1 Целые числа

Множество целых чисел обозначим Z.

$$Z = \{0; \pm 1; \pm 2; \ldots; \pm n; \ldots\}$$

Говоря "число", мы подразумеваем целое число.

Говорят, что число $a \in Z$ **делит** число $b \in Z$, если найдется такое число $k \in Z$, что $b = a \cdot k$, говорят также, что b **делится** на a. Обозначение: $a \mid b$. a называется также **делителем** b.

Пример: $4 \mid 16,\ 4 \not\mid 15$

Число p называется **простым**, если его делителями являются **только** числа $\pm 1, \pm p$, т.е.:

$$d \mid p \Rightarrow d = \pm 1 \text{ или } d = \pm p$$

Пример: $2, 3, 5, 7$ -- простые числа, $4, 6, 9$ -- нет.

Основная теорема арифметики: любое число разлагается в произведение простых множителей, причем это разложение однозначно с точностью до порядка множителей:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ \alpha_i > 0$$

Пример: $36 = 2^2 \cdot 3^2$

Наибольший общий делитель (НОД) двух чисел a и b -- это такое число k, которое делит оба числа a и b и делится на любое другое число, которое делит a и b. Обозначение: НОД(a, b) или просто (a, b).

Числа a, b называются **взаимно простыми**, если $(a, b) = 1$

НОД всегда существует и определен однозначно с точностью до знака.

Разложение на простые множители для НОД получится из разложений для a и b, если взять простые множители входящие в оба разложения с минимальной степенью вхождения.

Пример: $(12, 18) = (2^2 \cdot 3, 3^2 \cdot 2) = 2 \cdot 3 = 6,\ (15, 14) = (3 \cdot 5, 2 \cdot 7) = 1$

Наименьшее общее кратное (НОК) двух чисел a и b -- это такое число k, которое делится на оба числа a и b и делит любое другое число, которое делится на a и b. Обозначение: НОК(a, b) или просто $[a, b]$.

Разложение на простые множители для НОК получится из разложений для a и b, если взять простые множители входящие хотя бы в одно разложение с максимальной степенью вхождения.

Пример: $[12, 18] = (2^2 \cdot 3, 3^2 \cdot 2) = 2^2 \cdot 3^2 = 36,\ [15, 14] = (3 \cdot 5, 2 \cdot 7) = 3 \cdot 5 \cdot 2 \cdot 7 = 210$

Имеет место формула:

$$a \cdot b = (a,\ b) \cdot [a,\ b]$$

Для любых чисел a и b найдутся однозначно определенные числа q и r, такие что

$$a = b \cdot q + r,\ |r| < |b|$$

Нахождение q и r осуществляется с помощью "деления столбиком" чисел.

Пример: $19 = 3 \cdot 6 + 1$. При делении 19 на 3 в остатке получим 1.

1.1 Алгоритм Евклида нахождения НОД(a, b)

Найдутся однозначно определенные числа q_i и r_i такие что:

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ \ldots &\quad \ldots \quad \ldots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n \\ r_{n-1} &= r_n \cdot q_{n+1} \end{aligned} \tag{1}$$

последний ненулевой остаток (в данном случае r_n) и есть НОД.

Для любых двух чисел a и b найдутся числа u и v, такие что $a \cdot u + b \cdot v = (a, b)$. Для их нахождения нужно выразить r_1 через a и b в первой из формул (1), подставить во вторую, потом выразить r_2 через a и b во второй из формул (1) и подставить выражения для r_1 и r_2 в третью формулу и т. д., пока не получим выражения для r_n.

Числа u и v определены неоднозначно. Для другой пары $u',\ v'$ имеем $a \cdot u' + b \cdot v' = (a, b)$ и, следовательно, $(u - u')a = (v' - v)b = t[a,\ b]$ для некоторого t. Откуда:

$$u' = u - \frac{t[a,\ b]}{a} = u - \frac{t \cdot b}{(a,\ b)}$$

Анологичное выражение можно написать для v'. Эти формулы позволяют выбрать наименьшие значения для u и v.

НОД n чисел $a_1, \ldots, a_n$ это такое число d, которое:

1. делит все числа $a_1, \ldots, a_n$
2. делится на любое другое число, обладающее свойством 1

Обозначение: $d = (a_1, \ldots, a_n)$

Имеет место формула:

$$(a_1, \ldots, a_n) = (\ldots((a_1, a_2), a_3) \ldots a_n)$$

т.е. НОД можно вычислять последовательно. Сперва НОД первых двух чисел, потом НОД этого НОД с третьим числом, и т.д.

Сформулировать аналогичные результаты для НОК

2 Примеры

2.1 Нахождение разложения для НОД(a, b)

Пусть

$$\begin{aligned} a &= 116 \\ b &= 36 \end{aligned}$$

Найдем (a, b):

$$\begin{aligned} 116 &= 36 \cdot 3 + 8 \\ 36 &= 8 \cdot 4 + 4 \\ 8 &= 4 \cdot 2 \end{aligned}$$

Откуда $(a, b) = 4$ (последний ненулевой остаток)

Получим из последней выкладки выражение для НОД:

$$\begin{aligned} a &= 3b + 8 \Rightarrow a - 3b = 8 \\ b &= (a - 3b) \cdot 4 + 4 \Rightarrow b - (a - 3b) \cdot 4 = 4 \end{aligned}$$

Или:

$$13b - 4a = 4$$

Итак $u = -4,\ v = 13$.

Другие значения: $u = -4 + \frac{36}{4} = 5,\ v = 13 - \frac{116}{4} = -16$ (**объяснить!**)

2.2 Нахождение разложения для НОД(a, b, c)

Пусть

$$\begin{aligned} a &= 116 \\ b &= 36 \\ c &= 102 \end{aligned}$$

Так как $(a, b) = 4$, то $(a, b, c) = ((a, b), c) = (4, 102)$
Далее:

$$\begin{aligned} 102 &= 4 \cdot 25 + 2 \\ 4 &= 2 \cdot 2 \end{aligned}$$

Итак: $(a, b, c) = 2$
Имеем:

$$c = 4 \cdot 25 + 2 \Rightarrow c = (13b - 4a) \cdot 25 + 2$$

Откуда:

$$2 = 100a - 325b + c$$

Итак $u_1 = 100,\ u_2 = -325,\ u_3 = 1$