Оглавление

Лекция 4

29.09.2023

0.1 Алгоритм Евклида

Лемма 1. $\forall a, b, k$НОД(a, b) = НОД(a + kb, b)

Доказательство. M_1 - мнодество общих делителей a, b
M_2 - множество общих делителей a + kb, b
докажем, что $M_1 = M_2$

1. $M_1 \subset M_2$

   $\exists d \in M_1 \Rightarrow a \vdots d, b \vdots d \Rightarrow kb \vdots d \Rightarrow a + kb \vdots d \Rightarrow d - \text{общий делитель}$

2. $M_2 \subset M_1$

   $\exists d \in M_2 \Rightarrow a + kb \vdots d, b \vdots d \Rightarrow a = (a + kb) - kb \vdots d \Rightarrow d \in M_1$ Q.E.D.

$\square$

Теорема 1. (Алгоритм Евклида) для любых a, b алг. Евклида заканчивается за конечное число шагов, и его резуьтат равен НОД(a, b)

Доказательство.

1. Алгоритм заканвивается:

   $a \geq b > r_1 > r_2 > \ldots > 0, \text{где} r_i - \text{остаток}$

2. Результат равен НОД(a, b)

   если $a \vdots b$, то НОД(a, b) = b

   если $a \not\vdots b$, то итог алгоритма не меняет НОД:

   НОД(a, b) = НОД(a, - bq, b) Q.E.D.

$\square$

0.2 Линейное представление НОД

Теорема 2. (Линейное представление НОД) Пусть $a, b \in \mathbb{N}$

1. $\exists x, y \in \mathbb{Z} : ax + by = (a, b)$
2. Пусть k - общий делитель a, b. Тогда $(a, b) \vdots k$

Доказательство. Положим $M = \{au + bv : u, v \in \mathbb{Z}\}$

Обозначним через d наименьший положительный элемент M через x, y - такие числа, что $d = ax + by$

Докажем:

1. d - общий делитель a и b
2. если k - общий делитель a и b, то $k \vdots d$

Докажем, что $a, b \vdots d$
Пусть $a \not\vdots d$. Делим a на d с остатком:
$a = dq + r, 0 < r < d$
$r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy) \in M$
$0 < r < d, r \in M \Rightarrow d-$не наименьший положительный, противоречие
аналогично, $b \vdots d$
Докажем, что если k - общий делитель a и b, то $k \vdots d$:
$d = ax + by$
$a \vdots k \Rightarrow ax \vdots k \wedge b \vdots k \Rightarrow by \vdots k \Rightarrow ax + by \vdots k$ Q.E.D.

□

Замечание. Линейное представление можно найти с помощью алгоритма Евклида

Замечание. Уравнение $ax + by = c$ имеет решения $\Leftrightarrow c \vdots (a, b)$

0.3 Простые числа

Определение 1. числа a и b - взаимно простые, если $(a, b) = 1$

Определение 2. Числа $a_1, a_2, \ldots, a_k$ называются взаимно простыми в совокупности, если $(a_1, a_2, \ldots, a_k) = 1$

Определение 3. Числа $a_1, a_2, \ldots, a_k$ называются попарно взаимно промтыми, если любые два из них - взаимно простые

Пример. 6, 10, 15 - взаимно простые в совокупности, но не попарно

Лемма 2. Числа a и b взаимно просты $\Leftrightarrow \exists x, y : ax + by = 1$

Доказательство. $\Rightarrow$: по теореме о линейном представлении НОД
$\Leftarrow$: Пусть $d = (a, b), d \neq 1$. Тогда $ax + by \,\vdots\, d, 1 \not\vdots\, d$. противоречие, Q.E.D. □

Свойство. (взаимная простота с произведением) Если каждое из чисел $a_1, a_2, \ldots, a_k$ взаимно просты с b, то $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ тоже взаимно просто с b

Доказательство. (Индукция) База k = 2. Докажем, что если a_1, a_2 взаимно просты с b, то $a_1 a_2$ взаимно просты с b. По лемме (2): $\exists x_1, y_1, x_2, y_2 :$ $a_1 x_1 + b y_1 = 1, a_2 x_2 + b y_2 = 1$. Перемножим:
$(a_1 a_2)(x_1 x_2) + b(a_1 x_1 y_2 + y_1 a_2 x_2 + b y_1 y_2) = 1$
Получили линейное представление 1 через $a_1 a_2$ и d $\Rightarrow a_1 a_2, b$ - взаимно просты
Переход $k \to k + 1$
$\underline{a_1, a_2, \ldots, a_k}, a_{k+1}$ взаимно просты с b
$a_1, a_2, \ldots, a_k$ взаимно просты с b $\overset{\text{ИП для k}}{\Rightarrow}$ $a_1 \cdots a_2 \cdot \ldots \cdot a_k$ □

Свойство.
1. Пусть $ab \,\vdots\, c$, a и c взаимно просты. Тогда $a \,\vdots\, c$
2. Пусть $a \,\vdots\, b, a \,\vdots\, c$, b и c взаимно просты. Тогда $a \,\vdots\, bc$

Доказательство.
1. $\exists x, y : ax + cy = 1$. Умножим на b:
   $(ab)x + bcy = b$
   $\vdots c$
   $ab \,\vdots\, c$ – по условию $\Rightarrow abx \,\vdots\, c \wedge bcy \,\vdots\!\Rightarrow b \,\vdots\, c$
2. $a = bk, a = cm, \exists x, y : bx + cy = 1$. Умножим на k:
   $k = \underbrace{bk}_{a}x + cyk = ax + cyk = cmx + cyk \,\vdots\, c \Rightarrow k \,\vdots\, c$
   $k = cz, a = bk = (bc)z \,\vdots\, bc$ Q.E.D.

□

Свойство. Число p называется простым, если $p > 1$ и у p нет натуральных делителей, кроме 1 и p

Свойство. Число n называется составным, если n > 1 и n - не простое

Обозначение. множество простых чисел - P

Свойство. число a составное $\Leftrightarrow \exists b, c : a = bd, 1 < b, c < a$

Доказательство.
1. $\Rightarrow$: $a \notin P$, тогда у a есть делитель $b : b \neq 1, b \neq a \Rightarrow 1 < b < a$
   $\exists c : a = bc, c = \frac{a}{b}, \frac{a}{a} < c < \frac{a}{1}$
2. $\Leftarrow$: $a = bc, 1 < b < a \Rightarrow$ у a есть делитель $\neq 1, \neq a \Rightarrow a \notin P$ Q.E.D.

□

Лемма 3. У любого натурального числа, большего 1, есть хотя бы один протой делитель

Доказательство. (Индукция)

1. База n = 2, делителя 2
2. Переход. Предположим, что $n > 2, \forall k : 1 < k < n$ у k есть простой делитель. Докажем, что у n есть простой делитель
   (a) случай 1: n - простое $\Rightarrow n -$ простой делитель n
   (b) случай 2: n - составное $\Rightarrow$ у n есть делитель, $n = km, 1 < k, m < n$

   По индукции: $\exists p \in P : k \vdots p \Rightarrow n \vdots p$ Q.E.D.

□

Теорема 3. (Евклида) Множество простых чисел бесконечно

Доказательство. Пусть $p_1, p_2, \dots, p_k$ - все простые числа

Положим $N = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$, Тогда по лемме у N есть некий простой делитель, $N p_1, p_2, \dots, p_k$, т.к. $\Rightarrow 1 \vdots p_i$ - невозможно

Значит N - простое. Противоречие. Q.E.D.

□

Теорема 4. (Дирихле) Пусть (a, m) = 1. Тогда $\exists$ бесконечно много простых чисел вида $a + km$ (Доказательство слишком сложное)

0.4 Основная теорема арифметики

Теорема 5. Любое натуральное число, большее 1 можно представить в виде произведения простых чисел. С точностью представления до порядка сравнения.

Доказательство.

1. Существование: Индукция
   (a) База n = 2, 2 = 2 - разложение
   (b) Переход: Предположим, что все числа, меньшие n, раскладываются в произведение простых. Докажем для n.
      i. случай 1: n - простое, n = n - разложение
      ii. случай 2: n - составное, тогда $\exists p : p \in P, n \vdots p, 1 < p < n$
      $1 < \frac{n}{p} < n$ По инд. предположению $\frac{n}{p}$ можно разложить: $\frac{n}{p} = p_1 p_2 \cdot \dots \cdot p_k \Rightarrow n = p \cdot p_1 p_2 \cdot \dots \cdot p_k \Rightarrow$ существование доказано.

2. Единственность.

   Пусть n - наименьшее число, которое можно разложить двумя способами: $n = p_1 \cdot \ldots \cdot p_k, n = q_1 \cdot \ldots \cdot q_m$ Если $p_i = q_j$ для неких i, j, то $\frac{n}{p_i} = \frac{n}{q_j}$ - тоже раскладывается двумя способами, n - не минимальное, <u>противоречие</u> $\Rightarrow \forall i, j : p_i \neq q_j \Rightarrow p_i, q_j$ - взаимно простые

   Далее: $q_1 \neq p_1, q_2 \neq p_1, \ldots, q_m \neq p_1 \Rightarrow q_1, p_1$ – взаимно просты,

   q_2, p_1 – взаимно просты,

   $\vdots$

   q_m, p_1 – взаимно просты,

   Значит, $n = q_1 \cdot \ldots \cdot q_m \not\vdots\, p_1$, при этом $n = p_1 \cdot \ldots \cdot p_k \,\vdots\, p_1$ - противоречие, единственность доказана.

Q.E.D. $\square$

Свойство. Пусть $p \in P, a_1, \ldots a_k \,\vdots\, p$, тогда для некотрого $a_i \,\vdots\, p$

Пусть не делится, тогда:

$a_1 = p_{11} \cdot p_{12} \cdot \ldots$

$a_2 = p_{21} \cdot p_{22} \cdot \ldots$

$\vdots$

Получаем: $\underbrace{a_1 \cdot a_2 \cdot \ldots a_k}_{\text{делится на p}} = \underbrace{p_{11} \cdot p_{12} \ldots}_{\text{не делится на p}} \Rightarrow$ противоречие. Q.E.D.