Конспект Шорохова Сергея
Если нашли опечатку/ошибку - пишите @le9endwp

Теория чисел и основные алгебраические структуры

- $\mathbb{Z}$ - целые числа $+ - \cdot >$
- $\mathbb{N}$ - натуральные числа
- $\mathbb{R}$ - вещественные числа

Аксиома индукции. $A \subset \mathbb{N}; A \neq \varnothing \Rightarrow$ в A есть наименьший элемент
Th. о делении с остатком
$$\begin{cases} \text{a, b} \in \mathbb{Z} \\ \text{b} \neq 0 \end{cases} \Rightarrow \exists! q, r \in \mathbb{Z} : a = b \cdot q + r, 0 \leq r < |b|$$

Доказательство

- Существование
  1. $a > 0, b > 0$ fix b
     Пусть не так, есть плохие a (множество плохих $a \neq \varnothing$)
     Пусть a_0 - наименьшее плохое, значит $a_0 - 1$ - хорошее, можно разделить с остатком
     $a_0 - 1 = b \cdot q + r, 0 \leq r < b$, тогда
     $a_0 = (b \cdot q + r) + 1, r + 1 < b$
     $a_0 = b \cdot (q + 1)$, т.е. a_0 - хорошее
  2. $a < 0, b > 0$
     $-a = b \cdot q + r, 0 \leq r < b$
     $a = -b \cdot q - r$
     2.1. $r = 0$
          $a = b \cdot (-q) + 0$
     2.2. $r > 0$
          $a = b \cdot (-q) - b + b - r = b \cdot (-q - 1) + b - r, 0 < r < b \Rightarrow 0 < b - r < b$
  3. $b < 0, -b > 0$
     $a = -b \cdot q + r = b \cdot (-q) + r, 0 \leq r < b$
- Единственность
  Пусть q, q', r, r'
  $a = b \cdot q + r$
  $a = b \cdot q' + r'$
  $a - a = b \cdot q + r - b \cdot q' - r'$
  $0 = b \cdot (q - q') + (r - r')$
  $r' - r = b \cdot (q - q'), q \neq q', |q - q'| \geq 1$
  $|b \cdot (q - q')| \geq |b|$
  $r', r \in [0; |b| - 1]$
  $|r - r'| < |b| - 1$ Противоречие $\Rightarrow q = q', r = r'$

Def. $a, b \in \mathbb{Z}, a \,\vdots\, b (b|a)$, если $\exists c \in \mathbb{Z} : a = bc$

Rem. $0 \,\vdots\, 0$ $\forall x \in \mathbb{Z} 0 = 0 \cdot x$
Основные свойства делимости:

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

2. $a \vdots 1$

3. $a, b \vdots c \Rightarrow a + b \vdots c$

4. $a, k \vdots c \Rightarrow k \cdot a \vdots c$

5. $a \vdots a$

6. $a \vdots b, b \vdots a \Rightarrow a = \pm b$

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

8. $ac \vdots bc, c \neq 0 \Rightarrow a \vdots b$

Доказательство

3. $a \vdots c \Rightarrow \exists q_a : a = q_a \cdot c$

   $b \vdots c \Rightarrow \exists q_b : b = q_b \cdot c$

   $a + b = (q_a + q_b) \cdot c$

6. $a = bx$

   $b = ay$

   $a = ayx$

   $$a = a(xy) \Rightarrow \left[\begin{array}{c} a = 0, b \neq 0 \\ a \neq 0, xy = 1 \Rightarrow x, y = \pm 1, a = \pm b \end{array}\right.$$

8. $ac \vdots bc, c \neq 0$

   $ac = bc \cdot x$

   $c \cdot a = c \cdot bx \Rightarrow a = bx \ (a \vdots b)$

Задача: при каких $a, b, c \in \mathbb{Z}$ уравнение $ax + by = c$ имеет решение в целых числах ($\Leftrightarrow$ из чего состоит $< a, b >$? $c \in < a, b >$?)

Def. Идеалом называется подмножество $I \subset \mathbb{Z}$:

1. $I \neq \varnothing$

2. $a, b \in I \Rightarrow a + b \in I$

3. $a \in I, k \in \mathbb{Z} \Rightarrow a \cdot k \in I$

Ex. 1 $c \in \mathbb{Z}$

$< c > = \{n \cdot c\} = \{x \in \mathbb{Z} | x \vdots c\}$ - идеал, порожденный c - главный идеал

Ex. 2 $c_1, c_2 \cdots c_k \in \mathbb{Z}$

$< c_1, c_2 \cdots c_k > = \{n_1 c_1 + n_2 c_2 + \cdots + n_k c_k | n_i \in \mathbb{Z}\}$

Th. в $\mathbb{Z}$ любой идеал - главный

Доказательство

I - идеал в $\mathbb{Z}$, хотим $b \in \mathbb{Z}, I = < b >$

1. $I = \{0\} = < 0 >$

2. $\exists a \in I, a \neq 0 \Rightarrow a \in I, a \in \mathbb{N}$. Рассмотрим наименьший натуральный $b \in I$
   Докажем $I =< b >$
   $< b >\subset I, b \in I, k \cdot b \in I$
   $a \in I$ делим с остатком
   $a = bq + r, 0 \leq r < b$
   $r = a - bq$ $b \in I \Rightarrow -bq \in I \Rightarrow a - bq \in I \Rightarrow r \in I$
   $r \in \mathbb{N}$ - противоречие (b - наименьшее) $\Rightarrow r \notin \mathbb{N} \Rightarrow r = 0$

В частности $\forall a, b \in \mathbb{Z}$ $\exists d :< a, b >=< d >$
Def. $a, b \in \mathbb{Z}$ НОД$(a, b) = gcd(a, b) = (a, b)$ - такое $d \in \mathbb{Z}$, что:

1. $a \vdots d, b \vdots d$

2. $\forall d' : a \vdots d', b \vdots d' \Rightarrow d \vdots d'$

Rem. НОД определен однозначно с точностью до знака

Доказательство

$$\begin{cases} \text{d}_1 = (a, b) \Rightarrow a \vdots d_1, b \vdots d_1, d_2 \vdots d_1 \\ \text{d}_2 = (a, b) \Rightarrow a \vdots d_2, b \vdots d_2, d_1 \vdots d_2 \end{cases} \Rightarrow d_1 = \pm d_2$$

Th. $a, b \in \mathbb{Z}$

1. $\exists (a, b) = d$

2. $\exists x, y \in \mathbb{Z} : ax + by = d$ - линейное представление НОДа

3. $ax + by = c$ имеет решение $\Leftrightarrow c \vdots d$

Доказательство 1

Рассмотрим $I =< a, b >$ - по предыдущей теореме он главный
$< d >=< a, b >$
$d = d \cdot 1 \in I \Rightarrow d \in < a, b >$, т.е. $\exists x, y : ax + by = d$
$d = (a, b) \begin{cases} \text{a } \vdots \text{d' } \Rightarrow ax \vdots d' \; b \vdots d' \Rightarrow by \vdots d' \end{cases} \Rightarrow d \vdots d'$

$a = a \cdot 1 + b \cdot 0 \in < a, b >=< d > \Leftrightarrow a \vdots d$

Аналогично $b \vdots d$

Доказательство 3

$$\Rightarrow: \; c = ax + by \begin{cases} a \vdots (a, b) \\ b \vdots (a, b) \end{cases} \Rightarrow c = ax + by \vdots (a, b)$$

$\Leftarrow$: Пусть $c \vdots (a, b) = d$, т.е. $c = d \cdot k, k \in \mathbb{Z}$
   $ax + by = d$
   $a_{new} = ak, b_{new} = bk$
   $a_{new}x + b_{new}y = dk$

Lem. $(a, b) = (a, b - a)$

$$\begin{cases} \text{a, b } \vdots \text{d} \Rightarrow b - a \Rightarrow d \\ \text{a, b-a } \vdots \text{d} \Rightarrow b = a + (b - a) \vdots d \end{cases} \Rightarrow \text{одинаковые общие делители}$$

Следствие: $b = aq + r \Rightarrow (a, b) = (a, r)$. Доказывается аналогично лемме
Алгоритм Евклида:

1. $a = bq + r_1$

   $b = r_1 q + r_2$

   $\dots$

2. $(a, b) = (r_1, b) = (r_1, r_2) \cdots, \exists i \in \mathbb{N} : r_i = 0$

3. $(a, b) = \cdots = (r_k, r_k + 1) = (r_k, 0) = r_k$

Rem. $a_1, a_2 \cdots a_k \in \mathbb{Z}$
$\exists (a_1, a_2 \cdots a_k) = d \ \exists x_1 \cdots x_k \in \mathbb{Z} :$
$d = x_1 a_1 + x_2 a_2 + \cdots + x_k a_k$

Доказательство

Рассмотрим идеал $< a_1, a_2 \cdots a_k > \exists d :< d >=< a_1 \cdots a_k >$. Далее все как при $k = 2$
Def. $a, b \in \mathbb{Z}$ называются взаимнопростыми, если $(a, b) = 1$
Lm. a, b - взаимнопросты $\Leftrightarrow \exists x, y : ax + by = 1$

Доказательство

$\Rightarrow$ $(a, b) = 1 \Rightarrow \exists x, y : ax + by = 1$

$\Leftarrow$ $ax + by = 1 \Rightarrow 1 \vdots (a, b)$ $(a, b) = 1$

Lm. об отбрасывании взаимнопростого множителя

$$a, b, c \in \mathbb{Z} \begin{cases} ab \vdots c \\ (a, c) = 1 \end{cases} \Rightarrow b \vdots c$$

Доказательство

$ab = cx$

$ay + cz = 1 \Rightarrow aby + cbz = b \vdots c$
Def. $p \in \mathbb{Z}$. p называется простым, если

1. $|p| > 1$

2. $p \neq xy$ $|x|, |y| < |p|$

Ясно, что это равносильно тому, что p имеет ровно 4 делителя $(\pm 1, \pm p)$

Lm. p - простое $\Leftrightarrow ab \vdots p \Rightarrow \left[\begin{array}{l} a \vdots p \\ \\ b \vdots p \end{array} \right., |p| > 1$

Доказательство

$$\Leftarrow \ p = xy \Rightarrow xy \vdots p \Rightarrow \left[\begin{array}{l} x \vdots p \\ \\ y \vdots p \end{array} \right. \Rightarrow \left[\begin{array}{l} |x| \geq p \\ |y| \geq p \end{array} \right.$$

$\Rightarrow$ Пусть p - простое, $ab \vdots p$

$$\left[\begin{array}{l} (a, p) = 1 \Rightarrow b \vdots p \\ \\ (a, p) = p \Rightarrow a \vdots p \end{array} \right.$$

Основная теорема арифметики
$x \in \mathbb{Z}, x \neq 0$

1. $\exists p_1, p_2 \cdots p_k$ - простые > 0

   $\varepsilon = sgn(n)$

   $a_1, a_2 \cdots a_k \in \mathbb{N}$

   $x = \varepsilon p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, p_i \neq p_j$

2. Это разложение единственное с точностью до порядка сомножителей

   $x = \varepsilon_1 p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

   $x = \varepsilon_2 q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$

   $p_i, q_i > 0$, тогда $\varepsilon_1 = \varepsilon_2, k = l$

   $\exists \{i_1, i_2 \cdots i_k\} = \{1, 2 \cdots k\}:$

   $p_{i_1} = q_1 \ a_{i_1} = b_1, p_{i_2} = q_2 \ a_{i_2} = b_2$

Доказательство

Будем доказывать единственность и существование разложения $n = p_1 p_2 \cdots p_s, p_i$ - простые, $n \in \mathbb{N}$

1. Существование:

   Пусть есть плохие n (множество плохих непусто)

   n_0 - наименьшее плохое

   - n_0 - простое
     $p_1 = n_0, s = 1$
     $n_0 = p_1$?? $\Rightarrow n_0$ - хорошее
   - n_0 - составное $\Rightarrow n_0 = n_1 n_2 \ n_1, n_2 < n_0$
     n_1, n_2 - хорошие $\Leftrightarrow \begin{cases} n_1 = p_1 p_2 \cdots p_k, p_i \text{ - простое} \\ n_2 = q_1 q_2 \cdots q_s, q_i \text{ - простое} \end{cases} \Rightarrow n_0 = n_1 n_2 = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_s \Rightarrow n_0$ - хорошее

2. Единственность:

   Пусть есть плохие n

   n_0 - наименьшее из плохих

   $\begin{cases} n_0 = p_1 p_2 \cdots p_k \\ n_0 = q_1 q_2 \cdots q_s \end{cases} \quad p_i, q_i$ - простые

   $$p_1 p_2 \cdots p_k = n_0 \vdots q_1 \Rightarrow \left[\begin{array}{l} p_1 \vdots q_1 \\ p_2 \cdots p_k \vdots q_1 \end{array}\right. \Rightarrow \left[\begin{array}{l} p_1 \vdots q_1 \\ p_2 \vdots q_1 \\ p_3 \cdots p_k \vdots q_1 \end{array}\right. \Rightarrow \cdots \Rightarrow \left[\begin{array}{l} p_1 \vdots q_1 \\ p_2 \vdots q_1 \\ \cdots \\ p_k \vdots q_1 \end{array}\right.$$

   $\exists p_i \vdots q_1$

   $p_i, q_1 > 0 \ q_1 \neq 1 \Rightarrow q_1 = p_i$

   Итак: $\exists i : p_i = q_1 \Rightarrow p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_k = q_2 q_3 \cdots q_s = n_1$, $n_1 < n_0 \Rightarrow n_1$ - хорошее $\Rightarrow$ разложения $p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_k$ и $q_2 q_3 \cdots q_s$ совпадают ??

$n = \varepsilon p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, p_1 < p_2 < \cdots < p_k$ - каноническое разложение
$n = \prod\limits_{p \in \mathbb{P}} p^{v_p(n)}$, почти все $v_p(n) = 0$
$v_p(n)$ - степеньь вхождения p в n
Свойства степени вхождения:

1. $v_p(ab) = v_p(a) + v_p(b)$

2. $v_p(a+b) \geq min(v_p(a), v_p(b))$
   если $v_p(a) \neq v_p(b)$, то $v_p(a+b) = min(v_p(a), v_p(b))$

Rem. $v_p(a)$ - это такое n, что $a \vdots p_n, a \not\vdots p^{n+1}$

Доказательство

1. Напишем разложения:
   $a = p^{v_p(a)} \cdot \prod\limits_{q \neq p} q^{v_q(a)}$
   $b = p^{v_p(b)} \cdot \prod\limits_{q \neq p} q^{v_q(b)}$
   $ab = p^{v_p(a)+v_p(b)} \cdot \prod\limits_{q \neq p} q^{v_q(a)+v_q(b)}$
   $a = p^n x$, $b = p^m y$
   НУО $n \geq m$
   $a + b = p^m p^{n-m} x + p^m y = p^m(p^{n-m}x + y) \vdots p^m = p^{min(n,m)}$
   $n \neq m$ $p^{n-m} x \vdots p \Rightarrow p^{n-m}x + y \not\vdots p \Rightarrow p^m(p^{n-m}x + y) \not\vdots p^{m+1}$
   $m = v_p(a+b)$

Следствия из ОТА
Утверждение: $a = \prod\limits_{p_i \in \mathbb{P}} p_i^{a_i}$, $b = \prod\limits_{p_i \in \mathbb{P}} p_i^{b_i}$
Тогда

1. $a \vdots b \Leftrightarrow a_i \geq b_i \forall i$

2. $\exists c : a = c^k \Leftrightarrow a_i \vdots k \forall i$

3. Число a имеет $\tau(a) = \prod(a_i + 1)$ натуральных делителей

Доказательство

1. $a = bx, x = \prod p_i^{x_i}$
   $\prod p_i^{a_i} = \prod p_i^{b_i} \cdot \prod p_i^{x_i} = \prod p_i^{b_i + x_i} \Leftrightarrow a_i = b_i + x_i \forall i \Leftrightarrow a_i \geq b_i \forall i$

2. Упражнение

3. $|\{$ делители a $\}| = |\{p_1^{b_1} p_2^{b_2} \cdots p_s^{b_s} | \begin{matrix} b_1 \in \{0, 1 \cdots a_1\} \\ b_2 \in \{0, 1 \cdots a_2\} \\ \cdots \\ b_s \in \{0, 1 \cdots a_s\} \end{matrix} \}| = |\{(b_1 \cdots b_s) | b_i \leq a_i\}| = |\{0 \cdots a_1\} \times \{0 \cdots a_2\} \times \cdots \times$
   $\{0 \cdots a_s\}| = (a_1 + 1)(a_2 + 1) \cdots (a_s + 1)$

Def. c - наименьшее общее кратное a, b
$a, b, c \in \mathbb{Z}$ если

1. $c \vdots a, c \vdots b$

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

Утверждение $a = \prod p_i^{a_i}, b = \prod p_i^{b_i}$
$(a, b) = \prod p_i^{min(a_i, b_i)}$
$\exists [a, b] = \prod p_i^{max(a_i, b_i)}$

Доказательство

1. $min(a_i, b_i) \begin{matrix} \leq a_i \\ \leq b_i \end{matrix}$

   $\begin{matrix} \prod p_i^{a_i} \\ \prod p_i^{a_i} \end{matrix} \vdots \prod p_i^{min(a_i,b_i)}$, т.е. $a, b \vdots \prod p_i^{min(a_i,b_i)}$

   $a, b \vdots \prod p_i^{c_i}$ $\forall i$ $\begin{matrix} c_i \leq a_i \\ c_i \leq b_i \end{matrix} \Rightarrow c_i \leq min(a_i, b_i) \Rightarrow \prod p_i^{min(a_i,b_i)} \vdots \prod p_i^{c_i}$

2. НОК - аналогично

Отступление
Решаем диофантовы уравнения
$x^2 - y^2 = 100$ $(x-y)(x+y) = 2^2 \cdot 5^2 \Rightarrow$ знаем $(x-y)$, $(x+y)$ (находим их из разложения 100) $\Rightarrow$ находим x, y
Отступление от теории чисел

Основные алгебраические структуры

Def. Группой называется пара $(G, *)$, где G - множество, $*$ - бинарная операция на G, такая, что:

1. $(a * b) * c = a * (b * c)$ - ассоциативность

2. $\exists e : a * e = e * a = a, e$ - нейтральный элемент

3. $\forall a \in G \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$

Если $a * b = b * a$ (коммутативность), то G - абелева (коммутативная) группа