

**Алгоритм Евклида.
Линейные диофантовы
уравнения с двумя
неизвестными**

1. Целые числа. Делимость с остатком

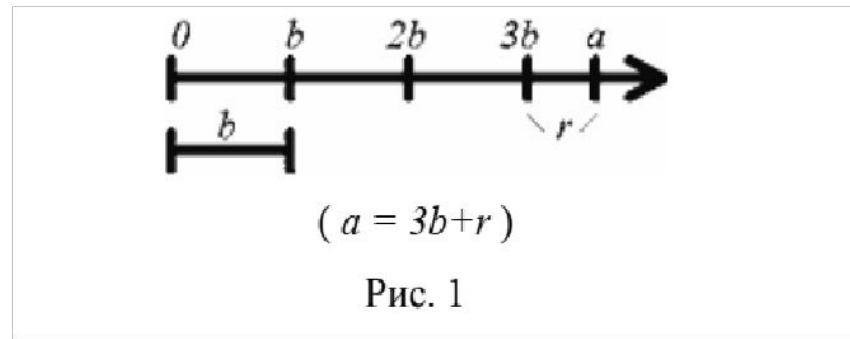
Элементарная теория чисел имеет дело с натуральными числами $1, 2, 3, \dots$ (множество натуральных чисел обозначается символом \mathbb{N}) и целыми числами $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$ (множество целых чисел обозначается символом \mathbb{Z}).

Определение. Пусть $a, b \in \mathbb{Z}$. Число a делится на число b , если найдется такое число $q \in \mathbb{Z}$, что $a = qb$. Синонимы: a кратно b , b - делитель a . Запись: $a \mathbb{Z} b$ или $b | a$.

Пусть $a_1 + a_2 + \dots + a_n = c_1 + c_2 + \dots + c_k$ - равенство сумм целых чисел. Если все слагаемые в этом равенстве, кроме одного, кратны b , то и оставшееся слагаемое обязано быть кратным b .

Теорема. Для данного целого отличного от нуля числа b , всякое целое число a единственным образом представимо в виде $a = bq + r$, где $0 \leq r < |b|$.

Доказательство. Ясно, что одно представление числа a равенством $a = bq + r$ мы получим, если возьмем bq равным наибольшему кратному числа b , не превосходящему a (см. Рис. 1).



Тогда, очевидно, $0 \leq r < |b|$. Докажем единственность такого представления. Пусть $a = bq + r$ и $a = bq_1 + r_1$ - два таких представления. Значит, $0 = a - a = b(q - q_1) + (r - r_1)$. Здесь 0 делится на b ; $b(q - q_1)$ делится на b , следовательно, $(r - r_1)$ обязано делиться на b . Так как $0 \leq r < |b|$ и $0 \leq r_1 < |b|$, то $r - r_1 < b$ и $r - r_1$ делится на b , значит, $r - r_1$ равно нулю, а, значит, и $q - q_1$ равно нулю, т.е. два таких представления совпадают. ■

2. Наибольший общий делитель

Определение. Число $d \in \mathbb{N}$, делящее одновременно числа $a, b, c, \dots, k \in \mathbb{N}$, называется общим делителем этих чисел. Наибольшее d с таким свойством называется наибольшим общим делителем. Обозначение: $d = (a, b, c, \dots, k)$.

Теорема (Свойство 1). Если $(a, b) = d$, то найдутся такие целые числа u и v , что $d = au + bv$.

Доказательство. Рассмотрим множество $P = \{au + bv \mid u, v \in \mathbb{Z}\}$. Очевидно, что $P \subseteq \mathbb{Z}$, а (можно проверить, что P - идеал в \mathbb{Z}). Очевидно, что $a, b, 0 \in P$. Пусть $x, y \in P$ и $y \neq 0$. Тогда остаток от деления x на y принадлежит P . Действительно:

$$x = yq + r, 0 \leq r < y,$$

$$r = x - yq = (au_1 + bv_1) - (au_2 + bv_2)q = a(u_1 - u_2q) + b(v_1 - v_2q) \in P.$$

Пусть $d \in P$ - наименьшее положительное число из P . Тогда a делится на d . В самом деле, $a = dq + r_1, 0 \leq r_1 < d, a \in P, d \in P$, значит, $r_1 \in P$, следовательно, $r_1 = 0$. Аналогичными рассуждениями получается, что b делится на d , значит, d - общий делитель a на b .

Далее, раз $d \in P$, то $d = au_0 + bv_0$. Если теперь d_1 - общий делитель a и b , то $d_1 \mid (au_0 + bv_0)$, т.е. $d_1 \mid d$. Значит, $d \geq d_1$ и d - наибольший общий делитель. ■

Теорема (свойство 2). Для любых целых чисел a и k , справедливо:
 $(a, ka) = a$; $(1, a) = 1$.

Теорема (свойство 3). Если $a = bq + c$, то совокупность общих делителей a и b совпадает с совокупностью общих делителей b и c , в частности, $(a, b) = (b, c)$.

Доказательство. Пусть $d \mid a$, $d \mid b$, тогда $d \mid c$. Пусть $d \mid c$, $d \mid b$, тогда $d \mid a$. ■

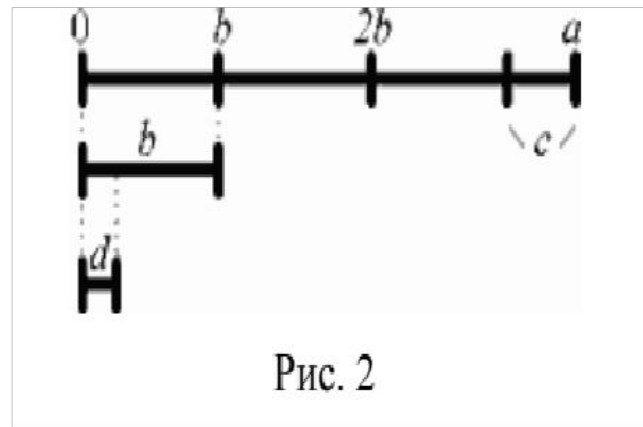


Рис. 2

Если d целое число раз укладывается в a на b , то, очевидно, что d обязано целое число раз уложиться и в c .

Теорема (свойство 4). Пусть a, b и m - произвольные целые числа. Тогда $(am, bm) = m(a, b)$.

Доказательство. Если d - наибольший общий делитель чисел a и b , $dm | am$ и $dm | bm$, т.е. dm - делитель am и bm . Покажем, что dm - наибольший общий делитель этих чисел. Поскольку d - наибольший общий делитель чисел a и b , то согласно свойству 1, для некоторых целых чисел u и v выполнено равенство $d = au + bv$. Умножив это равенство на m , получим равенство: $dm = am u + bm v$.

Видно, что если некоторое число s делит одновременно am и bm , то s обязано делить и dm , т.е. $s \leq dm$, следовательно, dm - наибольший общий делитель. ■

Теорема (свойство 5). Пусть s - делитель a и b . Тогда: $\left(\frac{a}{s}, \frac{b}{s}\right) = \frac{(a, b)}{s}$.

Теорема (свойство 6). Если $(a, b) = 1$, то $(ac, b) = (c, b)$.

Доказательство. Пусть $(c, b) = d$. Имеем: $d | b$, $d | c$, следовательно, $d | ac$, т.е. d - делитель ac и b . Пусть теперь $(ac, b) = s$. Имеем: $s | b$, $s | ac$, s - делитель b , т.е. либо $s = 1$, либо s не делит a . Это означает, что $s | c$, значит $s | d$. Итак, d и s делятся друг на друга, т.е. $d = s$. ■

3. *Взаимно простые числа*

Определение. Целые числа a и b называются взаимно простыми, если $(a, b) = 1$.

Вспоминая свойство 1 из предыдущего пункта, можно заметить, что два числа a и b являются взаимно простыми тогда и только тогда, когда найдутся целые числа u и v такие, что $au + bv = 1$.

4. Алгоритм Евклида

Алгоритмом Евклида мы называем совокупность последовательных действий, позволяющих найти наибольший общий делитель двух натуральных чисел.

Теорема 7. Если $a = bq + c$, то $(a, b) = (b, c)$.

Для отыскания (a, b) при $a > b$ применяется алгоритм Евклида, основанный на теореме 7.

Алгоритм Евклида состоит в получении равенств вида:

$a = bq_0 + r_1$	$0 < r_1 < b$
$b = r_1q_1 + r_2$	$0 < r_2 < r_1$
$r = r_2q_2 + r_3$	$0 < r_3 < r_2$
.....
$r_{n-2} = r_{n-1}q_{n-1} + r_n$	$0 < r_n < r_{n-1}$
$r_{n-1} = r_nq_n$	

Тогда $(a, b) = r_n$ - последнему не равному нулю остатку алгоритма Евклида.

Пример 1. Найти с помощью алгоритма Евклида $(2004, 1941)$.

Решение. $2004 = 1941 \cdot 1 + 63$

$$1941 = 63 \cdot 30 + 51$$

$$63 = 51 \cdot 1 + 12$$

$$51 = 12 \cdot 4 + 3$$

$$12 = 3 \cdot 4$$

Итак, $(2004, 1941) = 3$.

Пример 2. Найти с помощью алгоритма Евклида $(525, 231)$.

Решение. Ниже приводится запись деления уголком, и каждый раз то, что было в уголке, т.е. делитель, приписывается к остатку от деления с левой стороны, а остаток, как новый делитель, берется в уголок:

Запись того же самого в виде цепочки равенств:

$$525 = 231 \cdot 2 + 63$$

$$231 = 63 \cdot 3 + 42$$

$$63 = 42 \cdot 1 + 21$$

$$42 = 21 \cdot 2$$

Таким образом, $(525, 231) = 21$. Линейное представление наибольшего общего делителя:

$$\begin{aligned} 21 &= 63 - 42 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 = \\ &= 525 - 231 \cdot 2 - (231 - (525 - 231 \cdot 2) \cdot 3) = \\ &= 525 \cdot 4 - 231 \cdot 9, \end{aligned}$$

следовательно, $u = 4$ и $v = -9$.

4. Линейные диофантовы уравнения с двумя неизвестными

Диофантовыми называются уравнения вида

$$ax + by = c,$$

где a, b, c – целые числа. При этом решения ищутся в целых числах.

Пусть требуется решить линейное диофантово уравнение:

$$ax + by = c,$$

где $a, b, c \in \mathbb{Z}$; a и b - не нули.

Пусть $(a, b) = d$. Тогда $a = a_1d$; $b = b_1d$ и уравнение выглядит так:

$$a_1d \cdot x + b_1d \cdot y = c, \text{ т.е. } d(a_1x + b_1y) = c.$$

Ясно, у такого уравнения решение существует только тогда, когда $d \mid c$.

Пусть d делит c . Поделим обе части уравнения на d и всюду далее будем считать $(a, b) = 1$.

Случай 1. Пусть $c = 0$, уравнение имеет вид $ax + by = 0$ - «однородное диофантово уравнение». Далее, получаем $x = -\frac{b}{a}y$.

Так как x должен быть целым числом, то $y = at$, где t - произвольное целое число (параметр). Значит $x = -bt$ и решениями однородного диофантова уравнения $ax + by = 0$ являются все пары вида $\{-bt, at\}$, где $t = 0; \pm 1; \pm 2; \dots$. Множество всех таких пар называется общим решением однородного диофантова уравнения, любая же конкретная пара из этого множества называется частным решением.

Случай 2. Пусть $c \neq 0$. Этот случай закрывается следующей теоремой.

Теорема. Пусть $(a,b)=1$, $\{x_0, y_0\}$ - частное решение диофантова уравнения $ax + by = c$. Тогда его общее решение задается формулами:

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at. \end{cases}$$

Доказательство. То, что правые части указанных в формулировке теоремы равенств действительно являются решениями, проверяется их непосредственной подстановкой в исходное уравнение. Покажем, что любое решение уравнения $ax + by = c$ имеет именно такой вид, какой указан в формулировке теоремы. Пусть $\{x^*, y^*\}$ - какое-нибудь решение уравнения $ax + by = c$. Тогда $ax^* + by^* = c$, но ведь и $ax_0 + by_0 = c$. Вычтем из первого равенства второе и получим:

$$a(x^* - x_0) + b(y^* - y_0) = 0$$

- однородное уравнение. Далее, воспользуемся случаем 1, пишем сразу общее решение: $x^* - x_0 = -bt$, $y^* - y_0 = at$, откуда получаем:

$$\begin{cases} x^* = x_0 - bt \\ y^* = y_0 + at. \end{cases}$$

Пример 3. Решить в целых числах уравнение $7x + 12y = 43$.

Решение. Воспользуемся алгоритмом Евклида:

$$12 = 7 \cdot 1 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2$$

Значит, наибольший общий делитель 7 и 12 равен 1, а его линейное выражение следующее:

$$1 = 5 - 2 \cdot 2 = 5 - (7 - 5) \cdot 2 = (12 - 7) - (7 - (12 - 7) \cdot 2) = 12 \cdot 3 + 7 \cdot (-5),$$

т.е. $u = -5$, $v = 3$. Частное решение:

$$x_0 = uc = -5 \cdot 43 = -215$$

$$y_0 = vc = 3 \cdot 43 = 129.$$

Общее решение диофантового уравнения:

$$x = -215 - 12t$$

$$y = 129 + 7t.$$

легко видеть, что при $t = -18$, получаются $x = 1$, $y = 3$.