Определение 1. Пусть $a, b \in \mathbb{Z}$, причём $a \neq 0$ или $b \neq 0$. *Наибольшим общим делителем* a и b называется наибольшее целое число, делящее как a, так и b. Обозначение: НОД(a, b) или просто (a, b).
В том случае, когда $(a, b) = 1$, говорят, что числа a и b *взаимно простые*.

Задача 1. Пусть $a, b, k \in \mathbb{Z}$, причём $b \neq 0$. Докажите, что **а)** $(a, b) = (a - b, b)$; **б)** $(a, b) = (a - kb, b)$; **в)** если $a \vdots b$, то $(a, b) = |b|$; **г)** если r — остаток при делении a на b, то $(a, b) = (b, r)$.

Задача 2. Для каждого $n \in \mathbb{N}$ вычислите **а)** $(n, n+1)$; **б)** $(n, n+6)$; **в)** $(2n+3, 5n+7)$; **г)** $(n-1, n^3)$.

Задача 3°. Пусть $a, b \in \mathbb{Z}$, причём $a \neq 0$ или $b \neq 0$. Обозначим через M множество всех чисел, представимых в виде $ax + by$ (x и y — целые числа). Пусть d — наименьшее положительное число в M. Докажите, что: **а)** каждое число из M делится на любой общий делитель чисел a и b; **б)** каждое число из M делится на d; **в)** $d = (a, b)$.

Задача 4°. (*алгоритм Евклида*) Пусть $a, b \in \mathbb{Z}$, причём $b \neq 0$. Разделим a на b с остатком:

$$a = bq_1 + r_1, \text{ где } 0 \leqslant r_1 < b.$$

Если $r_1 = 0$, то процесс заканчивается. Если же $r_1 > 0$, то мы разделим b на r_1 с остатком:

$$b = r_1 q_2 + r_2, \text{ где } 0 \leqslant r_2 < r_1.$$

В том случае, когда $r_2 = 0$, процесс заканчивается. Если же $r_2 > 0$, то

$$r_1 = r_2 q_3 + r_3, \text{ где } 0 \leqslant r_3 < r_2,$$

и так далее. Докажите, что: **а)** процесс закончится через конечное число шагов; **б)** если r_n последний ненулевой остаток, то $r_n = (a, b)$.

Задача 5. Найдите **а)** $(347, 207)$; **б)** $(-475, -76)$; **в)** $(6188, 4709)$; **г)** $(7581, 1767)$; **д)** $(10946, 17711)$.

Задача 6. Для всех $m, n \in \mathbb{N}$ вычислите: **а)** $(\overbrace{11\ldots1}^{1001}, \overbrace{11\ldots1}^{57})$; **б)** (f_n, f_{n+1}); **в)*** (f_n, f_m); **г)*** $(2^n - 1, 2^m - 1)$; **д)*** $(2^{2^m} + 1, 2^{2^n} + 1)$. Здесь f_n — n-ое число Фибоначчи.

Задача 7. От прямоугольника со сторонами a и b, где $a > b$, отрезают квадрат со стороной b. Если получившийся прямоугольник не является квадратом, операцию повторяют.
а) На какие квадраты будет разрезан прямоугольник 16×22?
б) На какие квадраты будет разрезан прямоугольник 6188×4709?
в)* Какие прямоугольники окажутся разрезанными на конечное число квадратов?
г)* На какие квадраты будет разрезан прямоугольник $1 \times \sqrt{2}$?

Задача 8°. Пусть $a, b \in \mathbb{Z}$, причём $a \neq 0$ или $b \neq 0$. Как при помощи алгоритма Евклида найти такие целые числа x и y, что $ax + by = (a, b)$?

Задача 9. Найдите $x, y \in \mathbb{Z}$ такие, что $ax + by = (a, b)$, если **а)** $a = 525$, $b = 231$; **б)** $a = 645$, $b = 381$.

Задача 10. Пусть $a, b \in \mathbb{Z}$, причём $a \neq 0$ или $b \neq 0$. Докажите, что
а) для любого натурального k выполнено равенство $(ka, kb) = k \cdot (a, b)$;
б) если m — общий натуральный делитель чисел a и b, то $(a/m, b/m) = (a, b)/m$.

Задача 11. Пусть $a, b \in \mathbb{Z}$, причём $a \neq 0$ или $b \neq 0$. Докажите, что числа a и b взаимно просты тогда и только тогда, когда существуют такие целые x и y, что $ax + by = 1$.

Задача 12°. Пусть числа a, b и c — целые числа, не равные нулю. Докажите, что
а) если $ab \vdots c$, причём $(a, c) = 1$, то $b \vdots c$; **б)** если $c \vdots a$ и $c \vdots b$, причём $(a, b) = 1$, то $c \vdots ab$.

Определение 2. Уравнение, которое требуется решить в целых числах, называется *диофантовым*. *Линейным диофантовым уравнением* (от двух переменных) называется уравнение вида $ax + by = c$, где $a, b, c \in \mathbb{Z}$. Если же $c = 0$, то оно называется *однородным* (линейным диофантовым уравнением).

1а	1б	1в	1г	2а	2б	2в	2г	3а	3б	3в	4а	4б	5а	5б	5в	5г	5д	6а	6б	6в	6г	6д	7а	7б	7в	7г	8	9а	9б	10а	10б	11	12а	12б

Задача 13. **а)** Пусть (x_1, y_1) и (x_2, y_2) — два решения однородного уравнения. Докажите, что пары $(x_1 + x_2, y_1 + y_2)$ и $(x_1 - x_2, y_1 - y_2)$ также являются решениями однородного уравнения.
б) Пусть (x_1, y_1) и (x_2, y_2) — два решения линейного диофантового уравнения. Докажите, что пара $(x_1 - x_2, y_1 - y_2)$ является решением соответствующего однородного уравнения.
в) Докажите, что линейное уравнение $ax + by = c$ имеет решение в целых числах тогда и только тогда, когда c делится на (a, b).
г) Пусть $c \vdots (a, b)$. Придумайте способ, как находить хотя бы одно решение уравнения $ax + by = c$.
д)° Пусть (x_0, y_0) — одно из решений линейного диофантова уравнения $ax + by = c$. Докажите, что множество всех решений $\{(x, y)\}$ описывается формулами $x = x_0 + \dfrac{bt}{(a, b)}$, $y = y_0 - \dfrac{at}{(a, b)}$, где $t \in \mathbb{Z}$.
е)* Пусть $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. При каких k разрешимо диофантово уравнение $a_1x_1 + a_2x_2 + \ldots + a_nx_n = k$?

Задача 14. Решите следующие диофантовы уравнения: **а)** $21x + 9y = 7$; **б)** $17x + 23y = 36$; **в)** $31x - 133y = 2$; **г)** $7581x - 1767y = 171$; **д)** $nx + (2n - 1)y = 3$.

Задача 15. При каких a и b можно заплатить в кассу один рубль, имея на руках неограниченное количество a-рублёвых купюр, если в кассе есть неограниченное количество b-рублёвых купюр?

Задача 16. По окружности длины a см катится колесо, длина обода которого равна b см (a и b натуральные, $(a, b) = d$). В колесо вбит гвоздь, который оставляет отметки на окружности. Сколько отметок оставит гвоздь?

Определение 3. Пусть $f, g \in \mathbb{R}[x]$, причём $f \neq 0$ или $g \neq 0$. *Наибольшим общим делителем* f и g называется многочлен наибольшей степени, делящий как f, так и g. Обозначение: НОД(f, g) или (f, g). В том случае, когда $(f, g) = 1$, говорят, что многочлены f и g *взаимно простые*.

Задача 17°. Пусть $f, g \in \mathbb{R}[x]$, причём $f \neq 0$ или $g \neq 0$. Обозначим через M множество всех многочленов, представимых в виде $fu + gv$, где $u, v \in \mathbb{R}[x]$. Пусть d — один из многочленов наименьшей степени в M.
а) Докажите, что каждый многочлен из M делится на любой общий делитель многочленов f и g.
б) Докажите, что каждый многочлен из M делится на d.
в) Докажите, что (f, g) всегда существует, причём определен лишь с точностью до константы.
г) Сформулируйте и докажите алгоритм Евклида для многочленов.
д) Докажите, что (f, g) делится на любой другой общий делитель этих многочленов.
е) Докажите, что существуют $u, v \in \mathbb{R}[x]$ такие, что $(f, g) = uf + vg$.

Задача 18. Найдите (f, g), если **а)** $f(x) = x^2 - 4x + 3$ и $g(x) = 2x^2 + 4x - 6$; **б)** $f(x) = \frac{2}{3}x^4 + x^3 - \frac{1}{4}x^2 + 1$ и $g(x) = x^2 - x + \frac{1}{2}$; **в)** $f(x) = x^m - 1$ и $g(x) = x^n - 1$, где $m, n \in \mathbb{N}$.

Задача 19. Найдите (f, g) и его линейное выражение через $f, g \in \mathbb{R}[x]$, если
а) $f(x) = x^4 + x^3 - 3x^2 - 4x - 1$ и $g(x) = x^3 + x^2 - x - 1$;
б) $f(x) = x^4 + 2x^3 - x^2 - 4x - 2$ и $g(x) = x^4 + x^3 - x^2 - 2x - 2$.

Задача 20*. **а)** Для двух натуральных чисел, меньших миллиона, провели алгоритм Евклида. Докажите, что он состоял не более чем из 40 шагов.
б) Усовершенствуем алгоритм Евклида следующим образом. Будем заменять пару (a, b) на пару (b, r'), где $a \equiv r' \pmod b$ и $-b/2 < r \leqslant b/2$. Докажите, что такой ускоренный алгоритм Евклида также приведет к (a, b), причём если $|a| < 10^6$ и $|b| < 10^6$, то ему потребуется не более 20 шагов.
в) Для каких чисел от 1 до 100 алгоритм Евклида работает дольше всего?
г) А для каких чисел от 1 до 100 дольше всего работает ускоренный алгоритм Евклида?

Задача 21*. У Миши с Юрой есть шоколадка в форме равностороннего треугольника со стороной n, разделённая бороздками на дольки — равносторонние треугольники со стороной 1. За один ход можно отломать от шоколадки треугольный кусок вдоль бороздки и съесть его, а остаток передать противнику. Тот, кто получает последний кусок — треугольник со стороной 1 выигрывает. Если же игрок не может сделать ход, то он проигрывает. Кто выиграет при правильной игре, если Миша ходит первым?

13 а	13 б	13 в	13 г	13 д	13 е	14 а	14 б	14 в	14 г	14 д	15	16	17 а	17 б	17 в	17 г	17 д	17 е	18 а	18 б	18 в	19 а	19 б	20 а	20 б	20 в	20 г	21