



Числа, вычисления и свойства чисел

Теория и разобранные примеры

Свойства, условия применения и пошаговые объяснения. Используйте оглавление и закладки PDF для перехода к нужной теме.

Содержание

01. Делимость: язык, а не операция	3
02. Теорема о делении с остатком	3
03. Почему алгоритм Евклида сохраняет НОД	4
04. Тождество Безу рождается из алгоритма Евклида	5
05. Лемма Евклида и уникальность простых множителей	5
06. НОД и НОК через показатели простых множителей	6
07. Квадраты, кубы и число делителей	7
08. Сравнения по модулю выводятся из делимости	8
09. Признаки делимости - следствия из десятичной записи	10
10. Линейные диофантовы уравнения	10
11. Полный разбор: Евклид превращается в решение уравнения	11
12. Полный разбор: делители, квадрат и куб в одной модели	12
13. Полный разбор: большая степень без вычисления	13
14. Полный разбор: цифры как переменные	13
15. Принцип Дирихле как доказательство неизбежности	14
16. Как строится доказательство	15
17. Теорема о делении с остатком: полное доказательство существования	15
18. Простые показатели как единая модель НОД, НОК и делителей	16
19. Два полезных следствия о квадратах и делимости	17
20. Три полноценных доказательных разбора	18
21. Практикум восстановления доказательства	19
22. Делимость на взаимно простые множители: доказательство без пропуска	19
23. Высокий уровень: показатели простых множителей в конструкции	20
24. Нечётное число делителей и полный квадрат	21
25. Классическое доказательство: $n^5 - n$ делится на 30	22

26. Выходной контроль: шесть вопросов	23
27. Быстрая проверка понимания	23
28. Эталонный разбор 1 • НОД и НОК как распределение простых степеней	24
29. Эталонный разбор 2 • Наибольший делитель выражения $n^7 - n$	24
30. Как объяснить метод замены одного элемента	25
31. Целочисленная точка и доказательство полноты	25

01. Делимость: язык, а не операция

Сначала на числах. 18 конфет можно разложить поровну в 3 коробки без остатка: $18 = 3 \cdot 6$. Это записывают $3 \mid 18$ и читают «3 делит 18». Порядок чисел важен: запись $18 \mid 3$ была бы неверной.

Определение. Для целых a и b , где $b \neq 0$, запись $b \mid a$ означает, что существует целое k такое, что

$$a = bk.$$

Из определения сразу выводятся основные факты.

Следствие 1. Если $d \mid a$ и $d \mid b$, то для любых целых x, y

$$d \mid (ax + by).$$

Доказательство. Из $a = du$ и $b = dv$ получаем

$$ax + by = d(ux + vy).$$

Правая часть содержит целый множитель после d , значит делимость доказана.

Следствие 2. Если $a \mid b$ и $b \mid c$, то $a \mid c$.

Доказательство. Пусть $b = ak$, $c = bt$. Тогда $c = a(kt)$.

Эти две короткие схемы нужно уметь восстанавливать. На них держатся алгоритм Евклида, признаки делимости и большая часть доказательств №19.

02. Теорема о делении с остатком

Остаток на понятном примере. Из 23 предметов можно составить 4 полные группы по 5; ещё 3 предмета останутся. Поэтому $23 = 5 \cdot 4 + 3$. Остаток меньше 5: если бы осталось 5 или больше, можно было бы составить ещё одну полную группу.

Теорема. Для любого целого a и натурального m существуют единственные целые q и r такие, что

$$a = mq + r, \quad 0 \leq r < m.$$

Почему существование правдоподобно. На числовой прямой кратные m разбивают её на промежутки длины m . Число a попадает ровно в один такой промежуток $[mq, m(q+1))$. Расстояние от левой границы и есть $r = a - mq$.

Доказательство единственности. Предположим, что

$$a = mq_1 + r_1 = mq_2 + r_2,$$

где $0 \leq r_1, r_2 < m$. Тогда

$$m(q_1 - q_2) = r_2 - r_1.$$

Правая часть по модулю меньше m . Единственное кратное m с таким свойством - ноль. Поэтому $r_1 = r_2$ и затем $q_1 = q_2$.

Пояснение. Остаток - не результат кнопки калькулятора. Это единственный представитель числа среди $0, 1, \dots, m - 1$.

03. Почему алгоритм Евклида сохраняет НОД

Зачем нужен НОД. Из 84 карандашей и 30 ручек нужно сделать максимальное число одинаковых наборов, используя всё. Число наборов должно делить и 84, и 30. Алгоритм Евклида даёт $84 = 2 \cdot 30 + 24$, $30 = 24 + 6$, $24 = 4 \cdot 6$, поэтому НОД равен 6. Получатся 6 наборов по 14 карандашей и 5 ручек.

Пусть

$$a = bq + r.$$

Теорема. Множество общих делителей пар (a, b) и (b, r) совпадает. Поэтому

$$\text{НОД}(a, b) = \text{НОД}(b, r).$$

Доказательство в обе стороны.

Шаг 1.

Если $d \mid a$ и $d \mid b$, то $d \mid (a - bq) = r$. Значит, d - общий делитель b и r .

Шаг 2.

Если $d \mid b$ и $d \mid r$, то $d \mid (bq + r) = a$. Значит, d - общий делитель a и b .

Мы не просто получили одинаковый наибольший делитель - доказали совпадение **всех** общих делителей. Поэтому повторная замена пары на «меньшее число и остаток» законна на каждом шаге.

Пример.

$$391 = 299 \cdot 1 + 92,$$

$$299 = 92 \cdot 3 + 23,$$

$$92 = 23 \cdot 4.$$

Последний ненулевой остаток равен 23, следовательно, $\text{НОД}(391, 299) = 23$.

04. Тожество Безу рождается из алгоритма Евклида

Теорема Безу. Для ненулевых целых a, b существуют целые x, y такие, что

$$ax + by = \text{НОД}(a, b).$$

Доказательство-конструкция. Каждый остаток алгоритма Евклида является целой линейной комбинацией a и b . Действительно, первый остаток $r_1 = a - bq_1$. Следующий остаток выражается через b и r_1 , а значит - снова через a и b . Продолжая обратную подстановку, выражаем последний ненулевой остаток, то есть НОД, в виде $ax + by$.

Для предыдущего примера:

$$23 = 299 - 3 \cdot 92 = 299 - 3(391 - 299) = 4 \cdot 299 - 3 \cdot 391.$$

Значит, $x = -3$, $y = 4$ - один из наборов коэффициентов Безу.

05. Лемма Евклида и уникальность простых множителей

Лемма Евклида. Если простое число p делит произведение ab , то $p \mid a$ или $p \mid b$.

Доказательство. Если $p \nmid a$, то $\text{НОД}(p, a) = 1$. По Безу существуют целые x, y такие, что

$$px + ay = 1.$$

Умножим на b :

$$pbx + aby = b.$$

Первое слагаемое слева делится на p . Второе тоже делится на p , потому что p делит ab . Следовательно, вся левая часть делится на p , а значит, p делит b .

Почему число 1 не простое и не составное

Определение. Простое натуральное число больше 1 и имеет ровно два натуральных делителя: 1 и само число. Составное натуральное число можно представить как произведение двух натуральных чисел, каждое из которых больше 1.

Число 1 имеет ровно один натуральный делитель и не представляется как произведение двух чисел больше 1. Поэтому оно не простое и не составное.

Это не формальная прихоть. Если бы 1 считалась простым числом, разложение было бы неединственным:

$$6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1^k \cdot 2 \cdot 3$$

для любого k . Исключение единицы сохраняет однозначность языка простых множителей.

Основная теорема арифметики

Теорема. Каждое натуральное число $n > 1$ раскладывается в произведение простых множителей, и это разложение единственно с точностью до порядка множителей.

Доказательство существования. Если n простое, разложение готово. Если составное, $n = ab$, где $1 < a, b < n$. Разлагаем a и b тем же способом. Числа уменьшаются, поэтому процесс обязательно заканчивается простыми множителями.

Доказательство единственности. Пусть есть два разложения

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t.$$

Простое p_1 делит произведение справа. По лемме Евклида оно равно одному из простых q_j . Сокращаем общий множитель и повторяем рассуждение. В конце остаются одинаковые наборы простых множителей.

06. НОД и НОК через показатели простых множителей

Запишем

$$a = \prod_p p^{\alpha_p}, \quad b = \prod_p p^{\beta_p},$$

где отсутствующему простому множителю соответствует показатель 0.

Теорема.

$$\text{НОД}(a, b) = \prod_p p^{\min(\alpha_p, \beta_p)},$$

$$\text{НОК}(a, b) = \prod_p p^{\max(\alpha_p, \beta_p)}.$$

Доказательство. Делитель обоих чисел не может содержать степень p выше ни α_p , ни β_p . Наибольшая допустимая степень - минимум. Кратное обоих чисел должно содержать не меньше каждой из двух степеней; наименьшая допустимая степень - максимум. Единственность простого разложения позволяет рассматривать каждый простой множитель отдельно.

Следствие. Для положительных a, b

$$\text{НОД}(a, b) \text{НОК}(a, b) = ab.$$

Доказательство. Для каждого простого p

$$\min(\alpha_p, \beta_p) + \max(\alpha_p, \beta_p) = \alpha_p + \beta_p.$$

Показатели простых множителей в обеих частях совпадают.

07. Квадраты, кубы и число делителей

Пусть

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}.$$

Теорема. Число n является квадратом тогда и только тогда, когда все α_i чётны.

Доказательство. Если $n = t^2$, каждый показатель простого множителя в t удваивается. Обратно, при чётных α_i число

$$t = p_1^{\frac{\alpha_1}{2}} \dots p_s^{\frac{\alpha_s}{2}}$$

натурально и $t^2 = n$.

Аналогично n является кубом тогда и только тогда, когда все показатели кратны 3.

Теорема о числе делителей.

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1).$$

Доказательство. Любой натуральный делитель имеет единственный вид

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad 0 \leq \beta_i \leq \alpha_i.$$

Для β_i есть $\alpha_i + 1$ независимый выбор. По правилу произведения число наборов равно произведению количеств выборов.

Пример: минимальное дополнение до куба. Если

$$n = 2^4 \cdot 3^2 \cdot 5,$$

то до кратных трём показателей не хватает 2^2 , 3 и 5^2 . Минимальный множитель равен

$$k = 2^2 \cdot 3 \cdot 5^2.$$

Минимальность доказана покомпонентно: для каждого простого добавлен наименьший возможный показатель.



Делители 216 имеют вид $2^i \cdot 3^j$. Четыре зелёные точки соответствуют квадратам.

08. Сравнения по модулю выводятся из делимости

Сравнение по модулю - одинаковые остатки. Числа 17 и 5 при делении на 4 дают остаток 1. Их разность 12 делится на 4, поэтому $17 \equiv 5 \pmod{4}$. Мы заменяем большое число меньшим, сохраняя информацию об остатке.

Определение.

$$a \equiv b \pmod{m}$$

означает $m \mid (a - b)$. Это равносильно тому, что a и b имеют одинаковый остаток при делении на m .

Теорема об операциях. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то

$$a + c \equiv b + d \pmod{m},$$

$$ac \equiv bd \pmod{m}.$$

Доказательство сложения. Разность

$$(a + c) - (b + d) = (a - b) + (c - d)$$

делится на m .

Доказательство умножения.

$$ac - bd = c(a - b) + b(c - d),$$

и оба слагаемых делятся на m .

Отсюда степени можно считать по остаткам, но не «по правилу», а потому что умножение сохраняет сравнимость.

Квадратичные остатки

Чтобы найти все остатки квадратов по модулю m , достаточно возвести в квадрат представителей $0, 1, \dots, m - 1$. Полнота обеспечена теоремой о делении с остатком.

Модуль	Проверка	Возможные остатки квадрата
4	$0^2, 1^2, 2^2, 3^2$	0, 1
8	квадраты остатков от 0 до 7	0, 1, 4
3	$0^2, 1^2, 2^2$	0, 1
5	квадраты остатков от 0 до 4	0, 1, 4

Пример невозможности. Уравнение $x^2 + y^2 = 4k + 3$ не имеет целых решений: каждый квадрат даёт остаток 0 или 1 по модулю 4, поэтому сумма не может дать остаток 3.

09. Признаки делимости - следствия из десятичной записи

Рассмотрим натуральное число с известным разложением на простые множители:

$$N = a_0 + 10a_1 + 10^2a_2 + \dots + 10^ka_k.$$

Делимость на 9 и 3

Поскольку $10 \equiv 1 \pmod{9}$, то $10^j \equiv 1 \pmod{9}$ для любого j . Следовательно,

$$N \equiv a_0 + a_1 + \dots + a_k \pmod{9}.$$

Тот же вывод работает по модулю 3. Значит, признак суммы цифр - не отдельная магическая команда, а замена каждой степени десятки на остаток 1.

Делимость на 11

Поскольку $10 \equiv -1 \pmod{11}$, степени десятки чередуют остатки $1, -1, 1, -1, \dots$. Поэтому N сравним по модулю 11 с чередующейся суммой цифр.

Делимость на 4 и 8

Так как $100 \equiv 0 \pmod{4}$, все разряды, кроме последних двух, исчезают по модулю 4. Аналогично $1000 \equiv 0 \pmod{8}$, поэтому делимость на 8 определяется последними тремя цифрами.

10. Линейные диофантовы уравнения

Рассмотрим

$$ax + by = c,$$

где требуются целые x, y .

Теорема. Решение существует тогда и только тогда, когда

$$\text{НОД}(a, b) \mid c.$$

Необходимость. Если решение есть, то каждый общий делитель a и b делит левую часть, следовательно, делит c .

Достаточность. Пусть $d = \text{НОД}(a, b)$ и $c = dt$. По Безу существуют u, v такие, что $au + bv = d$. Умножая на t , получаем

$$a(ut) + b(vt) = c.$$

Значит, $(x_0, y_0) = (ut, vt)$ - целое решение.

Все решения. Если (x_0, y_0) - одно решение, то

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t.$$

Здесь t - любое целое число.

Проверка подстановкой доказывает достаточность этой формы; вычитание двух решений показывает, что других нет. Если нужны положительные решения, остаётся наложить два неравенства на параметр t .

11. Полный разбор: Евклид превращается в решение уравнения

Решим в целых числах

$$391x + 299y = 23.$$

Алгоритм Евклида уже дал

$$23 = 4 \cdot 299 - 3 \cdot 391.$$

Поэтому одно решение:

$$x_0 = -3, \quad y_0 = 4.$$

Так как $d = \text{НОД}(391, 299) = 23$, все решения имеют вид

$$x = -3 + \frac{299}{23}t = -3 + 13t,$$

$$y = 4 - \frac{391}{23}t = 4 - 17t,$$

где t - любое целое число.

Почему форма полна. Пусть (x, y) - другое решение. Вычтем равенства для (x, y) и (x_0, y_0) :

$$391(x - x_0) + 299(y - y_0) = 0.$$

После деления на 23:

$$17(x - x_0) = -13(y - y_0).$$

Числа 17 и 13 взаимно просты, поэтому $13 \mid (x - x_0)$ и $17 \mid (y - y_0)$. Значит, разности имеют именно указанную параметрическую форму.

Проверьте себя. Что изменится, если справа будет 24? Решений не будет, потому что 23 не делит 24. Это нужно установить до попытки подбора.

12. Полный разбор: делители, квадрат и куб в одной модели

Рассмотрим натуральное число с известным разложением на простые множители:

$$N = 2^4 \cdot 3^3 \cdot 5^2.$$

Сколько делителей

Для делителя независимо выбираются показатели:

$$0 \leq \alpha \leq 4, \quad 0 \leq \beta \leq 3, \quad 0 \leq \gamma \leq 2.$$

Поэтому

$$\tau(N) = 5 \cdot 4 \cdot 3 = 60.$$

Сколько квадратных делителей

Показатели квадратного делителя должны быть чётными. Для двойки возможны 0, 2, 4 - три выбора; для тройки 0, 2 - два; для пятёрки 0, 2 - два. Итого

$$3 \cdot 2 \cdot 2 = 12.$$

Минимальное дополнение до квадрата

Нечётный показатель есть только у простого 3. Поэтому минимальный множитель равен 3. Утверждение о минимальности доказывается тем, что любой квадрат обязан иметь чётный показатель тройки.

Минимальное дополнение до куба

До кратных трём показателей не хватает 2^2 и 5. Для тройки добавлять ничего не нужно. Значит,

$$k = 2^2 \cdot 5 = 20.$$

Один и тот же набор показателей отвечает сразу на четыре разных вопроса. Это и есть смысл модели простых множителей.

13. Полный разбор: большая степень без вычисления

Найдём последние две цифры числа 7^{2026} .

Работаем по модулю 100:

$$7^1 \equiv 7,$$

$$7^2 \equiv 49,$$

$$7^3 \equiv 43,$$

$$7^4 \equiv 1 \pmod{100}.$$

После появления единицы цикл повторяется: умножение каждого остатка на $7^4 \equiv 1$ его не меняет. Поскольку

$$2026 = 4 \cdot 506 + 2,$$

получаем

$$7^{2026} \equiv 7^2 \equiv 49 \pmod{100}.$$

Последние две цифры - 49.

Почему остаток 0 при делении показателя на длину цикла не означает «нулевую позицию». Если показатель кратен 4, используется четвёртый элемент цикла, потому что нумерация степеней начинается с 1. Формально $7^{4q} = (7^4)^q \equiv 1$.

Проверка полноты. Мы не угадывали период по первым совпавшим цифрам. Равенство $7^4 \equiv 1$ доказывает, что с этого места любой остаток повторится после умножения на единицу.

14. Полный разбор: цифры как переменные

Найдём все четырёхзначные числа вида $3a7b$, делящиеся на 36.

Запись числа:

$$N = 3000 + 100a + 70 + b.$$

Так как $36 = 4 \cdot 9$ и $\text{НОД}(4, 9) = 1$, достаточно и необходимо проверить делимость на 4 и на 9.

По последним двум цифрам число $70 + b$ делится на 4. Среди цифр b это даёт

$$b = 2 \quad \text{или} \quad b = 6.$$

По признаку 9:

$$3 + a + 7 + b \equiv 0 \pmod{9}.$$

- При $b = 2$ получаем $a + 12 \equiv 0 \pmod{9}$, поэтому $a = 6$.
- При $b = 6$ получаем $a + 16 \equiv 0 \pmod{9}$, поэтому $a = 2$.

Ответ: 3672 и 3276.

Почему других чисел нет. Перебраны все цифры b , допустимые по делимости на 4, а для каждого такого b сравнение по модулю 9 имеет единственную цифру a от 0 до 9.

15. Принцип Дирихле как доказательство неизбежности

Теорема. Если $n + 1$ объект распределён по n ящикам, то хотя бы в одном ящике лежат не менее двух объектов.

Доказательство от противного. Если в каждом ящике не более одного объекта, всего объектов не более n . Это противоречит их количеству $n + 1$.

Числовое следствие. Среди любых $m + 1$ целых чисел найдутся два с одинаковым остатком при делении на m .

Доказательство. Ящики - классы остатков $0, 1, \dots, m - 1$, объекты - выбранные числа. Два числа в одном ящике имеют разность, делящуюся на m .

Пример. Среди любых 11 целых чисел найдутся два, разность которых делится на 10. Важно назвать и объекты, и ящики; фраза «по Дирихле» без построения соответствия не является доказательством.

0	1	2	3	4
5	6	7	8	9

Десять классов остатков по модулю 10. Среди одиннадцати чисел два попадают в один класс.

16. Как строится доказательство

Тип пункта	Что нужно доказать	Недостаточный ответ
а) пример	построенный объект выполняет все условия	число без проверки
б) существование или невозможность	пример либо противоречие из необходимых условий	фраза «очевидно нельзя»
в) общий факт	рассуждение для произвольного допустимого объекта и полнота случаев	проверка нескольких чисел

Протокол решения.

Шаг 1.

Перевести словесные условия в делимость, остатки, показатели простых множителей или диапазоны цифр.

Шаг 2.

Назвать доказанный факт, который связывает ограничения.

Шаг 3.

Получить конструкцию либо необходимое условие.

Шаг 4.

Проверить обратимость переходов.

Шаг 5.

Отдельно проверить границы, знаки, ноль и полноту перебора.

Критерий программы 55-100. Если ученик забыл признак или формулу, но за 30-60 секунд восстановил её из определения, это сильный результат. Если ученик назвал формулу, но не может объяснить её происхождение, понимание не сформировано.

17. Теорема о делении с остатком: полное доказательство существования

В основной части уже доказана единственность частного и остатка. Теперь закроем вторую половину теоремы: покажем, почему подходящие q и r действительно существуют для любого целого a и натурального m .

Неотрицательное делимое

Доказательство. Пусть a неотрицательно. Если $a < m$, берём $q = 0$ и $r = a$. Если $a \geq m$, последовательно вычитаем m . После каждого вычитания число уменьшается хотя бы на 1, поэтому процесс не может продолжаться бесконечно. В некоторый момент останется число r , для которого $0 \leq r < m$. Количество выполненных вычитаний обозначим q . Тогда $a = mq + r$.

$$a = mq + r, \quad 0 \leq r < m.$$

Здесь доказательство не ссылается на кнопку калькулятора и не использует ещё не определённую целую часть числа. Оно одновременно доказывает существование и даёт алгоритм нахождения q и r .

Отрицательное делимое

Доказательство. Для положительного числа $-a$ уже существуют Q и R такие, что $-a = mQ + R$, где $0 \leq R < m$. Если $R = 0$, то $a = m(-Q)$, и остаток равен нулю. Если $R > 0$, перепишем равенство так:

$$a = m(-Q - 1) + (m - R).$$

Число $m - R$ лежит между 0 и m , поэтому это допустимый остаток. Например, $-37 = 5 \cdot (-8) + 3$. Остаток равен 3, а не -2 , потому что по определению он должен быть неотрицательным и меньше модуля.

Проверка понимания. Найдите частное и остаток при делении -52 на 7 и объясните, почему запись $-52 = 7 \cdot (-7) - 3$ не является стандартным делением с остатком.

18. Простые показатели как единая модель НОД, НОК и делителей

Рассмотрим два числа и не будем применять отдельные готовые формулы. Разложим их на простые множители:

$$756 = 2^2 \cdot 3^3 \cdot 7, \quad 840 = 2^3 \cdot 3 \cdot 5 \cdot 7.$$

Решение. Общий делитель может содержать только те простые множители, которые присутствуют в обоих числах, и не выше меньшего показателя. Поэтому для 2 берём показатель 2, для 3 - показатель 1, для 7 - показатель 1. Простое 5 не входит в НОД.

$$\text{НОД}(756, 840) = 2^2 \cdot 3 \cdot 7 = 84.$$

Общее кратное обязано содержать оба исходных числа как делители. Поэтому для каждого простого множителя берём больший показатель:

$$\text{НОК}(756, 840) = 2^3 \cdot 3^3 \cdot 5 \cdot 7 = 7560.$$

Доказательство равенства $\text{НОД} \cdot \text{НОК} = ab$ теперь видно без запоминания. Для каждого простого числа меньший и больший показатели в сумме дают сумму исходных показателей. Значит, произведения имеют одинаковое разложение на простые множители.

Задача. Сколько общих натуральных делителей у 756 и 840? Любой общий делитель является делителем их НОД, то есть числа $84 = 2^2 \cdot 3 \cdot 7$. Показатель двойки можно выбрать тремя способами, тройки - двумя, семёрки - двумя.

$$(2 + 1)(1 + 1)(1 + 1) = 12.$$

Почему это важно. Одна модель отвечает на вопросы о НОД, НОК, количестве делителей, квадрате, кубе и минимальном дополнении. Ученик сильной группы должен не переключаться между шестью правилами, а видеть показатели простых множителей.

19. Два полезных следствия о квадратах и делимости

Если квадрат делится на простое число

Теорема. Если квадрат целого числа n делится на простое число p , то само n делится на p .

Доказательство. В разложении n^2 показатель каждого простого множителя вдвое больше показателя в n . Если p делит n^2 , его показатель в n^2 положителен. Этот показатель чётный, поэтому он не меньше 2. Следовательно, в n показатель p не меньше 1, а значит, p делит n .

Контрпример к неверному расширению. Если составное число 12 делит n^2 , из этого не следует, что 12 делит n . При $n = 6$ квадрат 36 делится на 12, но 6 на 12 не делится. Для составного делителя нужно анализировать показатели каждого простого множителя отдельно.

Когда квадрат делится на 12

Задача. Докажите: если n^2 делится на 12, то n делится на 6. Число $12 = 2^2 \cdot 3$. В n^2 показатель двойки не меньше 2, значит, в n он не меньше 1. Показатель тройки в n^2 не меньше 1, но он чётный, поэтому фактически не меньше 2; в n показатель тройки не меньше 1. Следовательно, n содержит множители 2 и 3.

$$6 \mid n.$$

Проверка. Обратное утверждение тоже верно: если n делится на 6, то n^2 делится на 36, а значит, и на 12. Поэтому условие можно сформулировать как равносильность.

20. Три полноценных доказательных разбора

Разбор 1. Невозможность по остаткам

Задача. Докажите, что уравнение $x^2 + y^2 = 8k + 6$ не имеет целых решений.

Решение. Любое целое число при делении на 8 имеет один из остатков 0, 1, 2, 3, 4, 5, 6, 7. Квадраты этих остатков дают только 0, 1 или 4. Поэтому сумма двух квадратов может дать остаток 0, 1, 2, 4 или 5, но не 6. Правая часть имеет остаток 6. Получено противоречие.

Почему доказательство полное. Мы проверили не несколько удобных чисел, а все восемь классов остатков. Теорема о делении с остатком гарантирует, что другого класса у целого числа нет.

Разбор 2. Линейное уравнение и положительные решения

Задача. Найдите все целые решения уравнения $84x + 126y = 210$ и определите, есть ли среди них решения с $x > 0$ и $y > 0$.

Решение. НОД(84, 126) = 42, и 42 делит 210, поэтому решения существуют. После деления на 42 получаем $2x + 3y = 5$. Одно решение: $x = 1, y = 1$. Все решения имеют вид:

$$x = 1 + 3t, \quad y = 1 - 2t, \quad \text{где } t - \text{целое число.}$$

Проверка полноты. Подстановка даёт $2(1 + 3t) + 3(1 - 2t) = 5$. Если x и y положительны, то $1 + 3t > 0$ и $1 - 2t > 0$. Для целого t обе системы выполняются только при $t = 0$. Значит, единственное положительное решение - $(1; 1)$.

Разбор 3. Цифры и два независимых условия

Задача. Найдите все четырёхзначные числа вида $4a5b$, которые делятся на 45.

Решение. Так как $45 = 5 \cdot 9$ и НОД(5, 9) = 1, нужны делимость на 5 и на 9. Из делимости на 5 получаем $b = 0$ или $b = 5$. Сумма цифр равна $9 + a + b$ и должна делиться на 9.

При $b = 0$ допустимы $a = 0$ или $a = 9$. При $b = 5$ условие $14 + a$ кратно 9 даёт $a = 4$. Получаем числа 4050, 4950 и 4455.

Проверка. Для каждого найденного числа отдельно проверяем исходный вид, четырёхзначность и делимость на 45. Других ответов нет, потому что перебраны оба возможных значения последней цифры и все цифры a от 0 до 9, удовлетворяющие сравнению.

21. Практикум восстановления доказательства

- **Опора 1:** «Общий делитель делит любую целую линейную комбинацию». Восстановите доказательство неизменности НОД в алгоритме Евклида.
- **Опора 2:** «Последний ненулевой остаток выражается через исходные числа». Восстановите тождество Безу на конкретной паре 391 и 299.
- **Опора 3:** «Простое число делит произведение». Покажите, где в доказательстве леммы Евклида используется простота p .
- **Опора 4:** «Каждая степень десятки имеет известный остаток». Выведите признаки делимости на 9 и на 11.
- **Опора 5:** «Показатели простых множителей независимы». Докажите критерий квадрата и формулу числа делителей.

Критерий ответа. Ученик должен назвать исходное определение, выполнить хотя бы один содержательный переход, указать использованное условие и объяснить полноту. Название теоремы без этой цепочки не засчитывается.

22. Делимость на взаимно простые множители: доказательство без пропуска

Теорема. Если a и b взаимно просты, a делит n и b делит n , то произведение ab делит n .

Доказательство. Из $a|n$ существует целое k такое, что $n = ak$. Поскольку $b|n$, число b делит произведение ak . У чисел a и b нет общих простых делителей. Поэтому каждый простой множитель b обязан входить в k с не меньшим показателем: иначе в произведении ak его не хватило бы для делимости на b . Значит, $b|k$.

$$k = bt, \quad \text{поэтому} \quad n = ak = abt.$$

Получили $ab|n$. Это тот переход, который используется в признаке делимости на 72: делимость на 8 и на 9 можно объединить, потому что $\text{НОД}(8, 9) = 1$.

Контрпример. Без взаимной простоты утверждение неверно. Число 12 делится на 4 и на 6, но не делится на 24. Общий множитель 2 был дважды учтён при перемножении условий.

Следствие. Если числа $a_1, a_2, \dots, a_k$ попарно взаимно просты и каждое из них делит n , то их произведение делит n . Доказательство выполняется последовательным применением теоремы: сначала объединяем первые два множителя, затем полученное произведение с третьим и так далее.

23. Высокий уровень: показатели простых множителей в конструкции

Минимальное число с пятнадцатью делителями

Задача. Найдите наименьшее натуральное число, у которого ровно 15 натуральных делителей.

Решение. Если $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots$, то число делителей равно $(\alpha_1 + 1)(\alpha_2 + 1) \dots$. Число 15 раскладывается как 15 или как $5 \cdot 3$. Поэтому возможны два типа показателей: 14 либо 4 и 2.

Для первого типа минимально число $2^{14} = 16384$. Для второго типа больший показатель нужно поставить у меньшего простого числа: $2^4 \cdot 3^2 = 144$. Если поменять показатели местами, получится $2^2 \cdot 3^4 = 324$, то есть больше.

Наименьшее число равно 144.

Почему перебор полный. Других разложений числа 15 на множители, большие единицы, нет. Добавление нового простого множителя создало бы ещё один множитель не меньше 2 в формуле количества делителей.

Одновременно получить квадрат и куб

Задача. Найдите наименьшее натуральное n , для которого $72n$ является квадратом, а $100n$ - кубом.

Разложим исходные числа: $72 = 2^3 \cdot 3^2$, $100 = 2^2 \cdot 5^2$. Обозначим показатели простых 2, 3, 5 в n через u, v, w .

Для квадрата показатели в $72n$ должны быть чётными: $u + 3$ чётно, $v + 2$ чётно, w чётно. Для куба показатели в $100n$ должны делиться на 3: $u + 2$ делится на 3, v делится на 3, $w + 2$ делится на 3.

Наименьшие неотрицательные показатели, выполняющие обе пары условий: $u = 1, v = 0, w = 4$. Для любого другого простого множителя показатель должен одновременно быть чётным и делиться на 3, поэтому минимально он равен нулю.

$$n = 2 \cdot 5^4 = 1250.$$

Проверка: $72 \cdot 1250 = 90000 = 300^2$; $100 \cdot 1250 = 125000 = 50^3$. Минимальность доказана отдельно для каждого простого показателя, а не только сравнением нескольких кандидатов.

24. Нечётное число делителей и полный квадрат

Теорема. Натуральное число имеет нечётное число натуральных делителей тогда и только тогда, когда оно является полным квадратом.

Доказательство через пары делителей

Каждому делителю d числа n соответствует парный делитель $\frac{n}{d}$. Обычно эти два делителя различны, поэтому делители разбиваются на пары и их количество чётно. Непарный делитель появляется только тогда, когда $d = \frac{n}{d}$, то есть $d^2 = n$. Следовательно, нечётное число делителей возможно только у квадрата.

Обратно, если $n = s^2$, делитель s образует пару сам с собой, а все остальные делители по-прежнему разбиваются на различные пары. Поэтому общее число делителей нечётно.

Доказательство через простые показатели

Если $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то число делителей равно $(\alpha_1 + 1) \dots (\alpha_k + 1)$. Произведение нечётно тогда и только тогда, когда каждый множитель $\alpha_i + 1$ нечётен, то есть каждый α_i чётен. Это в точности критерий полного квадрата.

Задача. Может ли натуральное число иметь ровно 45 делителей и не быть квадратом? Нет. Число 45 нечётно, поэтому по доказанной теореме любое число с таким количеством делителей является квадратом.

Произведение всех делителей

Если делители n разбить на пары d и $\frac{n}{d}$, произведение каждой пары равно n . При чётном количестве делителей τ произведение всех делителей равно $n^{\frac{\tau}{2}}$.

Если n - квадрат и количество делителей нечётно, один делитель $\sqrt{n}$ остаётся без пары. Остальные $(\tau - 1)$ делителей образуют $\frac{\tau - 1}{2}$ пар, поэтому общее произведение равно $n^{\frac{\tau-1}{2}} \cdot \sqrt{n}$, что снова соответствует степени $n^{\frac{\tau}{2}}$.

Пример. У числа $72 = 2^3 \cdot 3^2$ количество делителей равно $4 \cdot 3 = 12$. Следовательно, произведение всех его натуральных делителей равно 72^6 . Перечислять двенадцать делителей не требуется.

Вопрос ученику. Где в доказательстве используется положительность натуральных делителей? Объясните, почему для целых делителей с учётом знаков парная модель выглядела бы иначе.

25. Классическое доказательство: $n^5 - n$ делится на 30

Задача. Докажите, что для любого целого n число $n^5 - n$ делится на 30. Поскольку $30 = 2 \cdot 3 \cdot 5$ и числа 2, 3, 5 попарно взаимно просты, достаточно отдельно доказать делимость на каждый из трёх множителей.

Делимость на 2

Если n чётно, оба слагаемых n^5 и n чётны. Если n нечётно, n^5 также нечётно, а разность двух нечётных чисел чётна. В обоих случаях $n^5 - n$ делится на 2.

Делимость на 3

Любое целое n при делении на 3 имеет остаток 0, 1 или 2. Остаток 2 удобно записать как -1 . Для остатков 0, 1 и -1 пятая степень имеет тот же остаток, что и само число. Поэтому разность $n^5 - n$ даёт остаток 0 по модулю 3.

Делимость на 5

При делении на 5 достаточно проверить остатки 0, ± 1 и ± 2 . Для 0 и ± 1 утверждение очевидно. Для 2 получаем $2^5 - 2 = 32 - 2 = 30$, а для -2 - противоположное число -30 . Все значения делятся на 5.

Итак, $n^5 - n$ делится на 2, на 3 и на 5. По теореме о взаимно простых делителях оно делится на их произведение 30.

Почему перебор не является угадыванием. Теорема о делении с остатком гарантирует, что перечисленные классы покрывают все целые числа. Мы проверили не несколько примеров n , а все возможные остатки.

Более короткое родственное утверждение

Из разложения $n^3 - n = n(n-1)(n+1)$ видно, что произведение трёх последовательных целых чисел делится на 2 и на 3: среди них есть чётное число и ровно одно число, кратное 3. Поэтому $n^3 - n$ делится на 6.

Вопрос ученику. Почему из делимости на 2 и на 3 можно сделать вывод о делимости на 6, а из делимости на 4 и на 6 нельзя автоматически получить делимость на 24? Ответ должен содержать условие взаимной простоты.

Экзаменационный стандарт. В доказательстве для произвольного n необходимо показать полноту классов остатков и только затем объединить независимые условия делимости.

26. Выходной контроль: шесть вопросов

Шаг 1.

Почему число 1 не простое и не составное и как это связано с единственностью разложения?

Шаг 2.

Докажите равенство $\text{НОД}(a, b) = \text{НОД}(b, a - bq)$.

Шаг 3.

Восстановите доказательство $\text{НОД}(a, b)\text{НОК}(a, b) = ab$.

Шаг 4.

Почему квадрат не может давать остаток 2 по модулю 4?

Шаг 5.

Выведите признак делимости на 9 из десятичной записи.

Шаг 6.

Докажите критерий существования целых решений $ax + by = c$.

27. Быстрая проверка понимания

Вопрос ученику	Критерий полного ответа
Почему 1 не простое число?	У него один положительный делитель; иначе исчезает единственность разложения.
Почему алгоритм Евклида сохраняет НОД?	Множества общих делителей пар (a, b) и (b, r) совпадают.
Когда $ax + by = c$ имеет целые решения?	Тогда и только тогда, когда $\text{НОД}(a, b)$ делит c .
Почему квадрат не даёт остаток 2 по модулю 4?	Проверяются два класса чётности.
Что нужно доказать в задаче «найдите все»?	Построить ответы и доказать отсутствие других.
Как проверить конструкцию №19?	Поочерёдно проверить каждое условие исходной задачи.

Два общих эталона по теме урока: №19: делимость, НОД/НОК, число делителей и доказательство максимальности. Это не набор коротких шаблонов, а полные модели экзаменационного рассуждения.

28. Эталонный разбор 1 • НОД и НОК как распределение простых степеней

Условие

Натуральные числа a и b удовлетворяют $\text{НОД}(a, b) = 18$ и $\text{НОК}(a, b) = 3780$.

а) Приведите пример такой упорядоченной пары.

б) Найдите количество всех упорядоченных пар (a, b) .

Решение с обоснованием

Шаг 1. Запишем $a = 18u, b = 18v$. Условие на НОД равносильно $\text{НОД}(u, v) = 1$.

Шаг 2. Из $\text{НОД}(a, b) \cdot \text{НОК}(a, b) = ab$ получаем $uv = \frac{3780}{18} = 210 = 2 \cdot 3 \cdot 5 \cdot 7$.

Шаг 3. Из взаимной простоты u и v следует: каждый из четырёх простых множителей целиком выбирает одно из двух чисел. Значит, упорядоченных распределений $2^4 = 16$.

Шаг 4. Например, $u = 1, v = 210$ дают пару $(18; 3780)$.

Контроль полноты. Любое распределение четырёх простых множителей создаёт взаимно простые u, v , и каждое допустимое u, v возникает ровно одним способом.

Ответ. а) например, $(18; 3780)$; б) 16 пар.

Экзаменационный акцент. Ключевой критерий: не только получить число 16, но и доказать взаимно однозначное соответствие с распределениями.

29. Эталонный разбор 2 • Наибольший делитель выражения $n^7 - n$

Условие

Найдите наибольшее натуральное k , для которого $n^7 - n$ делится на k при любом целом n .

Решение с обоснованием

Шаг 1. Для любого n числа n^7 и n имеют одинаковую чётность, поэтому $n^7 - n$ делится на 2.

Шаг 2. По остаткам $0, \pm 1 \pmod{3}$ имеем $n^7 \equiv n \pmod{3}$, значит, выражение делится на 3.

Шаг 3. По малой теореме Ферма $n^7 \equiv n \pmod{7}$, поэтому выражение делится на 7. Числа 2, 3, 7 попарно взаимно просты, следовательно, делимость на 42 доказана.

Шаг 4. Чтобы доказать максимальность, используем два значения: при $n = 2$ получаем 126, при $n = 3$ - 2184. Их НОД равен 42, поэтому любой универсальный k обязан делить 42.

Контроль полноты. Доказаны и достаточность $k = 42$ для произвольного n , и невозможность большего k через НОД двух конкретных значений.

Ответ. $k = 42$.

Экзаменационный акцент. Полный ответ требует отдельного доказательства максимальности; одной делимости на 42 недостаточно.

30. Как объяснить метод замены одного элемента

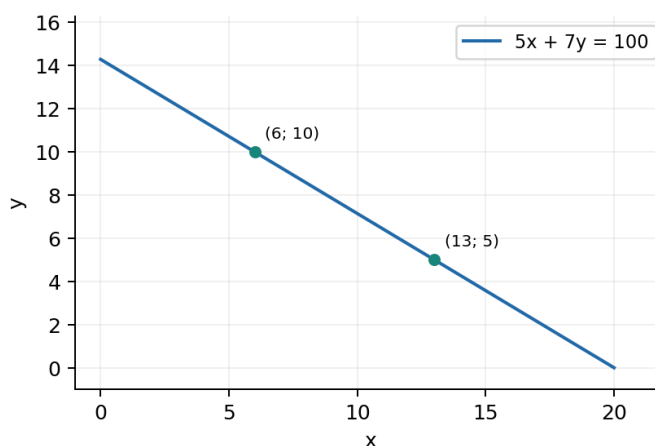
В задачах о средних арифметических удобно сравнивать два набора, различающиеся ровно одним элементом. Например, если суммы любых четырёх чисел делятся на 4, то суммы $u+c+d+e$ и $v+c+d+e$ дают разность $u-v$, делящуюся на 4. Общие слагаемые исчезают.

Если дополнительно целым является среднее любых пяти, разность $u-v$ делится и на 5. Взаимная простота 4 и 5 даёт модуль 20. В конце нужно доказать обратное утверждение и построить набор, достигающий найденной оценки. Это отличает полное решение от одного необходимого ограничения.

31. Целочисленная точка и доказательство полноты

На прямой $5x + 7y = 100$ бесконечно много действительных точек, но положительных целочисленных только две. Из сравнения по модулю 5 следует $y = 5k$, затем $x = 20 - 7k$. Условия положительности оставляют $k = 1, 2$.

Рисунок помогает увидеть точки, а параметризация доказывает, что других нет. При переходе от положительных к неотрицательным решениям границы нужно проверить заново.



Положительным целым координатам соответствуют только две точки.