Целые числа. Основная теорема арифметики.

Шашков С.

Делимость чисел

Определение 1. Пусть a и b — целые числа, причём $b \neq 0$. Говорят, что a *делится на* b, если существует такое целое число c, что $a = bc$. В этом случае говорят, что a *кратно* числу b; число b называется *делителем* числа a, число c называется *частным* от деления a на b.
Обозначение: $a \vdots b$ (a делится на b) или $b \mid a$ (b делит a).

Разберём простейшие свойства делимости целых чисел. Они понадобятся нам в дальнейшем и будут использоваться повсеместно.

Лемма 1. *Если a, b, c и d — целые числа и если $a \vdots c$ и $b \vdots c$, то $(a \pm b) \vdots c$.*

□ По определению найдутся такие числа x и y, что $a = cx$ и $b = cy$. Тогда $(a \pm b) = c(x \pm y)$. Следовательно, $(a \pm b) \vdots c$. ■

Лемма 2. *Если a, b и c — целые числа и если $a \vdots c$, то $ab \vdots c$.*

□ По определению найдётся такое число x, что $a = cx$. Тогда $ab = bcx = c(bx)$. Следовательно, $ab \vdots c$. ■

Лемма 3. *Если a, b, c и d — целые числа и если $a \vdots c$ и $b \not\vdots c$, то $(a + b) \not\vdots c$.*

□ Допустим обратное, $(a + b) \vdots c$. По определению найдутся такие числа x и z, что $a = cx$ и $(a + b) = cz$. Тогда $b = (a + b) - a = cz - cx = c(z - x)$. Следовательно, $b \vdots c$. Получено противоречие, из которого следует, что $(a + b) \not\vdots c$. ■

Деление с остатком

Определение 2. Пусть a и b — целые числа, $b > 0$. *Разделить* a на b *с остатком* значит найти такие целые числа k (неполное частное) и r (остаток), что $a = kb + r$ и $0 \leqslant r < b$.

Лемма 4. *Пусть a и b — целые числа, $b > 0$. Тогда частное и остаток определены однозначно.*

□ Докажем существование деления с остатком. Если $a \vdots b$, то всё очевидно из определения делимости. Пусть теперь $a \not\vdots b$. Отметим на числовой прямой все числа, кратные b. Они разобьют прямую на отрезки длины b. Точка a лежит на одном из них. Пусть kb — левый конец этого отрезка. Так как $a \not\vdots b$, то $kb > a$. Но по предположению $(k + 1)b < a$. Обозначим $kb - a$ через r. Мы получили, что $0 < r < b$. Следовательно, мы нашли нужные числа.

Докажем теперь, что деление с остатком возможно единственным образом. Рассмотрим два разложения $a = k_1 b + r_1 = k_2 b + r_2$, для которых $0 \leqslant r_1, r_2 < b$. Вычтем одно из другого: $0 = (k_1 - k_2)b + (r_1 - r_2)$. Пусть $k_1 \neq k_2$, тогда $|(k_1 - k_2)b| \geqslant b$. Однако $-b < r_1 - r_2 < b$, то есть $|k_1 - k_2| < b$. Получено противоречие, следовательно $k_1 = k_2$. И, значит, $r_1 = r_2$. ■

Простые числа

Определение 3. Натуральное число $p > 1$ называется *простым,* если оно имеет ровно два натуральных делителя: 1 и p. В противном случае оно называется *составным.*

Лемма 5. *Любое натуральное число, большее 1, либо само простое, либо раскладывается в произведение нескольких простых множителей.*

□ Допустим обратное, тогда найдётся не простое число, не раскладывающееся на несколько простых множителей. Воспользуемся методом математической индукции. Пусть n — наименьшее число с таким свойством. По предположению число n не простое, то есть найдётся делитель a, не равный 1 и p. Пусть $n = ab$ (b найдётся по определению $n \vdots a$). Тогда каждое из чисел a и b раскладывается в произведение нескольких простых множителей. Произведение этих разложений и будет давать разложение для числа $n = ab$. Получено противоречие. ■

Общие делители

Определение 4. Если число d делит числа a и b, то d называется *общим делителем* чисел a и b. Наибольший среди общих делителей чисел a и b называется *наибольшим общим делителем* a и b (обозначение: (a, b)). В том случае, когда $(a, b) = 1$, говорят, что числа a и b *взаимно простые.*

Лемма 6. *Для любых целых чисел a и b, не равных одновременно нулю, существует наибольший общий делитель.*

□ Единица — общий делитель, поэтому общие делители у a и b есть. Осталось доказать, что среди них есть максимальный. По предположению хотя бы одно из чисел не равно нулю. Обозначим модуль этого числа через n. Очевидно, что любой общий натуральный делитель не может быть больше n. Следовательно, общих натуральных делителей от 1 до n штук, а среди них всегда можно выбрать максимальный. ■

Лемма 7. *Пусть a и b — натуральные числа, $a > b$, r — остаток от деления a на b, и x — произвольное целое число. Тогда $(a, b) = (a + xb, b) = (b, r)$.*

□ Из лемм 1 и 2 следует, что для любого x число $a + xb$ делится на (a, b). Поэтому $(a + xb, b) \geqslant (a, b)$. Но в то же время, $a = (a + xb) - xb$, поэтому число a делится на $(a + xb, b)$. Следовательно, $(a + xb, b) \leqslant (a, b)$. Отсюда $(a, b) = (a+xb, b)$. Остаток r можно представить в виде $r = a-qb$, поэтому $(a, b) = (a-qb, b) = (b, r)$. ■

Лемма 8. *Пусть a и b — два фиксированных целых числа. Обозначим через I множество всех чисел, представимых в виде $ax + by$ (x и y — целые числа). Тогда каждое число в I делится на любой общий делитель a и b. Кроме того, любое число в I имеет вид $\alpha(a, b)$, где α — целое (в таких случаях пишут $I = (a, b)\mathbb{Z}$).*

□ Пусть d — наименьшее положительное число в I. Из лемм 1 и 2 следует, что любое число $ax + by$ делится на любой общий делитель a и b. В частности, число d делится на общий делитель (a, b).

Докажем, что любое число в I делится на d. Допустим обратное, пусть $G \in I$ не делится на d. Так как $d, G \in I$, то найдутся числа x_d, y_d и x_G, y_G такие, что $d = ax_d + by_d$ и $G = ax_G + by_G$. Число d минимальное в I, поэтому $G > d$. Поделим G на d с остатком: $G = dq + r$, откуда $r = G - dq = a(x_G - qx_d) + b(y_G - qy_d)$ и число r тоже представляется в виде $ax + by$. Но $0 < r < d$, что противоречит определению числа d.

Остался последний шаг: числа a и b также лежат в I, но с другой стороны все числа в I делятся на d. Следовательно, d — общий делитель a и b, который делится на (a, b). А значит, $d = (a, b)$. Для любого целого α число $\alpha(a, b) = a(\alpha x_d) + b(\alpha y_d)$, поэтому $\alpha(a, b) \in I$. ■

Лемма 9. *Пусть a и b — два фиксированных целых числа. Обозначим через D наименьшее натуральное число, делящееся на любой общий делитель a и b. Тогда $D = (a, b)$.*

□ Рассмотрим множество I из леммы 8. Мы доказали, что (a, b) — минимальное число в I, делится на любой общий делитель a и b, и само по определению является общим делителем. Следовательно, $D \vdots (a, b)$ и $D \leqslant (a, b)$. Значит, $D = (a, b)$. ■

Основная теорема арифметики

Лемма 10. *Пусть c — простое число, и $ac \vdots b$. Тогда либо a, либо c делится на b.*

□ Если $a \vdots b$, то лемма доказана. Предположим теперь, что $a \not\vdots b$. У числа b ровно два натуральных делителя: 1 и b. Следовательно, $(a, b) = 1$. По лемме 8, число $(a, b) = 1$ лежит в I, то есть для некоторых x и y верно: $ax + by = 1$. Домножим это равенство на c: $acx + bcy = c$. Число $acx \vdots b$, число bcy также делится на b. Следовательно, $c \vdots b$. ■

Лемма 11. *Пусть $(a, c) = 1$ и $ab \vdots c$. Тогда $b \vdots c$.*

□ По лемме 8 для некоторых x и y верно: $ax + cy = 1$. Домножим это равенство на b: $abx + cby = b$. Число $abx \vdots c$, число cby также делится на c. Следовательно, $b \vdots c$. ■

Теорема 1. (Основная теорема арифметики) *Докажите, что любое натуральное число можно разложить в произведение простых чисел. Это разложение единственно с точностью до перестановки сомножителей.*

□ По лемме 5 хотя бы одно разложение существует. Докажем, что разложение единственно с точностью до перестановки сомножителей. Единица представляется единственным образом. Допустим теперь, что найдутся числа с различными разложениями. Рассмотрим минимальное число n, для которого было есть хотя бы два различных разложения: $n = p_1 \dots p_k = q_1 \dots q_l$. Если какое p_i равно какому-то q_j, то на них можно сократить, и получится два различных разложения для меньшего числа n/p_i. Следовательно, делители слева и справа попарно различны. Число $q_1 \cdot (q_2 \dots q_l)$ делится на простое число p_1. По лемме 10, либо q_1, либо $(q_2 \dots q_l)$ делится на p_1. Но $q_1 \neq p_1$, поэтому $q_2 \dots q_l \vdots p_1$. Но тогда мы получили два разложения у числа меньшего числа n/p_1: у одного разложения есть простой множитель q_1, а у другого — нет. Противоречие. Значит, разложение единственно с точностью до перестановки сомножителей. ■

Алгоритм Евклида и решение диофантовых уравнений

Пусть a и b — два фиксированных натуральных числа, причём $a > b$. Будем последовательно заменять большее из этих чисел на остаток от деления большего на меньшее. Так как каждый раз хотя бы одно число уменьшается хотя бы на 1, то не более, чем за $a + b$ шагов мы получим пару $(r_n, 0)$. По лемме 7 НОД пары чисел на каждом шагу не меняется, поэтому $(a, b) = (r_n, 0) = r_n$.

Теперь на каждом шагу алгоритма Евклида будем выражать очередной остаток через a и b. Для этого в выражение $r_{k+1} = r_{k-1} - r_k q_k$, будем подставлять уже найденные на предыдущих шагах коэффициенты:

(a, b)	$a = bq_0 + r_1$	$r_1 = a + b(-q_0)$	$r_1 = ax_1 + by_1$
(b, r_1)	$b = r_1 q_1 + r_2$	$r_2 = b - r_1 q_1$	$r_2 = ax_2 + by_2$
(r_1, r_2)	$r_1 = r_2 q_2 + r_3$	$r_3 = r_1 - r_2 q_2$	$r_3 = ax_3 + by_3$
	$\dots$		
(r_{n-2}, r_{n-1})	$r_{n-2} = r_{n-1} q_{n-1} + r_n$	$r_n = r_{n-2} - r_{n-1} q_{n-1}$	$r_n = ax_n + by_n$
(r_{n-1}, r_n)	$r_{n-1} = r_n q_n$	$r_{n+1} = 0$	
$(r_n, 0)$			

Таким образом, мы сможем представить $(a, b) = r_n$ в виде $ax + by$.

Определение 5. Уравнение, которое требуется решить в целых числах, называется *диофантовым. Линейным диофантовым уравнением* называется уравнение вида $ax + by = c$. Для данного линейного уравнения уравнение $ax + by = 0$ называется *однородным.*

Лемма 12. *Диофантово уравнение $ax + by = c$ имеет решение тогда и только тогда, когда $c \vdots (a, b)$.*

□ Рассмотрим множество I из леммы 8. Существование решения уравнения равносильно тому, что $c \in I$. Мы уже знаем из леммы 8, что все числа в I имеют вид $\alpha(a, b)$. Поэтому уравнение $ax + by = c$ имеет решение тогда и только тогда, когда $c \vdots (a, b)$. ■

Лемма 13. *Пусть (x_0, y_0) — одно из решений линейного диофантового уравнения $ax + by = c$. Тогда множество всех решений $\{(x, y)\}$ описывается следующими формулами:*

$$x = x_0 + \frac{bt}{(a, b)}, \quad y = y_0 - \frac{at}{(a, b)}, \qquad t \in \mathbb{Z}. \tag{1}$$

□ Рассмотрим любое решение (x_1, y_1) нашего уравнения. Тогда

$$\begin{aligned} ax_0 + by_0 &= c \\ ax_1 + by_1 &= c \\ a(x_0 - x_1) + b(y_0 - y_1) &= 0 \end{aligned}$$

То есть пара $(x_0 - x_1, y_0 - y_1)$ является решением соответствующего однородного уравнения. Очевидно верно и обратное утверждение, если (α, β) — решение однородного уравнения, то для любого целого t пара $(x_0 + t\alpha, y_0 + t\beta)$ будет решением исходного уравнения. Поэтому нам необходимо найти все решения однородного уравнения $ax + by = 0$. Поделим равенство на (a, b) и перенесём b в левую часть:

$$\frac{a}{(a, b)} x = -\frac{b}{(a, b)} y.$$

Заметим, что $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$. Тогда по лемме 11 $x \vdots \frac{b}{(a,b)}$ и $y \vdots \frac{a}{(a,b)}$. Пусть $x = \alpha \frac{b}{(a,b)}$ и $y = \beta \frac{a}{(a,b)}$. Тогда

$$\frac{a}{(a, b)} \frac{b}{(a, b)} \alpha = -\frac{b}{(a, b)} \frac{a}{(a, b)} \beta.$$

Следовательно, $\alpha = -\beta$, и все решения однородного уравнения имеют вид $\left(t\frac{b}{(a, b)}, -t\frac{a}{(a, b)}\right)$. ■

Теперь понятно, как решить любое линейное диофантово уравнение $ax + by = c$. Сначала нужно найти (a, b). Если $c \not\vdots (a, b)$, то решений нет. Иначе с помощью алгоритма Евклида ищем такие x, y, что $ax + by = (a, b)$. Тогда пара $(x_0, y_0) = \left(\frac{c}{(a, b)} x, \frac{c}{(a, b)} y\right)$ является одним из решений уравнения. Далее все решения даются формулой 1.