Для зачета по каждому листку достаточно сдать все задачи со звездочками, либо все задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

АЛГЕБРА 2: делимость в кольцах и алгоритм Евклида

Наибольший общий делитель

Пусть R — кольцо.

Определение 2.1. Делители нуля в кольце R это такие ненулевые элементы x, y, что $xy = 0$. R называется **областью целостности**, если в R нет делителей нуля.

На протяжении этого листка, все кольца предполагаются областями целостности.

Определение 2.2. Обратимый элемент в R называется **единицей** кольца R.

Задача 2.1. Целые гауссовы числа – это комплексные числа вида $x + y\sqrt{-1}$, где x, y целые. Докажите, что они образуют кольцо. Оно обозначается $\mathbb{Z}[\sqrt{-1}\,]$.

Задача 2.2. Опишите все единицы в кольце целых гауссовых чисел.

Указание. Если комплексное число z обратимо в $\mathbb{Z}[\sqrt{-1}\,]$, то $z\overline{z}$ тоже обратимо в $\mathbb{Z}[\sqrt{-1}\,]$.

Задача 2.3. Зафиксируем целое положительное число n. Рассмотрим множество всех комплексных чисел вида $x + y\sqrt{-n}$, где x, y целые. Докажите, что это кольцо.

Задача 2.4 (*). Зафиксируем целое положительное нечетное число n. Рассмотрим множество всех комплексных чисел вида $\frac{x+y\sqrt{-3}}{2}$, где x, y одновременно четные либо одновременно нечетные. Докажите, что это кольцо, и опишите все единицы. Мы обозначим это кольцо $\widetilde{\mathbb{Z}[\sqrt{-3}]}$.

Определение 2.3. Пусть R кольцо, $x, y \in R$ элементы R. Если $x = yz$ в R, то говорят, что x **делится** на y в R, а y **делит** x. Отношение делимости обозначается $x \vdots y$.

Определение 2.4. Пусть R — кольцо, $x, y \in R$ элементы R. **Наибольший общий делитель** (НОД) x, y — это такой элемент $z \in R$, что z делит x и y, и для всякого z', делящего x, z' делит z. x и y называются **взаимно простыми**, если 1 – наибольший общий делитель x, y.

Вообще говоря, в произвольном кольце для произвольных элементов НОД может и не существовать.

Задача 2.5. Докажите, что если НОД существует, то он единственный с точностью до единицы: если z и z' – наибольшие общие делители x и y в кольце R, то $z = ez'$, где e – единица кольца R.

Задача 2.6. Пусть $\mathbb{Q}(2)$ - множество всех рациональных чисел, представленных дробями вида $\frac{p}{q}$ с нечетным знаменателем q. Докажите, что это множество замкнуто относительно умножения и сложения и образует подкольцо в кольце рациональных чисел.

Задача 2.7. Приведите пример необратимого элемента в $\mathbb{Q}(2)$.

Задача 2.8. Опишите единицы кольца $\mathbb{Q}(2)$.

Задача 2.9 (!). Докажите, что в $\mathbb{Q}(2)$ существует наибольший общий делитель любых двух элементов.

Указание. Докажите, что любой элемент $\mathbb{Q}(2)$ представим в виде $e2^n$, где e — единица.

Определение 2.5. Пусть p – элемент кольца R. Он называется **простым**, если для любых q, r с $p = qr$ либо q, либо r – единица кольца R.

Задача 2.10. Опишите все простые элементы в $\mathbb{Q}(2)$.

Делимость в кольце целых чисел

Задача 2.11. Пусть x, y – целые положительные числа, а $z = (x - ky)$ — остаток от деления x на y. Докажите, что если НОД(y, z) существует, то НОД(x, y) также существует, и равен НОД(y, z).

Определение 2.6. Алгоритм Евклида берет два целых положительных числа x, y, $x > y$, и выдает целое положительное число z.

а. Если x делится на y, алгоритм заканчивает свою работу и выдает в качестве результата y.

б. Если x не делится на y, алгоритм повторяет свою работу, примененный к числам $x_1 = y$, $y_1 = x - ky$, где $x - ky$ остаток от деления x на y.

Задача 2.12. Докажите, что алгоритм Евклида заканчивает свою работу после конечного числа итераций

Задача 2.13. Докажите, что результат применения алгоритма Евклида к целым числам x, y является НОД(y, z)

Задача 2.14. Решите задачу 1.26 из листка 1 (если вы ее еще не решили).

Задача 2.15. Докажите, что результат применения алгоритма Евклида к числам x, y выражается как линейная комбинация x и y с целыми коэффициентами: $z = ax + by$.

Задача 2.16. Пусть x, y – взаимно простые целые числа, а p – простое число. Предположим, что xy делится на p^α для некоторого натурального α. Докажите, что или x делится на p^α, или y делится на p^α.

Задача 2.17 (!). Выведите из этого однозначность разложения на простые множители: если целое положительное число x представлено в виде произведения простых чисел двумя способами, то эти два способа отличаются лишь порядком сомножителей.

Указание. Запишите x в виде произведения $p_i^{\alpha_i}$, где p_i разные простые числа, и воспользуйтесь предыдущей задачей, чтобы убедиться, что показатель α_i определен однозначно.

Факториальные кольца

Определение 2.7. Пусть R – кольцо. Два разложения $r \in R$ на простые множители, $r = p_1 p_2 ... p_k$, $r = q_1 q_2 ... q_k$ называются эквивалентными, если после некоторой перестановки сомножителей p_i и домножения простых сомножителей p_i на единицы кольца мы получим разложение $r = q_1 q_2 ... q_k$. Мы говорим, что R **факториальное**, или же **кольцо с однозначным разножением на множители**, если для любого $r \in R$ разложение r в произведение простых чисел существует и единственно с точностью до эквивалентности.

Замечание. Термин "факториальное" звучит страшно, но он, увы, вошел в традицию; по-английски, например, то же самое называется куда более понятным словосочетанием unique factorization ring (буквально "кольцо с единственным разложением").

Задача 2.18 (!). Пусть в кольце R существует разложение на простые множители, и наибольший общий делитель z любой пары элементов x, y. Пусть к тому же z выражается в R как линейная комбинация x, y: $z = ax + by$ с коэффициентами $a, b \in R$. Докажите, что R – факториальное кольцо.

Указание. Воспользуйтесь доказательством, приведенным выше для целых чисел.

Задача 2.19. Зафиксируем целое положительное число n. Рассмотрим кольцо $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{C}$ комплексных чисел вида $z = x + y\sqrt{-n}$, x и y целые. Докажите, что $|z|^2$ – целое для всех $z \in \mathbb{Z}[\sqrt{-n}]$.

Задача 2.20. Докажите, что z – единица в $\mathbb{Z}[\sqrt{-n}]$ тогда и только тогда, когда $|z|^2 = 1$.

Указание. $|z^{-1}|^2 = (|z|^2)^{-1}$.

Задача 2.21. Пусть z – такой элемент $\mathbb{Z}[\sqrt{-n}]$, что $|z|^2$ просто в $\mathbb{Z}$. Докажите, что z просто в $\mathbb{Z}[\sqrt{-n}]$.

Указание. $|zz'|^2 = |z|^2|z'|^2$.

Задача 2.22 (!). Рассмотрим кольцо $\mathbb{Z}[\sqrt{-3}]$. Докажите, что 2 и $1 \pm \sqrt{-3}$ простые. Выведите из этого, что $\mathbb{Z}[\sqrt{-3}]$ не факториально.

Указание. Воспользуйтесь соотношением $2^2 = 4$.

Деление с остатком в кольцах

Определение 2.8. Пусть R некоторое кольцо. Мы говорим, что в R **задано деление с остатком**, если для каждой пары x, y, $y \neq 0$ в R заданы $z, k \in R$, удовлетворяющее соотношению $z = x - ky$. В этом случае z называется **остатком от деления** и k **частным**.

Примеры. Деление с остатком задано в кольце целых чисел. Еще деление с остатком задано в кольце полиномов $k[t]$ над полем k:

$$\begin{array}{r|l} x^2 + 2x - 12 & x + 5 \\ \cline{2-2} \underline{x^2 + 5x} & x - 3 \\ \quad -3x - 12 & \\ \quad \underline{-3x - 15} & \\ \qquad\qquad 3 & \end{array}$$

Определение 2.9. Пусть в кольце R задано деление с остатком. **Алгоритм Евклида в** R применяется к паре x, y ненулевых элементов из R и определяется рекурсивно. Если x делится на y, алгоритм Евклида останавливается и выдает в качестве результата y. Если же x не делится на y, то алгоритм Евклида применяется к паре y, z, где z есть остаток от деления x на y. Априори, этот процесс может длиться бесконечно.

Задача 2.23 (!). Пусть в кольце R задано деление с остатком. Предположим, что алгоритм Евклида, примененный к паре $x, y \in R$, остановился через какое-то число шагов и выдал в качестве результата $z \in R$. Докажите, что

а. $z = ax + by$ для каких-то $a, b \in R$.

б. z есть наибольший общий делитель x и y.

Указание. Доказательство в случае произвольного кольца дословно такое же, как и для кольца целых чисел.

Определение 2.10. Пусть R кольцо. Говорится, что **в** R **существует алгоритм Евклида**, или же R **евклидово** если в R задано деление с остатком, и для любых $x, y \in R$ алгоритм Евклида заканчивается через конечное число шагов.

Задача 2.24 (!). Пусть в кольце R существует разложение на простые множители и алгоритм Евклида. Докажите, что R факториально.

Указание. Воспользуйтесь вышеприведенными задачами

Задача 2.25. Докажите, что кольцо $k[t]$ многочленов над полем k факториально.

Задача 2.26. Докажите, что уравнение $x \cdot y = 0$ неразрешимо (для $x, y \neq 0$) в $k[t] \mod P$ тогда и только тогда, когда многочлен P неприводим.

Целая часть $[z]$ комплексного числа $z = x + y\sqrt{-1}$ определяется как $[x+0.5]+[y+0.5]\sqrt{-1}$, где $[\ ]$ обозначает операцию взятия целой части для вещественного числа (если интерпретировать комплексные числа геометрически как точки плоскости $\mathbb{R}^2$, то $[z]$ – ближайшая к z точка с целыми координатами). Деление с остатком в кольце $\mathbb{Z}[\sqrt{-1}\,]$ целых гауссовых чисел определяется следующим образом: частное от деления с остатком z_1 на z_2 равно $[\frac{z_1}{z_2}]$, а остаток равен $z_1 - [\frac{z_1}{z_2}]z_2$.

Задача 2.27. Докажите, что $\left|z_1 - \left[\frac{z_1}{z_2}\right] z_2\right| < |z_2|$.

Задача 2.28. Докажите что в кольце $\mathbb{Z}[\sqrt{-1}\,]$ целых гауссовых чисел алгоритм Евклида всегда заканчивается.

Указание. Воспользуйтесь предыдущей задачей. Выведите, что на каждом шаге алгоритма Евклида уменьшается $\min(|z_1|^2, |z_2|^2)$.

Пусть $R = \mathbb{Z}[\sqrt{-n}]$ или $R = \widetilde{\mathbb{Z}[\sqrt{-3}]}$. Для любого $z \in \mathbb{C}$ обозначим за $[z]_R$ ближайшую к z точку комплексной плоскости, соответствующую числу из R. Если таких точек несколько, возьмем ту, в которой значение $Re[z]_R$ (вещественной части) больше, а если и таких точек несколько – возьмем ту, у которой $Im[z]_R$ (мнимая часть) больше. Определим деление z_1 на z_2 с остатком таким образом, что частное от деления с остатком z_1 на z_2 равно $[\frac{z_1}{z_2}]_R$, а остаток равен $z_1 - [\frac{z_1}{z_2}]_R z_2$.

Задача 2.29 (*). Докажите, что при $n = 1$ мы получим стандартное деление с остатком в $\mathbb{Z}[\sqrt{-1}\,]$

Задача 2.30 (*). Пусть $|z - [z]_R| < 1$ для всех $z \in \mathbb{C}$. Докажите, что на каждом шаге алгоритма Евклида уменьшается $|z_2|^2$.

Задача 2.31 (*). Пусть для каждой точки $z \in \mathbb{C}$ найдется $r \in R$ такой, что $|r - z| < 1$. Докажите, что R евклидово.

Задача 2.32 (*). Докажите, что следующие кольца евклидовы: $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\widetilde{\sqrt{-3}}]$.

Задача 2.33. Разложите число 2 на простые сомножители в $\mathbb{Z}[\sqrt{-1}\,]$.

Указание. Воспользуйтесь задачей 2.21.

Задача 2.34 (*). Разложите числа 3, 5, 7 на простые сомножители в $\mathbb{Z}[\sqrt{-1}\,]$.

Задача 2.35 (*). Докажите, что простое в $\mathbb{Z}$ число вида $p = 4k+3$ всегда просто в $\mathbb{Z}[\sqrt{-1}\,]$.

Указание. Докажите, что p не представимо в виде суммы квадратов

Задача 2.36. Пусть $z = a + b\sqrt{-1}$ целое гауссово число, которое не делится на $1 + \sqrt{-1}$. Предположим, что a и b взаимно просты. Докажите, что z и $\overline{z}$ взаимно просты.

Указание. Докажите, что если a и b взаимно просты в $\mathbb{Z}$, то 2 можно представить в виде линейной комбинации $a + b\sqrt{-1}$, $a - b\sqrt{-1}$.

Задача 2.37 (!). Пусть a, b, c – такие взаимно простые целые числа, что $a^2 + b^2 = c^2$. Докажите, что $c = |z|^2$, для какого-то $z \in \mathbb{Z}[\sqrt{-1}\,]$.

Указание. Воспользуйтесь тем, что $c^2 = (a + b\sqrt{-1}\,)(a - b\sqrt{-1}\,)$, а a, b взаимно просты. Примените единственность разложения на простые множители в $\mathbb{Z}[\sqrt{-1}]$, и выведите из этого, что каждый простой сомножитель $a + b\sqrt{-1}$, $a - b\sqrt{-1}$ встречается дважды.

Задача 2.38 (!). Укажите все тройки целых чисел a, b, c, таких, что $a^2 + b^2 = c^2$ ("укажите" следует понимать как "напишите формулу, которая дает все такие тройки при подстановке в нее целых чисел").

Указание. Воспользуйтесь предыдущей задачей.

Задача 2.39 (*). Укажите все тройки взаимно простых целых чисел a, b, c, таких, что $a^2 + 2b^2 = c^2$.

Задача 2.40. Примените однозначность разложения на множители в $\mathbb{Z}[\sqrt{-2}]$

Задача 2.41 (**). Укажите все тройки взаимно простых целых чисел a, b, c, таких, что $a^2 + 3b^2 = c^2$.