Теория чисел

Делимость

Определение. Целое число a *делится* на целое число $b \neq 0$, если существует целое число c такое, что $a = bc$. Обозначение. $a \vdots b$ или $b \mid a$.

Свойства делимости.

1. $a \vdots a$, $a \vdots 1$; $0 \vdots a$.

2. $a \vdots b$, $b \vdots c \Rightarrow a \vdots c$.

3. a) $a \vdots c$, $b \vdots c \Rightarrow a \pm b \vdots c$.

b) $a \vdots c$, $a \pm b \vdots c \Rightarrow b \vdots c$.

4. a) $a \vdots b \Rightarrow ac \vdots b$.

b) $a \vdots b \Leftrightarrow ac \vdots bc$.

c) $a \vdots b$, $c \vdots d \Rightarrow ac \vdots bd$. $\square \overset{4b}{\Rightarrow} ac \vdots bc$, $bc \vdots bd \overset{2}{\Rightarrow} ac \vdots bd$ ■

5. a) $a \vdots b$, $a \neq 0 \Rightarrow |a| \geqslant |b|$.

b) $a \vdots b$, $b \vdots a \Rightarrow |a| = |b|$.

6. $a \vdots b \Rightarrow a \vdots a/b$.

Упражнение. Докажите следующее свойства делимости самостоятельно:

4. d) $a \vdots b \Rightarrow a^n \vdots b^n$.

Замечание. 1. Свойство 3b) можно сформулировать следующим образом: “если сумма/разность двух чисел делится на c, то либо они оба делятся на c, либо оба не делятся”.

2. Свойство 6, несмотря на кажущуюся простоту, является достаточно полезным.

Остатки и сравнения

Утверждение. **(деление с остатком)** Для любых целых чисел a и $b \neq 0$ существует и единственная пара целых чисел q и r таких, что $a = bq + r$ и $0 \leqslant r < |b|$. Число q называется *неполным частным*, а число r — *остатком* при делении a на b.

Замечание. 1. Наши ученики **не** пишут $7 : 3 = 2$ (ост.1), они пишут $7 = 3 \cdot 2 + 1$.

2. Делимость является частным случаем деления с остатком.

Доказательство. **Существование.** Будем считать, что $b > 0$. Рассмотрим множество всех целых чисел, больших a/b. Среди них есть наименьшее, обозначим его $q + 1$. Тогда $q \leqslant a/b < q + 1$, $0 \leqslant a - bq < b$. Обозначим $a - bq$ за r. Тогда $a = bq + r$, $0 \leqslant r < b$, что и требовалось.

Единственность. Пусть $a = bq_1 + r_1$ и $a = bq_2 + r_2$. Докажем, что $q_1 = q_2$ и $r_1 = r_2$. Заметим, что $bq_1 + r_1 = bq_2 + r_2$, $b(q_1 - q_2) = r_2 - r_1$. Значит, $r_2 - r_1 \vdots b$, однако из того, что $0 \leqslant r_1$, $r_2 < |b|$ следует, что $|r_2 - r_1| < |b|$. Значит, по свойству 5a) получаем, что $r_2 - r_1 = 0$ и $r_2 = r_1$. Зная это, очевидно получается, что $q_1 = q_2$. ■

Утверждение. Числа a и b дают одинаковые остатки при делении на m тогда и только тогда, когда $a - b \vdots m$.

Доказательство. $\Rightarrow$: $a = mq_1 + r$, $b = mq_2 + r$, значит $a - b = m(q_1 - q_2) \vdots m$.

$\Leftarrow$: Пусть $a = mq_1 + r_1$, $b = mq_2 + r_2$. Тогда $a - b = m(q_1 - q_2) + (r_1 - r_2) \vdots m$. Так как $m(q_1 - q_2) \vdots m$, то и $r_1 - r_2 \vdots m$. Аналогично доказательству предыдущего утверждения тогда $r_1 = r_2$. ■

Определение. Будем говорить, что числа a и b *сравнимы по модулю* m, если $a - b \vdots m$. Обозначение. $a \equiv b \pmod m$ или $a \underset{m}{\equiv} b$.

Свойства сравнений.

0. $a \vdots m \Leftrightarrow a \underset{m}{\equiv} 0$.
1. $a \underset{m}{\equiv} a$.
2. $a \underset{m}{\equiv} b \Rightarrow b \underset{m}{\equiv} a$.
3. $a \underset{m}{\equiv} b,\ b \underset{m}{\equiv} c \Rightarrow a \underset{m}{\equiv} c$.
4. $a \equiv b \pmod m,\ m \vdots n \Rightarrow a \equiv b \pmod n$.
5. a) $a \underset{m}{\equiv} b \Rightarrow a \pm c \underset{m}{\equiv} b \pm c$.
   b) $a \underset{m}{\equiv} b,\ c \underset{m}{\equiv} d \Rightarrow a \pm c \underset{m}{\equiv} b \pm d$.
6. a) $a \underset{m}{\equiv} b \Rightarrow ac \underset{m}{\equiv} bc$.
   b) $a \underset{m}{\equiv} b,\ c \underset{m}{\equiv} d \Rightarrow ac \underset{m}{\equiv} bd$.
   c) $a \underset{m}{\equiv} b \Rightarrow a^n \underset{m}{\equiv} b^n$.
7. $ka \equiv kb \pmod{km} \Rightarrow a \equiv b \pmod m$.
8. $ac \underset{m}{\equiv} bc \not\Rightarrow a \underset{m}{\equiv} b$. Доказательство. $1 \cdot 2 \underset{2}{\equiv} 2 \cdot 2$, но $1 \not\underset{2}{\equiv} 2$ ■

Пример. Найти последнюю цифру числа a) 23^{23}; b) $77^{77^{77}}$.

Признаки делимости и равноостаточности.

Утверждение. Любое натуральное число в десятичной записи дает такой же остаток при делении:
1. на 2 и 5, как и его последняя цифра;
1′. на 2^n и 5^n, как и число, образованное последними n его цифрами;
2. на 3 и 9, как и его сумма цифр;
3. на 11, как и его *знакопеременная сумма* цифр (знакопеременной суммой цифр для числа $\overline{a_s a_{s-1} \dots a_1 a_0}$ называется выражение $\sum_{i=0}^{s} (-1)^i \cdot a_i$).

Замечание. Знание этих признаков порой сильно помогает решить задачу: если в задаче что-то делают с суммой цифр, то надо попробовать решать ее по модулю 9 или 3, если рассматривают несколько последних цифр — по модулю 2^n и/или 5^n и т.д.

Доказательство. Напомним, что

$$\overline{a_s a_{s-1} \dots a_1 a_0} = \sum_{i=0}^{s} a_i \cdot 10^i.$$

Если $i \geqslant n$, то $10^i \vdots 2^n, 5^n$; поэтому $\sum_{i=0}^{s} a_i \cdot 10^i \equiv \sum_{i=0}^{n-1} a_i \cdot 10^i = \overline{a_{n-1} \dots a_0} \pmod{2^n, 5^n}$. Таким образом, 1 и 1′ доказаны.

Для доказательства 2 заметим, что $10 \equiv 1 \pmod{3, 9}$, поэтому $10^i \equiv 1^i = 1 \pmod{3, 9}$. Значит, $\sum_{i=0}^{s} a_i \cdot 10^i \equiv \sum_{i=0}^{s} a_i \pmod{3, 9}$.

Аналогично для 3 заметим, что $10 \equiv -1 \pmod{11}$. Значит, $10^i \equiv (-1)^i \pmod{11}$ и $\sum_{i=0}^{s} a_i \cdot 10^i \equiv \sum_{i=0}^{s} (-1)^i \cdot a_i \pmod{11}$. ■

Наибольший общий делитель (НОД) и алгоритм Евклида

Определение. Число d называется *общим делителем* чисел a и b, если $a \vdots d$, $b \vdots d$.

Число d называется *наибольшим общим делителем (НОД)* чисел a и b, если из всех общих делителей чисел a и b оно является наибольшим (то есть для любого общего делителя d' чисел a и b выполнено неравенство $d' \leqslant d$).

Обозначение. $d = \text{НОД}(a, b)$, $d = \gcd(a, b)$ или просто $d = (a, b)$.

Утверждение. Для любых чисел a и b выполнено равенство $(a, b) = (a - b, b)$.

Доказательство. Для доказательства этого равенства докажем, что множества общих делителей чисел a и b и чисел $a-b$ и b совпадают. Тогда и наибольшие элементы в этих множествах будут совпадать. Для этого нам надо доказать, что любой общий делитель чисел a и b является общим делителем чисел $a - b$ и b и наоборот.

Пусть d — общий делитель чисел a и b. То есть $a \vdots d$ и $b \vdots d$. Тогда по свойствам делимости $a - b \vdots d$ и $b \vdots d$. Значит, d — общий делитель $a - b$ и b. Аналогично, если d — общий делитель $a - b$ и b, то по свойствам делимости тогда d — общий делитель $(a - b) + b = a$ и b. ■

Следствие. Для любых целых чисел a и b выполнено равенство $(a, b) = (r, b)$, где r — остаток при делении a на b.

Давайте теперь предположим, что числа a и b, $a \geqslant b$ — целые неотрицательные, не равные нулю одновременно, и на каждом шаге будем большее число заменять на разность большего и меньшего.

Заметим, что рано или поздно числа перестанут изменяться (почему?), то есть одно из чисел станет равно 0:

$$(a, b) = (a - b, b) = \ldots = (d, 0) = d.$$

Однако такой алгоритм имеет свои недостатки, поэтому рассмотрим другой алгоритм, в котором большее число будем заменять на остаток при делении его на меньшее. Для удобства обозначим $a = r_0$, $b = r_1$. Таким образом,

$$(a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{k-1}, r_k) = \ldots = (r_s, 0) = d,$$

Здесь r_i — остаток при делении r_{i-2} на r_{i-1}, $r_{s+1} = 0$ (почему такой найдется?), $r_s = d$.

Именно этот алгоритм поиска наибольшего общего делителя называется *алгоритм Евклида*, но мы, допуская вольность речи, и первый алгоритм будем так называть.

Следствие. **(линейное представление НОД)** Для любых целых a и b существуют такие целые x и y, что $a \cdot x + b \cdot y = d$, где $d = (a, b)$.

Доказательство. Пусть $(a, b) = (b, c_2) = (c_2, c_3) = \ldots = (c_s, 0) = d$ — алгоритм Евклида для a и b ($a = c_0$, $b = c_1$, $c_s = d$). То есть $c_i = c_{i-2} - q_i c_{i-1}$.

Докажем индукцией по n, что c_n является линейной комбинацией a и b.

База. $n = 0$, $n = 1$: действительно, $c_0 = a = a \cdot 1 + b \cdot 0$, $c_1 = b = a \cdot 0 + b \cdot 1$.

Переход. $n = k - 1$, $n = k \longrightarrow n = k + 1$.

Предположение индукции. $c_{k-1} = a \cdot x_{k-1} + b \cdot y_{k-1}$, $c_k = a \cdot x_k + b \cdot y_k$.

$$\begin{aligned} c_{k+1} &= c_k - q_{k+1} c_{k-1} = a \cdot x_k + b \cdot y_k - a \cdot q_{k+1} x_{k-1} - b \cdot q_{k+1} y_{k-1} = \\ &= a \cdot (x_k - q_{k+1} x_{k-1}) + b \cdot (y_k - q_{k+1} y_{k-1}). \end{aligned}$$

Первое равенство — из алгоритма Евклида, второе — предположение индукции.

Переход доказан. Значит, $d = c_s = a \cdot x + b \cdot y$. ■

Пример. Пусть мы хотим найти наибольший общий делитель и его линейное представление для чисел 13 и 21. Тогда, согласно алгоритму Евклида имеем

$$(21,13) = (13,8) = (8,5) = (5,3) = (3,2) = (2,1) = (1,0) = 1.$$

Доказательство предыдущего утверждения дает какой-то алгоритм нахождения линейного представления НОД, однако мы рассмотрим сейчас немного другой.

В начале мы представим 1 как линейную комбинацию пары $(2,1)$, потом $(3,2)$, ..., потом $(21,13)$. Итак,

$$\begin{aligned} 1 &= 2\cdot 0 + 1\cdot 1 = 2\cdot 0 + (3-2)\cdot 1 = 3\cdot 1 + 2\cdot(-1) = 3\cdot 1 + (5-3)\cdot(-1) = \\ &= 5\cdot(-1) + 3\cdot 2 = 5\cdot(-1) + (8-5)\cdot 2 = 8\cdot 2 + 5\cdot(-3) = \\ &= 8\cdot 2 + (13-8)\cdot(-3) = 13\cdot(-3) + 8\cdot 5 = 13\cdot(-3) + (21-13)\cdot 5 = \\ &= 21\cdot 5 + 13\cdot(-8). \end{aligned}$$

Следствия из существования линейного представления НОД
Основная теорема арифметики

Утверждение. Для любых натуральных чисел a, b и c выполнено равенство $(ac, bc) = c\cdot(a,b)$.

Доказательство. Пусть $(ac,bc) = d$, $(a,b) = d_1$. Нам надо доказать, что $d = cd_1$.

Поскольку $a \vdots d_1$, $b \vdots d_1$, то $ac \vdots cd_1$, $bc \vdots cd_1$, то есть cd_1 — общий делитель чисел ac и bc, поэтому $cd_1 \leqslant d$.

Согласно утверждению о линейном представлении НОД, существуют такие x и y, что $d_1 = ax + by$, умножая это равенство на c, получаем $cd_1 = acx + bcy$. Заметим, что $acx \vdots ac \vdots d$ и $bcy \vdots bc \vdots d$. Значит и $cd_1 = anx + amy \vdots d$, но тогда $cd_1 \geqslant d$.

Значит, $cd_1 \leqslant d$ и $cd_1 \geqslant d$, то есть $cd_1 = d$, что и требовалось. ■

Утверждение. Пусть $a \vdots n$, $a \vdots m$ и $(n,m) = 1$. Тогда $a \vdots nm$.

Доказательство. Так как $(n,m) = 1$, то существуют такие x и y, что $nx + my = 1$. Умножим это равенство на a: $a = anx + amy$.

Заметим, что $anx \vdots an \vdots mn$ и $amy \vdots am \vdots nm$. Значит и $a = anx + amy \vdots nm$. ■

Утверждение. Пусть $ab \vdots n$ и $(b,n) = 1$. Тогда $a \vdots n$.

Доказательство. Так как $(b,n) = 1$, то существуют такие x и y, что $bx + ny = 1$. Умножим это равенство на a: $a = abx + any$.

Заметим, что $abx \vdots ab \vdots n$ и $any \vdots n$. Значит и $a = abx + any \vdots n$. ■

Следствие. (9-ое свойство сравнений) Пусть $an \underset{m}{\equiv} bn$ и $(n,m) = 1$, тогда $a \underset{m}{\equiv} b$.

Доказательство. Действительно, так как $(a-b)n = an - bn \vdots m$ и $(n,m) = 1$, то $a - b \vdots m$. ■

Напомним, что натуральное число p называется *простым*, если у него ровно 2 натуральных делителя: 1 и p. Множество простых чисел иногда обозначается $\mathbb{P}$.

Следствие. **(лемма Евклида)** Если $ab \vdots p$, где $p \in \mathbb{P}$, то или $a \vdots p$, или $b \vdots p$.

Доказательство. Пусть $a \nvdots p$, тогда легко проверить, что $(a,p) = 1$ и $b \vdots p$. ■

Следствие. Если $a_1 \cdot a_2 \cdot \ldots \cdot a_n \vdots p$, где $p \in \mathbb{P}$, то найдется такое $1 \leqslant i \leqslant k$, что $a_i \vdots p$.

Доказательство. Утверждение будет доказывать индукцией по n.

База: $n = 1$ — очевидно.

Переход: $n = k \longrightarrow n = k + 1$.

Предположение индукции. Если $a_1 \cdot a_2 \cdot \ldots \cdot a_k \vdots p$, где $p \in \mathbb{P}$, то найдется такое $1 \leqslant i \leqslant n$, что $a_i \vdots p$.

$a_1 \cdot a_2 \cdot \ldots \cdot a_{k+1} = (a_1 \cdot \ldots \cdot a_k) \cdot a_{k+1} \vdots p$ и или $a_1 a_2 \ldots a_k \vdots p$, или $a_{k+1} \vdots p$.

Если $a_{k+1} \vdots p$, то в качестве i возьмем $k+1$. Если $a_1 a_2 \ldots a_k \vdots p$, то по предположению индукции существует такое i, что $a_i \vdots p$, что и требовалось. Переход доказан. ■

Теорема. **(Основная теорема арифметики)** Любое натуральное число $n > 1$ можно представить в виде произведения простых, причем такое представление единственно с точностью до перестановки множителей.

Доказательство. **Существование.** Среди всех представлений n в виде $x_1 \cdot x_2 \cdot \ldots \cdot x_s$, $x_i > 1$ выберем то, где s — наибольшее. (Почему есть хотя бы одно такое представление?) Заметим, что наибольшее s существует, так как $n = x_1 \cdot x_2 \cdot \ldots \cdot x_s \geqslant 2^s$, поэтому s не может быть сколько угодно большим (так как существует степень двойки, большая n).

Если среди x_1, …, x_s есть не простое (пусть, не умаляя общности, это x_s), то тогда $x_s = x'_s \cdot x_{s+1}$, где x'_s, $x_{s+1} > 1$ и $n = x_1 \cdot \ldots \cdot x_{s-1} \cdot x'_s \cdot x_{s+1}$, противоречие с максимальностью s. Значит, все x_i простые, и мы нашли представление n в виде произведения простых.

Единственность. Рассмотри число n и пусть $p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_t$ — два его разложения на простые множители. Будем сокращать одинаковые множители в левой и правой частях до тех пор, пока это возможно.

Предположим, что по окончании этих действий, в какой-то из частей остались какие-то числа. Тогда, они остались и в другой. То есть, не умаляя общности, $p_1 \cdot \ldots \cdot p_{s'} = q_1 \cdot \ldots \cdot q_{t'}$. Заметим, что левая часть делится на p_1. Тогда, согласно предыдущему следствию, одно из оставшихся q_i также делится на p_1: $q_i \vdots p_1$. Но q_i и p_1 — простые, значит $q_i = p_1$ и мы можем сократить на p_1. Противоречие. Значит, наборы p_1, …, p_s и q_1, …, q_t различаются только перестановкой, что и требовалось. ■

Определение. Представление числа $n > 1$ в виде $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, где $p_i \in \mathbb{P}$, $p_1 < p_2 < \ldots < p_s$, $\alpha_i \in \mathbb{N}$ будем называть *каноническим представлением.*

Замечание. Основная теорема арифметики утверждает, что каноническое представление любого натурального числа $n > 1$ существует и единственно.