

БАЗОВАЯ ТЕОРИЯ ЧИСЕЛ

Содержание

1. Делимость целых чисел	2
1.1 Делимость и ее базовые свойства.	2
1.2 Деление с остатком	3
1.3 Сравнения по модулю	4
1.4 Десятичная запись числа. Признаки делимости.	4
1.5 Кольцо классов вычетов.	6
1.6 НОД и НОК.	7
1.7 Алгоритм Евклида. Обобщенный алгоритм Евклида.	8
1.8 Линейное представление НОД и решение уравнений в целых числах.	10

1. Делимость целых чисел

1.1 Делимость и ее базовые свойства.

В этом параграфе все числа целые, если иного не оговорено.

Definition 1. Число a делится на число $b \neq 0$ ($a : b$), если существует такое число c , что $a = b \cdot c$. В этом случае говорят, что b — делит a и пишут $b \mid a$.

Базовые факты, связанные с делимостью:

1. $a : 1$.
2. $a : m$ и $b \implies (a \pm b) : m, ab : m$.
3. $a : m$ и $b : m \implies \forall k, l \in \mathbb{Z} (ka \pm lb) : m$.
4. $a : m$ и $b \not: m \Leftrightarrow (a \pm b) \not: m \implies (a \pm b) \not: m$.
5. $a : m$ и $m : k \implies a : k$.
6. $b : a \implies |a| \leq |b|$.

Remark 1. Заметим, что с делением на 0 получается достаточно тонкий вопрос. Формально, 0 можно делить на 0 и результат будет произвольным, так как $\forall a \in \mathbb{Z} a \cdot 0 = 0$.

Доказательство. Всё это доказывается как-то так:

$$a : m \Leftrightarrow a = q \cdot m, q \in \mathbb{Z}, b : m \Leftrightarrow b = p \cdot m, p \in \mathbb{Z} \Rightarrow a \pm b = q \cdot m \pm p \cdot m = m \cdot (p + q) \Leftrightarrow (a \pm b) : m$$

□

Example 1. Найдите все такие натуральные числа a , что $\frac{2a+1}{a-2}$ — целое число.

Решение: $\frac{2a+1}{a-2} \in \mathbb{Z} \Leftrightarrow (2a+1) : (a-2)$, а значит и разность этих чисел делится на $(a-2)$.

То есть, $((2a+1) - (a-2)) : (a-2) \Leftrightarrow (a+3) : (a-2)$.

Кроме того, разность этого числа и $(a-2)$ также должна делиться на $(a-2)$, то есть $((a+3) - (a-2)) : (a-2) \Leftrightarrow 5 : (a-2)$.

То есть, $(a-2)$ — делитель числа 5, а значит он может быть равен 1, -1, 5, -5. Переберем все случаи, так как их не так много:

1. $a - 2 = -1 \Leftrightarrow a = 1$. $\frac{2a+1}{a-2} = \frac{2+1}{1-2} = -3 \in \mathbb{Z}$, а значит $a = 1$ подходит.
2. $a - 2 = 1 \Leftrightarrow a = 3$. $\frac{2a+1}{a-2} = \frac{6+1}{3-2} = 7 \in \mathbb{Z}$, а значит $a = 3$ подходит.
3. $a - 2 = -5 \Leftrightarrow a = -3$, но $a \in \mathbb{N}$, а значит этот случай не подходит.
4. $a - 2 = 5 \Leftrightarrow a = 7$. $\frac{2a+1}{a-2} = \frac{14+1}{7-2} = 3 \in \mathbb{Z}$, а значит $a = 7$ подходит.

Ответ: $\{1, 3, 7\}$.

Свойства четных и нечетных чисел:

1. Сумма двух последовательных натуральных чисел — нечетное число.
2. Сумма четного и нечетного чисел — нечетное число.
3. Сумма любого количества четных чисел — четное число.
4. Сумма четного количества нечетных чисел — четное число, в то время как сумма нечетного количества нечетных чисел — нечетное число.
5. Произведение двух последовательных натуральных чисел — четное число.

Theorem 1. Произведение двух последовательных натуральных чисел делится на 2. Произведение трёх последовательных натуральных чисел делится на 6.

Example 2. В ряд выписаны числа от 1 до 10. Можно ли расставить между ними знаки «+» и «−» так, чтоб значение полученного выражения было равно нулю?

Решение:

Среди чисел от 1 до 10 имеется ровно 5 нечетных чисел, а значит, их сумма, вне зависимости от того, с каким знаком их брать, будет нечетным числом, а значит и сумма всех чисел будет нечетным числом. То есть, нулем она быть не может, так как ноль - четное число.

Ответ: нет.

Definition 2. Число $p \in \mathbb{N}$ называется простым, если $p > 1$ и p не имеет положительных делителей, отличных от 1 и p .

Statement 1. Если p_1 и p_2 — простые числа и $p_1 : p_2$, то $p_1 = p_2$.

Theorem 2 (Евклид). Множество положительных простых чисел счетно.

Доказательство. Будет добавлено. □

Theorem 3. Для любого $k \in \mathbb{N}$ в натуральном ряду можно найти k составных чисел, непосредственно следующих друг за другом.

Доказательство. Будет добавлено. □

Definition 3. Натуральное число $n \in \mathbb{N}$ называется составным, если оно имеет хоть один положительный делитель, отличный от 1 и n .

Remark 2. Число 1 не является ни простым, ни составным.

1.2 Деление с остатком

Definition 4. Пусть a и $b \neq 0$ — два целых числа. Разделить число a на число b с остатком — значит найти такие целые числа q и r , что выполнены следующие условия:

1. $a = bq + r$
2. $0 \leq r < |b|$

При этом число q называется неполным частным, а число r — остатком от деления числа a на b .

Theorem 4. Для любых $a, b \in \mathbb{Z}$ существуют единственные $q, r \in \mathbb{Z}$, $0 \leq r < |b|$, что $a = bq + r$.

Доказательство. Будет написано. □

Corollary 1. Пусть $m \in \mathbb{N}$, $m > 1$. Каждое целое число при делении на m даёт некоторый остаток, причем остатков ровно m . Это могут быть числа $0, 1, \dots, m - 1$.

Рассмотрим некоторые элементарные методы вычисления остатка.

Theorem 5. Сумма (произведение) чисел a и b дает тот же остаток при делении на число m , что и сумма (произведение) остатков чисел a и b при делении на число m .

Example 3. Найдите остаток числа 2^{2012} при делении на 3.

Решение:

Заметим, что $2^{2012} = 4^{1006}$. Число 4 дает остаток 1 при делении на 3, а значит по теореме выше (о произведении остатков), 4^k даст остаток $1^k = 1$.

Ответ: 1.

1.3 Сравнения по модулю

Definition 5. Если целые числа a и b при делении на натуральное число m дают равные остатки, то говорят, что a сравнимо с b по модулю m и пишут $a \equiv b \pmod{m}$. Иначе говоря, такая запись означает, что $(a - b)$ делится на m .

При помощи таких обозначений громоздкое предложение « a дает остаток b при делении на c » теперь можно записать, как $a \equiv b \pmod{c}$.

На мой взгляд, работать с остатками в целом гораздо проще при помощи сравнений по модулю. У сравнений есть множество полезных свойств, рассмотрим самые основные:

Основные свойства сравнений по модулю:

1. Арифметические действия:

$$\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \implies \begin{cases} (a \pm c) \equiv (b \pm d) \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases}$$

2. Возведение в степень:

$$a \equiv b \pmod{m} \implies a^k \equiv b^k \pmod{m}$$

3. Перенос в другую часть равенства:

$$(a + b) \equiv c \pmod{m} \implies a \equiv (c - b) \pmod{m}$$

4. Транзитивность:

$$\begin{cases} a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{cases} \implies a \equiv c \pmod{m}$$

5. Если $ak \equiv bk \pmod{m}$, а числа k и m взаимнопросты, то $a \equiv b \pmod{m}$.

6. Если $a \equiv b \pmod{m}$, а d — делитель числа m , то $a \equiv b \pmod{d}$.

Доказательство. Будет добавлено.

□

Statement 2. Сравнимость по модулю — отношение эквивалентности.

Доказательство. Будет добавлено.

□

1.4 Десятичная запись числа. Признаки делимости.

Definition 6. Любое натуральное число представимо в виде:

$$n = \overline{a_k a_{k-1} \dots a_0} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_0$$

Такая запись называется десятичной записью числа n .

Example 4. Двухзначное число умножили на произведение его цифр, в результате чего получилось трехзначное число, состоящее из одинаковых цифр, совпадающих с последней цифрой исходного числа. Найдите исходное число.

Решение: Обозначим исходное двухзначное число за \overline{ab} .

Теперь мы можем переписать условие задачи в виде уравнения:

$$\overline{ab} \cdot (ab) = \overline{bbb} \Leftrightarrow (10a + b) \cdot ab = 100b + 10b + b \Leftrightarrow 10a^2b + ab^2 = 111b$$

Ясно, что при $b = 0$ условие не выполняется. Если $b \neq 0$, то на него можно поделить обе части:

$$10a^2 + ab = 111 \Leftrightarrow ab = 111 - 10a^2$$

Так как $ab > 0$, $10a^2 < 111$, а значит a либо 1, либо 2, либо 3. Рассмотрим случаи по порядку.

- Если $a = 1$, $b = 101$, а это невозможно, так как b — цифра.
- Если $a = 2$, $b = \frac{71}{2}$, а это невозможно, так как b — цифра.
- Если $a = 3$, $b = 7$. Тогда, искомое число — 37.

Ответ: 37.

Example 5. Найдите все натуральные числа, являющиеся степенью двойки, при зачеркивании первой цифры у которых получается число, также являющееся степенью двойки.

Решение: Пусть мы зачеркнули первую цифру числа 2^n , состоящего из $k+1$ цифр. Тогда $10^k < 2^n < 10^{k+1}$, $10^{k-1} < 2^m < 10^k$, а значит $\frac{1}{10^k} < \frac{1}{2^m} < \frac{1}{10^{k-1}}$.

Если перемножить первое и третье неравенства, то получится, что $1 < 2^{n-m} < 10^2 \iff 0 < n-m < 8$.

Так как цифру заканчивали слева, 2^n и 2^m заканчиваются на одну и ту же цифру, а значит:

$$2^n - 2^m \equiv 0 \pmod{10} \Leftrightarrow 2^m(2^{n-m} - 1) \equiv 0 \pmod{10} \Leftrightarrow 2^{n-m} - 1 \equiv 0 \pmod{5} \Leftrightarrow 2^{n-m} \equiv 1 \pmod{5}$$

Рассмотрим таблицу остатков от деления 2^n на 5:

2^n	2	4	8	16	32	64	128	...
Остаток от деления 2^n на 5	2	4	3	1	2	4	3	...

Учитывая при этом $1 < n-m < 8$, $n-m=4 \Leftrightarrow m=n-4$.

Обозначим зачеркнутую цифру числа 2^n за a . Тогда

$$2^n - a \cdot 10^k = 2^{n-4} \Leftrightarrow 2^{n-4} \cdot (2^4 - 1) = a \cdot 10^k \Leftrightarrow 2^{n-4} \cdot 3 \cdot 5 = a \cdot 2^k \cdot 5^k$$

Так как в левой части всего одна пятерка, $k=1$, а значит, искомое число двузначное.

Перебирая все двузначные степени двойки, понимаем, что подходят числа 32 и 64.

Ответ: 32, 64.

Признаки делимости натуральных чисел:

Theorem 6. (Признак делимости на 5)

Число a делится на 5 тогда и только тогда, когда последние цифры десятичной записи числа a — это 0 или 5.

Доказательство. Будет добавлено. □

Theorem 7. (Признак делимости на 3 и на 9)

Число $a \in \mathbb{Z}$ даёт такой же остаток от деления на 3 (и на 9), что и сумма цифр числа a .

Доказательство. Пусть $\overline{a_n a_{n-1} \dots a_2 a_1}$ — десятичная запись данного числа a , то есть

$$a = \overline{a_n a_{n-1} \dots a_2 a_1} = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \dots + a_1 \cdot 10^0$$

Так как $10 \equiv 1 \pmod{3}$, $10^i \equiv 1^i \pmod{3} \equiv 1 \pmod{3} \Rightarrow a_i \cdot 10^{i-1} \equiv a_i \pmod{3}$.

Применим это к каждому слагаемому и сложим все, получим:

$$a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \dots + a_1 \cdot 10^0 \equiv (a_n + a_{n-1} + \dots + a_2 + a_1) \pmod{3}$$

Так как $10 \equiv 1 \pmod{9}$, аналогичное доказательство проходит и для 9. □

Example 6. Два числа отличаются перестановкой цифр. Может ли их разность быть равной 20072008?

Решение:

Как мы помним, сумма цифр числа дает тот же остаток от деления на 9, что и само число. Значит, разность описанных в условии задачи чисел должна делиться на 9, так как у этих чисел одинаковая сумма цифр:

Пусть первое число - a , $a \equiv c \pmod{9}$, второе число b , $b \equiv c \pmod{9}$.

$$\begin{cases} a \equiv c \pmod{9} \\ b \equiv c \pmod{9} \end{cases} \implies a - b \equiv c - c \pmod{9} \iff a - b \equiv 0 \pmod{9} \iff (a - b) : 9.$$

Но, $20072008 \not\equiv 9$, а значит это невозможно.

Theorem 8. (Признак делимости на 2^n (5^n)) Число делится на 2^n (5^n) тогда и только тогда, когда число, составленное из первых n его разрядов (составленное из первых n его цифр), делится на 2^n (5^n).

Доказательство. Будет дописано. □

Theorem 9. (Признак делимости на 11) Число делится на 11 тогда и только тогда, когда разность суммы цифр, стоящих на нечетных местах и суммы цифр, стоящих на четных местах, делится на 11.

Доказательство. Будет дописано. □

Example 7. Рассмотрим число 305792608. $(8 + 6 + 9 + 5 + 3) - (0 + 2 + 7 + 0) = 22 : 11$, а значит $305792608 : 11$.

Example 8. На доске написано такое число: $72x3y$, где x и y - некоторые цифры. Замените звездочки цифрами так, чтобы полученное число делилось на 45.

Решение: Так как число должно делиться на 45, оно должно делиться на 5 и на 9 соответственно. Так как оно делится на 5, его последняя цифра либо 0, либо 5, а значит либо $y = 0$, либо $y = 5$. Так как число делится на 9, сумма его цифр должна делиться на 9. Рассмотрим сумму цифр числа:

$$(7 + 2 + x + 3 + y) : 9 \iff (x + y + 12) : 9$$

$y = 5$: $(x + 17) : 9$, а значит $x = 1$.

$y = 0$ $(x + 12) : 9$, а значит $x = 6$.

1.5 Кольцо классов вычетов.

Напомним, что

Definition 7. Множество R с операциями $<< + >>: R \times R \rightarrow R$ и $<< \cdot >>: R \times R \rightarrow R$ называют кольцом, если $\forall a, b, c \in R$

1. $a + b = b + a$ (коммутативность сложения)
2. $(a + b) + c = a + (b + c)$ (ассоциативность сложения)
3. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ассоциативность умножения)
4. $a \cdot (b + c) = a \cdot b + a \cdot c$ (левая дистрибутивность)
5. $(b + c) \cdot a = b \cdot a + c \cdot a$ (правая дистрибутивность)

Иными словами, R — кольцо, если R — Абелева группа по сложению, полугруппа по умножению и выполнены аксиомы левой и правой дистрибутивности.

Если в кольце R есть нейтральный элемент по умножению, то кольцо R называют кольцом с единицей.

Если умножение в кольце коммутативно, то кольцо называют коммутативным кольцом с единицей.

Definition 8. Множество обратимых (по умножению) элементов кольца R называют мультипликативной группой кольца R и обозначают R^* .

Definition 9. Полем называют коммутативное кольцо с единицей, где каждый ненулевой элемент обратим.

Как мы уже выяснили в предыдущем параграфе, сравнимость по модулю m — отношение эквивалентности, обозначим его за \sim_m .

Definition 10. Фактормножество \mathbb{Z}/\sim_m называют кольцом классов вычетов по модулю m и обозначают $\mathbb{Z}/m\mathbb{Z}$ (детали этого обозначения станут ясны несколько позже).

Remark 3. Заметим, что кольцо классов вычетов можно эквивалентно определить, как множество чисел $\{0, 1, \dots, m-1\}$ (то есть, остатков от деления на m) с операциями сложения и умножения «по модулю» (обозначим их за $\overline{+}$ и $\overline{\cdot}$), то есть

$$\forall x, y \in \mathbb{Z}/m\mathbb{Z} \quad x \overline{+} y = (x + y) \pmod{m}, \quad x \overline{\cdot} y = (x \cdot y) \pmod{m}$$

1.6 НОД и НОК.

Definition 11. Число b называется общим кратным чисел a_1, \dots, a_n , если $\forall i \in \{1, \dots, n\}: a_i \mid b$.

Definition 12. Рассмотрим множество \mathcal{M} всех общих кратных чисел a_1, \dots, a_n . Элемент $\min\{\mathcal{M}\}$ называется наименьшим общим кратным чисел a_1, \dots, a_n и обозначается $\text{lcm}(a_1, \dots, a_n)$ или $[a_1, \dots, a_n]$.

Theorem 10. (Свойства НОК)

1. Любое общее кратное нескольких чисел делится на их наименьшее общее кратное.
2. $\forall a_1, \dots, a_n \in \mathbb{Z} \setminus 0$ выполняется равенство

$$\text{lcm}(a_1, \dots, a_n) = \text{lcm}(\text{lcm}(a_1, \dots, a_{n-1}), a_n)$$

Доказательство. *Допишу.* □

Далее, говоря об общих делителях набора чисел, мы будем подразумевать, что в наборе содержится хотя бы одно ненулевое число.

Definition 13. Наибольшим общим делителем совокупности целых чисел называется наибольшее положительное число, делящее каждое из этих чисел. Наибольший общий делитель набора a_1, \dots, a_n обычно обозначается, как $\text{gcd}(a_1, \dots, a_n)$ или (a_1, \dots, a_n) .

Definition 14. Целые числа a, b называются взаимно простыми, если $\text{gcd}(a, b) = 1$.

Theorem 11. (Свойства НОД)

1. $\forall a, b \in \mathbb{Z} \quad \text{lcm}(a, b) \cdot \text{gcd}(a, b) = a \cdot b$.
2. $a \mid b \cdot c, \text{gcd}(a, b) = 1 \Rightarrow c \mid a$.
3. Наибольший общий делитель нескольких чисел делится на любой их общий делитель.

4. Справедливо равенство

$$\gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$$

Доказательство. Допишу.

☐

Statement 3. $\gcd(a, b) = \gcd(a, a + b) = \gcd(a, a - b)$.

1.7 Алгоритм Евклида. Обобщенный алгоритм Евклида.

В данном параграфе мы будем рассматривать алгоритм поиска наибольшего общего делителя двух натуральных чисел a и b . Ясно, что это можно сделать наивно, перебрав все натуральные числа $d \in \{1, \dots, \min(a, b)\}$ и проверив условия $d \mid a$, $d \mid b$, но это требует большого количества вычислений. Еще в древней греции был придуман алгоритм, решающий данную проблему гораздо лучше.

Lemma 1. Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$.

- Если $b \mid a$, то множество общих делителей чисел a и b совпадает с множеством делителей числа b . В частности, $\gcd(a, b) = b$.
- Предположим, что $a = bq + r$, $0 \leq r \leq |b|$. Тогда множество общих делителей чисел a и b совпадает с множеством общих делителей чисел b и r . В частности, $\gcd(a, b) = \gcd(b, r)$.

Доказательство. Будет дописано.

☐

Таким образом, мы поняли, что при нахождении $\gcd(a, b)$, мы можем заменять a на r , где $r < b$ (то есть, проделывая такие действия несколько раз, мы уменьшаем числа, а значит, в какой-то момент мы закончим).

Theorem 12. *(Алгоритм Евклида)*

Положим $r_0 = a$, $r_1 = b$, r_2, \dots, r_n — последующие делители, то есть

$$\begin{aligned} a &= r_0 = bq_1 + r_2, & 0 \leq r_2 < b \\ b &= r_1 = r_2q_2 + r_3, & 0 \leq r_3 < r_2 \\ r_2 &= r_3q_3 + r_4, & 0 \leq r_4 < r_3 \\ &\dots\dots\dots \\ r_{i-2} &= r_{i-1}q_{i-1} + r_i, & 0 \leq r_i < r_{i-1} \\ &\dots\dots\dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ &r_{n-1} = r_nq_n \end{aligned}$$

То есть, алгоритм останавливается, когда деление проходит без остатка. Алгоритм находит $\gcd(a, b) = r_n$.

Опишем теперь это в качестве алгоритма:

Алгоритм Евклида:

Вход: *Натуральные числа a, b , $b < a$.*

ВЫХОД: $\gcd(a, b)$.

1. Вычислить r — остаток от деления a на b .
2. Если $r = 0$, то $\gcd(a, b) = b$, алгоритм останавливается.
3. Если $r \neq 0$, то пару (a, b) заменяем на пару (b, r) , возвращаемся к первому шагу.

Доказательство. В соответствии с предыдущей леммы, имеем цепочку равенств:

$$\gcd(a, b) = \gcd(b, r_2) = \gcd(r_2, r_3) = \dots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

□

Example 9. Найдём при помощи алгоритма Евклида $\gcd(5160, 16920)$.

$$16920 = 3 \cdot 5160 + 1440$$

$$5160 = 3 \cdot 1440 + 840$$

$$1440 = 1 \cdot 840 + 600$$

$$840 = 1 \cdot 600 + 240$$

$$600 = 2 \cdot 240 + 120$$

$$240 = 2 \cdot 120$$

То есть, $\gcd(5160, 16920) = 120$.

Remark 4. Можно доказать, что количество делений, необходимое для вычисления с помощью алгоритма Евклида наибольшего общего делителя двух натуральных чисел, не превышает пятикратного количества цифр в десятичной записи меньшего из этих двух чисел.

Для нахождения НОД нескольких чисел (больше 2) есть немного более доработанная версия алгоритма Евклида.

Пусть дано множество натуральных чисел a_1, \dots, a_n и необходимо вычислить $\gcd(a_1, \dots, a_n)$. Заметим, что если $a_2 = a_1q + r$, $0 \leq r < |a_1|$, то по 1 множество общих делителей чисел a_1 и a_2 совпадает с множеством общих делителей чисел a_1 и r , а значит

$$\gcd(a_1, \dots, a_n) = \gcd(r, a_1, a_3, \dots, a_n)$$

НОД совокупности чисел не зависит от того, в каком порядке они записаны, а значит, каждое число может быть заменено на остаток от деления на любое другое число из этой совокупности.

Заметим, что такая операция уменьшает сумму чисел в списке (если $a_2 \geq a_1$) всегда, кроме случая, когда список имеет вид $(a_1, 0, \dots, 0)$ (но тогда ясно, что $\gcd(a_1, 0, \dots, 0) = a_1$).

Теперь ясно, как оформить это в качестве алгоритма:

Theorem 13. (Обобщенный алгоритм Евклида)

ВХОД: Совокупность натуральных чисел (a_1, \dots, a_n) .

ВЫХОД: $\gcd(a_1, \dots, a_n)$.

1. Переставим числа в списке (a_1, \dots, a_n) так, чтоб число на первом месте в списке было наименьшим из положительных чисел списка.
2. Если все числа a_2, \dots, a_n равны нулю, то $\gcd(a_1, \dots, a_n) = a_1$, алгоритм останавливается.
3. Заменить в списке (a_2, \dots, a_n) каждое из ненулевых чисел на его остаток от деления на a_1 . Вернуться к первому пункту алгоритма.

1.8 Линейное представление НОД и решение уравнений в целых числах.

Definition 15. Уравнения в целых числах принято называть диофантовыми.

Рассмотрим простейшее линейное диофантово уравнение $ax + by = c$. Такие уравнения могут иметь как бесконечно много решений, так и не иметь решений вообще.

Example 10. Например, рассмотрим два таких уравнения:

- Уравнение $19x + 12y = 1$ имеет бесконечно много решений, множество решений можно описать, как $x = -5 + 12t$, $y = 8 - 19t$, $t \in \mathbb{Z}$.
- Уравнение $2x - 6y = 3$ не имеет решений в целых числах, так как при любых $x, y \in \mathbb{Z}$ левая часть будет четной, а правая часть — нечетной.

Перед тем как переходить к критерию разрешимости таких уравнений мы докажем вспомогательное утверждение.

Theorem 14. (Линейное представление НОД)

Для любых целых a и b существуют целые u и v такие, что

$$au + bv = \gcd(a, b)$$

Доказательство. Для доказательства достаточно проделать «обратный ход» алгоритма Евклида. Развернём равенства из условия 12:

$$r_2 = a - bq_1$$

Подставим это во второе равенство:

$$r_3 = b - r_2q_2 = b - q_2(a - bq_1) = b(1 + q_1q_2) - aq_2$$

Теперь подставим это в третье равенство:

$$r_4 = r_2 - r_3q_3 = a - bq_1 - q_3(b(1 + q_1q_2) - aq_2) = a(1 + q_2q_3) - b(q_1 + q_3 + q_1q_2q_3)$$

Продолжая в том же духе, мы найдём $u, v \in \mathbb{Z}$: $r_n = au + bv = \gcd(a, b)$. □

Remark 5. Отметим, что эта теорема даёт не только существование, но и строит сами числа u и v (что, как мы увидим, важно на практике).

Линейное представление НОД в литературе иногда называют соотношением Безу.

В качестве примера использования этого утверждения докажем лемму, которая понадобится нам в будущем.

Лемма 2. (Лемма Евклида)

Если произведение нескольких сомножителей делится на простое число p , то по крайней мере один из сомножителей делится на простое число p .

Доказательство. Пусть $x \cdot y : p$, но $x \not: p$. Тогда, так как p — простое, $\gcd(x, p) = 1$, а значит, по 14 найдутся такие целые u и v , что

$$x \cdot u + p \cdot v = 1$$

Домножим на y слева и справа, получим

$$(x \cdot y) \cdot u + p \cdot v \cdot y = y$$

Оба слагаемых в левой части делятся на p , а значит, и правая делится на p . □

Theorem 15. Диофантово уравнение $ax+by = c$ разрешимо тогда и только тогда, когда $\gcd(a, b) \mid c$. В случае разрешимости решений всегда бесконечно много. Все они имеют вид

$$x = x_0 + \frac{b}{\gcd(a, b)}t, \quad y = y_0 - \frac{a}{\gcd(a, b)}t$$

где (x_0, y_0) — какое-либо фиксированное решение, а t — произвольное целое число.

Доказательство. *Допишу.* □

Remark 6. Если дети вдруг знают, что такое матрицы, то надо рассказать про диофантовы уравнения n переменных и матричные представления всего это дела.