Определение 1. Целое число $p > 1$ называется *простым,* если оно не имеет других положительных делителей, кроме 1 и себя. Говорят, что целое число $n > 1$ — *составное,* если оно не является простым.

Задача 1. Пусть n — произвольное целое число. Докажите, что наименьший натуральный делитель числа n, отличный от единицы, является простым числом.

Задача 2°. Докажите, что если целое число $p > 1$ не делится ни на одно из простых чисел, квадраты которых не превосходят p, то число p простое.

Задача 3. Докажите, что существует бесконечно много **а)°** простых чисел;
б) простых чисел вида $(4k-1)$, где $k \in \mathbb{N}$; **в)** простых чисел, не оканчивающихся на 1.

Задача 4°. Докажите, что если a и b — целые числа, а p — такое простое число, что ab делится на p, то либо a делится на p, либо b делится на p.

Задача 5°. (*Основная теорема арифметики*)
а) Докажите, что любое целое число, большее единицы, можно разложить в произведение простых чисел.
б) Докажите, что любое целое число n, большее единицы по модулю, однозначно представляется в виде $n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, где $p_1 < p_2 < \ldots < p_k$ — различные простые числа, а $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$.
Замечание 1. Разложение из задачи 5б называется *каноническим.*

Задача 6. **а)** На сколько нулей оканчивается число 2015!?
б)° (*Теорема Лежандра*) Докажите, что простое число p входит в каноническое разложение числа $n!$ в степени $[n/p] + [n/p^2] + [n/p^3] + \ldots$ (здесь $[x]$ — это целая часть числа x).

Задача 7. Найдите каноническое разложение: **а)** 7895250; **б)** 9919; **в)** 12345654321; **г)** 18!; **д)** C_{22}^{11}.

Задача 8. Пусть p — простое число, $m, n \in \mathbb{N}$. **а)** Докажите, что $C_p^k \vdots p$ при всех $0 < k < p$.
б)* В каких строках треугольника Паскаля все числа, кроме единиц, будут кратны p?
в)* Докажите, что простое число p входит в каноническое разложение числа C_{n+m}^n в степени, равной количеству переносов при сложении m с n в системе счисления с основанием p.
г)* Найдите наибольший общий делитель $(C_n^1, C_n^2, \ldots, C_n^{n-1})$.

Задача 9. Назовём чётное натуральное число n чётнопростым, если n не раскладывается в произведение двух чётных чисел. Например, 6 — чётнопростое, а 12 — нет. Какие пункты задач 4 и 5 останутся справедливыми, если в их формулировке заменить целые числа на чётные, а простые на чётнопростые?

Определение 2. *Наименьшим общим кратным* ненулевых целых чисел a и b называется наименьшее натуральное число, которое делится как на a, так и на b. Обозначение: НОК(a, b) или $[a, b]$.

Задача 10°. Пусть a и b — ненулевые целые числа. **а)** Докажите, что $[a, b]$ существует и единственно.
б) Как найти (a, b) и $[a, b]$, зная канонические разложения чисел a и b? **в)** Докажите, что $[a, b] \cdot (a, b) = ab$.
г) Верно ли, что любое общее кратное чисел a и b делится на $[a, b]$?
д) Найдите a и b, если $(a, b) = 15$ и $[a, b] = 840$.

Задача 11. Пусть $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. **а)** Найдите количество натуральных делителей числа n.
б)* Докажите, что сумма натуральных делителей числа n равна $\dfrac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \dfrac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \dfrac{p_k^{\alpha_k+1}-1}{p_k-1}$.
в)* Выведите формулу для суммы квадратов делителей числа n.

Задача 12*. Число, равное сумме всех своих натуральных делителей за исключением самого себя, называется *совершенным.* Докажите, что если числа p и $(2^p - 1)$ — простые, то число $2^{p-1} \cdot (2^p - 1)$ совершенно.

Задача 13*. Пусть $a, n \in \mathbb{N}$, $n > 1$. Докажите, что если $(a^n - 1)$ — простое число, то $a = 2$ и n — простое.
Замечание 2. Простые числа вида $(2^n - 1)$ называются *числами Мерсенна.*

Задача 14*. **а)** Докажите, что если число $(2^n + 1)$ — простое, то $n = 2^k$.
б) Докажите, что числа вида $(2^{2^k} + 1)$ являются взаимно простыми при различных k.
Замечание 3. Простые числа вида $(2^{2^k} + 1)$ называются *числами Ферма.*

1	2	3 а	3 б	3 в	4	5 а	5 б	6 а	6 б	7 а	7 б	7 в	7 г	7 д	8 а	8 б	8 в	8 г	9	10 а	10 б	10 в	10 г	10 д	11 а	11 б	11 в	12	13	14 а	14 б

Определение 3. Многочлен $p \in \mathbb{R}[x]$ называется *неприводимым,* если из равенства $p = fg$ следует, что либо $\deg(f) = 0$, либо $\deg(g) = 0$.

Задача 15°. **а)** Докажите, что если f и g — произвольные многочлены, а p — такой неприводимый многочлен, что $fg \vdots p$, то либо $f \vdots p$, либо $g \vdots p$.
б) Сформулируйте и докажите основную теорему арифметики для многочленов.

Задача 16°. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ — многочлен с целыми коэффициентами. Докажите, что если рациональное число $x = p/q$, где $(p, q) = 1$, является корнем многочлена f, то $a_0 \vdots p$, а $a_n \vdots q$.

Задача 17. Найдите каноническое разложение: **а)** $x^4 - 3x^2 + 2x$; **б)** $x^6 - 1$;
в)* $x^{10} + 2x^9 + 3x^8 + 4x^7 + 5x^6 + 6x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1$.

Определение 4. Пусть m — натуральное число, большее единицы. Обозначим через $\mathbb{Z}/m\mathbb{Z}$ множество остатков при делении на m, а через $\overline{n}$ — остаток от деления на m целого числа n. Определим в $\mathbb{Z}/m\mathbb{Z}$ операции суммы и произведения согласно следующим формулам: $a + b = \overline{a + b}$ и $a \cdot b = \overline{a \cdot b}$.

Задача 18. **а)** Докажите, что $\overline{a} = \overline{b}$ тогда и только тогда, когда $a \equiv b \pmod m$.
б) Составьте таблицы сложения и умножения в $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ и $\mathbb{Z}/10\mathbb{Z}$.

Задача 19°. Пусть p — простое число, $a \in \mathbb{Z}/p\mathbb{Z}$, причём $a \neq 0$. Докажите, что:
а) существует единственное число $x \in \mathbb{Z}/p\mathbb{Z}$ такое, что $ax \equiv 1 \pmod p$;
б) для любого $b \in \mathbb{Z}/p\mathbb{Z}$ сравнение $ax \equiv b \pmod p$ имеет ровно одно решение в $\mathbb{Z}/p\mathbb{Z}$;
в) числа a, $2a$, $3a$, …, $(p-1)a$ имеют попарно различные остатки при делении на p;
г) остаток от деления числа $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a$ на p не зависит от a;
д) (*Малая теорема Ферма*) $a^{p-1} \equiv 1 \pmod p$.
е)* Сколько решений в $\mathbb{Z}/m\mathbb{Z}$ имеет сравнение $ax \equiv b \pmod m$ для произвольного натурального $m > 1$?
Замечание 4. Решение сравнения $ax \equiv 1 \pmod p$ из задачи 19а называется *обратным* элементом к a. Обозначение: $x = a^{-1}$.

Задача 20. Пусть p — простое число, $a, b \in \mathbb{Z}/p\mathbb{Z}$.
а) Докажите, что $(a + b)^p \equiv a^p + b^p \pmod p$. **б)** Выведите из пункта а), что $a^p \equiv a \pmod p$.

Задача 21*. Пусть $\varphi(n)$ — количество натуральных чисел не превосходящих n и взаимно простых с ним.
а) Найдите $\varphi(p^k)$, если p — простое число, $k \in \mathbb{N}$. **б)** Верно ли, что если $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$?
в) Пусть $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Выведите формулу для $\varphi(n)$.
г) (*Теорема Эйлера*) Докажите, что если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod n$.
Замечание 5. Функция $\varphi(n)$ называется *функция Эйлера.*

Задача 22*. Пусть p — простое число, причём $p > 2$.
а) Докажите, что $x \equiv x^{-1} \pmod p$ тогда и только тогда, когда $x \equiv \pm 1 \pmod p$.
б) (*Теорема Вильсона*) Докажите, что $(p-1)! \equiv -1 \pmod p$.
в) Чему равно $(n-1)!$ в $\mathbb{Z}/n\mathbb{Z}$, если n — составное число?
г) Вычислите $(p-2)!$ в $\mathbb{Z}/p\mathbb{Z}$. **д)** Вычислите $((\frac{p-1}{2})!)^2$ в $\mathbb{Z}/p\mathbb{Z}$.

Задача 23*. **а)** Пусть p — простое число вида $(4k+1)$, где $k \in \mathbb{N}$. Докажите, что в этом случае сравнение $x^2 \equiv -1 \pmod p$ имеет ровно 2 решения.
б) Пусть p — простое число вида $(4k-1)$. Докажите, что сравнение $x^2 \equiv -1 \pmod p$ не имеет решений.
в) Какие простые числа могут входить в каноническое разложение числа вида (n^2+1), где $n \in \mathbb{N}$?
г) Докажите, что простых чисел вида $(4k+1)$ бесконечно много.

15 а	15 б	16	17 а	17 б	17 в	18 а	18 б	19 а	19 б	19 в	19 г	19 д	19 е	20 а	20 б	21 а	21 б	21 в	21 г	22 а	22 б	22 в	22 г	22 д	23 а	23 б	23 в	23 г

Примечание. Основам элементарной теории чисел посвящены VII, VIII и IX книги знаменитых «Начал» Евклида (ок. 325 г. - ок. 265 г. до н.э.). В них излагаются теория делимости и пропорций, доказывается бесконечность множества простых чисел, приводится алгоритм Евклида, строятся чётные совершенные числа. В своих трудах Евклид опирается на сочинения пифагорейцев (V век до н.э.), и по-видимому, это самая древняя по содержанию часть «Начал». Дальнейшие достижения европейских математиков в области теории чисел относятся к позднему Средневековью и Новому Времени, и связаны с именами таких учёных, как Марéн Мерсéнн (1588-1648 гг.), Пьер Фермá (1601-1665гг.) и Леонард Эйлер (1707-1783 гг.). На этом, конечно, развитие науки не остановилось, но из этой краткой исторической справки вы больше ничего не узнаете.