\, a \in R:\quad a \cdot 1 = 1 \cdot a = a$ (*существование единицы*).

Всюду в дальнейшем под словом «кольцо» будет подразумеваться коммутативное кольцо с единицей.

Задача 1. Какие из следующих множеств (с естественными операциями сложения и умножения) являются кольцами?
а) $\mathbb{N}$; **б)** $\mathbb{Z}$; **в)** $\mathbb{Q}$; **г)** $\mathbb{R}$; **д)** $\mathbb{Q}[x]$.

Задача 2. Приведите пример кольца, состоящего в точности из $n \in \mathbb{N}$ элементов.

Определение 2. Кольцо R называется *евклидовым,* если на нём определена *евклидова норма — функция* $N\colon R \to \mathbb{N} \cup \{0\}$ такая, что $N(a) = 0$ тогда и только тогда, когда $a = 0$, и возможно деление с остатком, то есть для любых $a, b \in R$, $b \neq 0$ существуют $q, r \in R$ такие, что $a = bq + r$ и $N(r) < N(b)$.

Замечание 1. Мы ещё будем дополнительно требовать, чтобы функция N была *мультипликативной,* то есть $N(a \cdot b) = N(a) \cdot N(b)$ для любых $a, b \in R$.

Задача 3. Какие из колец задачи 1 можно сделать евклидовыми, введя подходящую норму?

Задача 4. Существует ли евклидово кольцо из конечного числа элементов?

Определение 3. Множество $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, где i — мнимая единица, с естественными операциями сложения и умножения называется *кольцом гауссовых чисел.*

Задача 5. Пусть $z \in \mathbb{Z}[i]$. Нарисуйте на комплексной плоскости все гауссовы числа, кратные z.

Задача 6. Пусть $N(a + bi) = a^2 + b^2$.
а) Проверьте, что N удовлетворяет всем свойствам евклидовой нормы.
б) Докажите, что $\mathbb{Z}[i]$ — евклидово кольцо.

Задача 7. По аналогии с $\mathbb{Z}[i]$ рассмотрим кольцо $\mathbb{Z}[i\sqrt{n}]$ и определим $N(a + bi\sqrt{n}) = a^2 + nb^2$. Будет ли это кольцо евклидовым, если **а)** $n = 2$; **б)** $n = 3$; **в)** $n = 5$?

Определение 4. Элемент $a \in R$ называется *обратимым,* если существует элемент $b \in R$, такой что $ab = ba = 1$. В этом случае b называется *обратным* к a и обозначается a^{-1}.

Задача 8. Перечислите все обратимые элементы в $\mathbb{Z}[i]$ и $\mathbb{Z}[i\sqrt{2}]$.

Определение 5. Необратимый элемент $a \in R \setminus \{0\}$ называется *неприводимым,* если его нельзя представить в виде произведения двух необратимых элементов из $\mathbb{R}$.

Задача 9. Верно ли, что неприводимые элементы в $\mathbb{Z}$ — это в точности простые числа?

Определение 6. Пусть R — евклидово кольцо и $a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$ — два разложения некоторого его элемента a в произведение неприводимых множителей. Эти разложения *эквивалентны,* если

- $m = n$,
- Существует перестановка $\sigma \in S_n$ и набор обратимых элементов $o_1, o_2, \dots, o_n \in R$ такие, что $\forall i = 1, 2, \dots, n: \quad p_i = o_i q_{\sigma(i)}$.

Пример: $6 = 2 \cdot 3 = (-3) \cdot (-2)$ — два эквивалентных разложения целого числа 6 на неприводимые множители.

Определение 7. Пусть R — кольцо, такое что для любого необратимого элемента $a \in \mathbb{R} \setminus \{0\}$ существует разложение на неприводимые множители, причём оно единственно с точностью до эквивалентности. Тогда кольцо R называется *факториальным.*

Задача 10. Какие из колец задачи 1 факториальны?

Задача 11. Приведите пример нефакториального кольца.

Задача 12. (*Основная теорема арифметики для евклидовых колец*) Докажите, что любое евклидово кольцо является факториальным.

Указание. Вспомните, как доказывалась основная теорема арифметики для целых чисел.

Задача 13. Рассмотрим равенство $c^2 = a^2 + b^2 = (a + bi)(a - bi)$. Примените к нему основную теорему арифметики и получите явное описание всех Пифагоровых троек.

Задача 14. (*Описание неприводимых гауссовых чисел*)

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

б) Докажите, что если $z \in \mathbb{Z}[i]$ неприводимо, то $\overline{z}$ тоже неприводимо.

в) Докажите, что если $z \in \mathbb{Z}[i]$ неприводимо, то существует ровно одно простое число p, делящееся на z.

г) Докажите, что если $z \in \mathbb{Z}[i]$ неприводимо, то $N(z) = p$ или $N(z) = p^2$, где p — простое число.

д) Докажите, что простое число вида $p = 4k + 3$ является неприводимым гауссовым числом.

е) (*Лемма Вильсона*) Пусть p — простое. Докажите, что $((p-1)! + 1) \vdots p$.

ж) Пусть $p = 4k + 1$ — простое. Докажите, что найдётся $a \in \mathbb{Z}$, такое что $(a^2 + 1) \vdots p$.

з) Докажите, что простое число вида $p = 4k + 1$ является приводимым гауссовым числом.

и) Пусть $p = 2$ или $p = 4k + 1$ — простое. Докажите, что найдётся неприводимое число $z \in \mathbb{Z}[i]$, такое что $p = z\overline{z}$, причём такое z единственно с точностью до сопряжения и умножения на обратимые элементы.

к) Докажите, что никаких других (с точностью до умножения на обратимые элементы) неприводимых гауссовых чисел кроме упомянутых в пунктах **д** и **и** нет.

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

Задача 16. Сформулируйте и докажите теорему о том, как по разложению натурального числа на простые множители понять, представимо ли это число в виде суммы двух квадратов целых чисел.

Задача 17. **а)** Найдите натуральное число, которое представимо ровно 57-ю способами в виде суммы квадратов двух натуральных чисел. **б)*** Найдите наименьшее такое число.

1 а	1 б	1 в	1 г	1 д	2	3	4	5	6 а	6 б	7 а	7 б	7 в	8	9	10	11	12	13	14 а	14 б	14 в	14 г	14 д	14 е	14 ж	14 з	14 и	14 к	15	16	17 а	17 б