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
$$\begin{cases} a, b \in \mathbb{Z} \\ b \neq 0 \end{cases} \Rightarrow \exists! q, r \in \mathbb{Z} : a = b \cdot q + r, 0 \leq r < |b|$$

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

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

**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. $\exists x, y : ax + by = d$
$d = (a, b) \begin{cases} a \vdots d' \Rightarrow ax \vdots d' b \vdots d' \Rightarrow by \vdots d' \end{cases} \Rightarrow d \vdots d'$
$a = a \cdot 1 + b \cdot 0 \in < a, b >=< d > \Leftrightarrow a \vdots d$
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.** $(a, b) = (a, b - a)$
$$\begin{cases} a, b \vdots d \Rightarrow b - a \Rightarrow d \\ a, b - a \vdots d \Rightarrow b = a + (b - a) \vdots d \end{cases} \Rightarrow \text{одинаковые общие делители}$$
**Следствие:** $b = aq + r \Rightarrow (a, b) = (a, r)$. Доказывается аналогично лемме
**Алгоритм Евклида:**

1. $a = bq + r_1$
   $b = r_1 q + r_2$
   $\cdots$
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

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

   $\exists p_i \vdots q_1$

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

   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
**Rem.** Простейшие свойства группы

1. Нейтраьный элемент единственный
2. Обратный элемент единственный
3. $a, b \in G$
   - $a * x = b * x \Rightarrow a = b$ – свойство сокращения
   - Уравнения $a * x = b$ и $x * a = b$ имеют единственное решение

**Доказательство (?)**

- $a * x = b * x$
  $(a * x) * x^{-1} = (b * x) * x^{-1}$
  $a * (x * x^{-1}) = b * (x * x^{-1})$
  $a * e = b * e$
  $a = b$
- $a * x = b$
  $a^{-1} * (a * x) = a^{-1} * b$
  $(a^{-1} * a) * x = a^{-1} * b$
  $e * x = a^{-1} * b$
  $x = a^{-1} * b$
- $x * a = b$
  $\dots$
  $x = b * a^{-1}$

Главний пример ассоциативной, но не коммутативной операции – композиция
$f : A \to B$
$\{(a, f(a)) |_{f(a) \in B}^{a \in A}\}$
$g : B \to C$
$b \in B; g(b) \in C$
$a \to f(a) \to g(f(a)) \in C$
$g \circ f : A \to C$
$(g \circ f)(x) = g(f(x)) \ \forall x \in A$
**Rem.** Если $C \neq A$, то $f \circ g$ не существует
$A \to B \to C \to D$
$h \circ (g \circ f) : A \to D$
$(h \circ g) \circ f : A \to D$
и $h \circ (g \circ f) = (h \circ g) \circ f$
$\forall a \in A \ (h \circ (g \circ f))(a) = h(g \circ f)(a) = h(g(f(a))) = ((h \circ g) \circ f)(a)$
**Def.** $M$ – множество
$End(M) = \{f : M \to M\}$
Тогда на $End(M)$ определена бинарная ассоциативная операция $\circ$
$f, g : M \to M$; $f \circ g$; $M \to M \to M$
$End(M)$ замкнуто относительно композиции
**Аксиомы:**

1. Ассоциативность есть
2. $id_m(x) = x \ \forall x \in M$

   $(f \circ id_m)(x) = f(id_m(x)) = f(x)$

   $(id \circ f)(x) = id(f(x)) = f(x)$

   Т.е. $f \circ id = f$ и $id \circ f = f$

   $id_m$ – нейтральный элемент

**Rem.** Если в определение группы взять только аксиомы 1 и 2, то $G$ – моноид. $End(M)$ – моноид
$fix \ f(x) = a$
$g(f(x)) = f(a) - fix$
$g \circ f \neq id_m \ \forall g$
**Th.** $f : M \to M$ имеет обратное $\Leftrightarrow f$ – биекция
Т.е. $\forall y \in M \ f(x) = y$ имеет единственно решение
$f^{-1}(y) = x$
$f^{-1} \circ f(x) = f^{-1}(y) = x$
$f \circ f^{-1}(y) = f(x) = y$

$$\begin{cases} f^{-1} \circ f = id \\ f \circ f^{-1} = id \end{cases} \Rightarrow f^{-1} \text{ – биекция}$$

**Def.** $M$ – множество
$S(M) \subset End(M)$
$S(M) = \{f \in End(M) | f \text{ – биекция}\}$
$S(M)$ – симметрическая группа на множестве $M$, группа относительно $\circ$
**Rem.** $id$ – биекция; $id^{-1} = id$
$M = \{1, 2 \cdots n\}$
$S(M) = S_n$ – симметричная группа (группа перестановок)
**Def.** Кольцом называется тройка $(R, +, \cdot)$, где
$R$ – множество
$+, \cdot$ – бинарные операции на $R$ ($|R| > 1$)
Такие, что:

1. $(R, +)$ – абелева группа
   - $a + b = b + a$
   - $(a + b) + c = a + (b + c)$
   - $\exists 0 : a + 0 = a$
   - $\forall a \exists (-a) : a + (-a) = 0$

5. $\begin{matrix} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{matrix}$ – дистрибутивность

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ – у нас выполняется всегда

7. $\exists 1 : a \cdot 1 = 1 \cdot a = a$

8. $a \cdot b = b \cdot a$

9. $\forall a \in R, a \neq 0 \ \exists a^{-1} : a \cdot a^{-1} = 1$

Если выполняется 1-6, это ассоциативное кольцо
Если выполняется 1-7, это ассоциативное кольцо с 1
Если выполняется 1-6 и 8, это (ассоциативное) коммутативное кольцо
Если выполняется 1-8, это (ассоциативное) коммутативное кольцо с 1
Если выполняется 1-9, это поле
Если выполняется 1-7 и 9, это тело
**Простейшие свойства колец:**

1. $a \cdot 0 = 0$
2. $a \cdot (-1) = -a$

**Rem.** $R$ – поле $\Rightarrow \forall a, b \neq 0\ a \vdots b$
$a = b \cdot \frac{a}{b} = b \cdot (a \cdot b^{-1})$
Значит бессмыслены понятия простых, разложения на простые

# Кольца вычетов

$M, \{(a,b)\} \subset M \times M$ – отноешния на множестве $M$
$aRb$

- $aRb \Rightarrow bRa$ – симметричность
- $aRb, bRc \Rightarrow aRc$ – транзитивность
- $aRa$ – рефлексивность

Если выполняются все 3 пункта, то это отношения эквивалентности
$R$ – отноешние эквивалентности
$a \in M$
$\overline{a} = \{b \in M | aRb\}$ – класс Эквивалентности $a$

**Th.** Любые два класса эквивалентности $\overline{a}, \overline{b}$ : $\left[\begin{array}{l}\overline{a} \bigcap \overline{b} = \varnothing \\ \overline{a} = \overline{b}\end{array}\right.$

В итоге $M = \bigcup \overline{a}$ – разбиение на классы

**Def.** $a, b, n \in \mathbb{Z}$ $a$ сравнимо с $b$ по модулю $n$, если $(a-b) \vdots n$ обозначается $a \equiv b (modn) \Rightarrow \mathbb{Z}$ разбивается на классы эквивалентности. Обозначение: $R$ – отношение, $M/R$ – множество классов эквивалентности, $\sim$ – эквивалентность $M/\sim$ – множество классов эквивалентности – фактормножество

**Доказательство**

P: $a - a = 0 \vdots n \Rightarrow a = a$

C: $a \equiv b \Rightarrow a - b \vdots n \Rightarrow b - a \vdots n \Rightarrow b \equiv a$

T: $\begin{cases} a \equiv b \\ b \equiv c \end{cases} \Rightarrow \begin{cases} a - b \vdots n \\ b - c \vdots n \end{cases} \Rightarrow a - c = (a-b) + (b-c) \vdots n \Rightarrow a \equiv c$

**Rem.** $a \equiv b \Leftrightarrow a$ и $b$ имеют одинаковые остатки от деления на $n$

**Доказательство**

$\Leftarrow$ Упражнение

$\Rightarrow \begin{cases} a = q_a \cdot n + r \\ b = q_b \cdot n + r \end{cases} \Rightarrow a - b = n(q_a - q_b) + 0 \Rightarrow a \equiv b$

$(r_1 - r_2 \neq 0 \Rightarrow 0 < |r_1 - r_2| < n; r_1 - r_2 \not\vdots n)$

Элементы $\mathbb{Z}/\equiv$ – вычеты (классы вычетов) по модулю $n$
$\overline{3} = \{3; 3 \pm n; 3 \pm 2n \cdots\}$
Из Rem $\Rightarrow |\mathbb{Z}/\equiv| =$ n
$\mathbb{Z}/\equiv = \{\overline{0}; \overline{1} \cdots \overline{n-1}\}$
Обозначается $Z/nZ$
**Свойства сравнений:**
$\begin{cases} a \equiv b \\ c \equiv d \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \\ ac \equiv bd \end{cases}$

**Доказательство**

1. $(a+c)-(b+d)=(a-b)+(c-d) \,\vdots\, n$

2. $ac \equiv bc$, т.к. $ac-bc=c(a-b) \,\vdots\, n$

   $ad \equiv bd$, т.к. $ad-bd=d(a-b) \,\vdots\, n$

   По транзитивности $ac \equiv bc \equiv bd$

$a \equiv b \Leftrightarrow \overline{a}=\overline{b}$ в $Z/nZ$
Каноническое отображение:
$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
$a \to \overline{a}=\{a+nk | k \in \mathbb{Z}\}$
$\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\overline{2}\cdots\overline{n-1}\}$
$\begin{cases} a \equiv b \\ c \equiv d \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \\ ac \equiv bd \end{cases}$
Эти свойства позволяют перенести на $\mathbb{Z}/n\mathbb{Z}$ структуру кольца:
$\overline{a}+\overline{b}:=\overline{a+b}$
$\overline{a}\cdot\overline{b}=\overline{a\cdot b}$
Зачем для этго свойства?
Пусть $x, y$ – классы
Строим $x+y$ : выбираем $\begin{matrix} a:\overline{a}=x \\ b:\overline{b}=y \end{matrix} x+y:=\overline{a+b}$
Нужно показать, что результат не зависит от выбора $a$ и $b$
$\begin{cases} \overline{a}=\overline{c} \\ \overline{b}=\overline{d} \end{cases} \Leftrightarrow \begin{cases} a \equiv c \\ b \equiv d \end{cases} \Rightarrow a+c \equiv c+d \Leftrightarrow \overline{a+b}=\overline{c+d}$
С умножением аналогично
**Th.** $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ – коммутативное ассоциативное кольцо с 1

**Доказательство**

Надо проверить 8 аксиом, очев

Пусть $v \in \mathbb{Z}/n\mathbb{Z}$ $f(x)=bx$
$f:\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
Как устроена?
В $\mathbb{Q}$: $f(x)=bx$ – биекция $(b \neq 0)$
В $\mathbb{Z}$: $f(x)=bx$ – инъекция, но не сюрьекция

- $bx=by \Rightarrow x=y$
- Не все числа вида $bx$

**Утверждение** $f$ – биекция $\Leftrightarrow (a,n)=1$; $\overline{a}=b$, иначе это даже не инъекция

**Доказательство**

- $(b,n)=1 \Rightarrow \exists y,z : by+nz=1$

  $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1}\cdots\overline{n-1}\}$ $b=\overline{a}$

  Значения $f$: $\overline{0a},\overline{1a}\cdots\overline{(n-1)a}$

  Заметим, что если $\overline{ka}=\overline{la}$, т.е. $ka \equiv la$, то $\begin{cases} (k-l)a \,\vdots\, n \\ (a,n)=1 \end{cases} \Rightarrow k-l \,\vdots\, n \Rightarrow \overline{k}=\overline{l}$

  Таким образом $f$ – инъективно $\Rightarrow \overline{0a},\overline{1a}\cdots\overline{(n-1)a}$ – попарно различные классы $\Rightarrow$ это $\{\overline{0},\overline{1}\cdots\overline{n-1}\} \Rightarrow$ $f$ – сюрьекция

  **Упражнение:** доказать сюрьективность напрямую через $ay+bz=1$

- Пусть $(a, n) = d \neq 1$

  $a = dz;\ n = dy$

  Положим $x = \overline{y} \in \mathbb{Z}/n\mathbb{Z}$

  Тогда $f(x) = vx = \overline{dz} \cdot \overline{y} = \overline{dzy} = \overline{dy} \cdot \overline{z} = 0 \cdot \overline{z} = 0$ и $f(0) = 0$

  $x \neq \overline{0} = \{0 + nk | k \in \mathbb{Z}\} =< n > \Rightarrow f$ – неинъективна

**Следствие** $p$ – простое, $\mathbb{Z}/p\mathbb{Z}$ – поле

**Доказательство**

Пусть $\overline{a} \neq \overline{0}$, т.е. $a \not\vdots p \Rightarrow (a, p) = 1$, т.е. $x \to \overline{a} \cdot x$ сюрьективно
то есть $\exists b \in \mathbb{Z} : \overline{a} \cdot \overline{b} = 1 \Rightarrow \overline{b} = \overline{a}^{-1}$, т.е. у $\overline{a}$ есть обратный $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ – поле
Как найти этот обратный?
$\overline{a} \cdot \overline{x} = \overline{1};\ ax \equiv 1 \Leftrightarrow ax = 1 + py \Leftrightarrow ax - py = 1$ – линейное представление НОДа, т.е. $x, y$ существуют
Пусть $n$ – составное: $n = pq;\ p, q > 1$
$\overline{p} \cdot \overline{q} = \overline{0}$
$\overline{p}, \overline{q} \neq \overline{0}$ – кольцо с делителями нуля
**Def.** Область целостности – кольцо без делителей нуля
**Lem.**

1. Любое поле – область целостности
2. В области целостности $\begin{cases} ab = ac \\ a \neq 0 \end{cases} \Rightarrow b = c$

**Доказательство**

1. $K$ – поле; $a, b \in K : ab = 0$

   Пусть $a \neq 0 \Rightarrow \exists a^{-1}$

   $a^{-1} \cdot ab = a^{-1} \cdot 0 = 0$, т.е. $b = 0$

   Итак $ab = 0 \Rightarrow \left[\begin{array}{l} a = 0 \\ b = 0 \end{array}\right.$
2. $ab = ac;\ a \neq 0 \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$

**Rem.** $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$
$ax + by = c;\ (a, b) = 1$
$ax = c - by$
$ax \equiv c$
$\overline{a} \cdot \overline{x} = \overline{c}$ в $\mathbb{Z}/b\mathbb{Z}$
$\exists! \overline{x_0} : (a, b) = 1$
$ax \equiv c \Leftrightarrow x \equiv x_0$, т.е. $x = x_0 + bk, k \in \mathbb{Z}$
Тогда $y = \cdots$
**Утверждение** $\begin{cases} (m, n) = 1 \\ a, b \in \mathbb{Z} \end{cases} \Rightarrow$

1. $\exists x \in \mathbb{Z} : \begin{cases} \overline{x} = \overline{a} \text{в } \mathbb{Z}/m\mathbb{Z} \\ \overline{x} = \overline{b} \text{в } \mathbb{Z}/n\mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} x - a \vdots m \\ x - b \vdots n \end{cases}$
2. Пусть $x_0$ – такое, тогда все $x$, удовлетворяющие условию, это $\overline{x_0}$ в $\mathbb{Z}/mn\mathbb{Z}$

**Доказательство**

1. $x - a \vdots m$, т.е. $\begin{cases} x - a = my \\ x - b = nz \end{cases}$

   $my + a = x = nz + b \Rightarrow my - nz = b - a$ – имеет решение, т.к. $(m, n) = 1 \Rightarrow \exists$ соответствующие $x, y$

2. В $\mathbb{Z}/m\mathbb{Z}$ $\overline{x} = \overline{a} = \overline{x_0}$

   В $\mathbb{Z}/n\mathbb{Z}$ $\overline{x} = \overline{b} = \overline{x_0}$

   Т.е. $\begin{cases} x \equiv x_0 \ (mod\ m) \\ x \equiv x_0 \ (mod\ n) \end{cases} \Leftrightarrow \begin{cases} x - x_0 \vdots m \\ x - x_0 \vdots n \\ (a, b) = 1 \end{cases} \Leftrightarrow x - x_0 \vdots mn \Leftrightarrow \overline{x} = \overline{x_0}$ в $\mathbb{Z}/mn\mathbb{Z}$

Смысл: каждой паре остатков по модулю $m$ и по модулю $n$ соответствует единственный остаток по модулю $mn$

$m = 3;\ n = 5$

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 6 | 12 | 3 | 9 |
| 1 | 10 | 1 | 7 | 13 | 4 |
| 2 | 5 | 11 | 2 | 8 | 14 |

Биекция между $\mathbb{Z}/15\mathbb{Z}$ и $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

**Отступление:** произведение групп и колец

**Def.** $R_1, R_2$ – кольца

Их произведение – это $(R_1 \times R_2, +, \cdot)$, где $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$

$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$

**Утверждение** это и правда кольцо (аксиомы наследуются)

**Доказательство**

Очев

**Rem.** $R_1 \times R_2$ – не область целостности $(1, 0) \cdot (0, 1) = (0, 0)$

с группами аналогично:

$G_1, G_2$ – группы $\Rightarrow G_1 \times G_2$ – группа

$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$

Хотим сказать

$(m, n) > 1 \Rightarrow \mathbb{Z}/mn\mathbb{Z}$ и $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ – это одно и то же

**Def.** $R_1, R_2$ – кольца

Изоморфизм между $R_1$ и $R_2$ – биекция

$f : R_1 \to R_2$ такая, что

1. $f(a + b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1) = 1$

$R_1$ и $R_2$ изоморфны, если существует изоморфизм

$G_1, G_2$ – группы

Изоморфизм $f : G_1 \to G_2$ – биекция:

$f(xy) = f(x) \cdot f(y)\ \forall x, y \in G_1$

$G_1$ и $G_2$ изоморфны, если $\exists$ изоморфизм $f : G_1 \to G_2$

$G_1 \cong G_2$. Аналогично $R_1 \cong R_2$ ($R_1, R_2$ – кольца)

**Rem.** $e_1, e_2$ – нейтральные элементы в $G_1, G_2$; $f$ – изоморфизм $\Rightarrow f(e_1) = e_2$

$e_1 \cdot e_1 = e_1$

$\begin{cases} f(e_1 \cdot e_1) = f(e_1) \\ f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1) \end{cases} \Rightarrow f(e_1) \cdot f(e_1) = f(e_1) \cdot e_2 \Rightarrow f(e_1) = e_2$

Аналогично $f(a^{-1}) = f(a)^{-1}$

**Rem2.** Здесь биективность не важна

**Def.** Гомоморфизм отображение $f : G_1 \to G_2 : f(xy) = f(x) \cdot f(y)\ \forall x, y \in G_1$

**Def.** Гомоморфизм колец: $f : R_1 \to R_2$

$\begin{matrix} f(xy) = f(x) \cdot f(y) \\ f(x + y) = f(x) + f(y) \end{matrix} \forall x, y \in R_1$

**Def.** Гомоморфизм колец с 1: требуем еще $f(1_{R_1}) = 1_{R_2}$
**Def.** Изоморфизм между множествами $f : M_1 \to M_2$ – биекция
$f : \mathbb{Z} \to \mathbb{Z}$ $f(x) = kx$ $x \in \mathbb{Z}$

$$\begin{cases} k(x+y) = kx + ky \\ k(xy) \neq kx \cdot ky \end{cases} \Rightarrow f \text{ – не гомоморфизм колец } (k \neq 1)\text{, но гомоморфизм групп}$$

А если $k = \pm 1 \Rightarrow$ изоморфизм
$G$ – группа $f : G \to G$ $f(g) = g^{-1}$ – биекция $\Rightarrow$ изоморфизм, если $G$ – абелева

$$\begin{cases} f : \mathbb{R} \to \mathbb{R} \\ f(x) = e^x \\ e^{x+y} = e^x \cdot e^y \end{cases} \Rightarrow f \text{ – гомоморфизм, но точнее это } f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)\text{, но не изоморфизм}$$

$g : (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot)$ – изоморфизм
$g(x) = e^x$
**Th.** Китайская теорема об остатках

1. $(m, n) = 1$ $Z/mnZ \cong Z/mZ \times Z/nZ$
2. $m_1, m_2 \cdots m_k \in Z$ $(m_i, m_j) = 1$

   $Z/m_1m_2 \cdots m_kZ \cong Z/m_1Z \times \cdots \times Z/m_kZ$
3. $\forall a_1, a_2 \cdots a_n \in Z;\ m_1, m_2 \cdots m_n \in Z : (m_i, m_j) = 1$

$$\begin{cases} x \equiv a_1\ (mod\ m1) \\ x \equiv a_2\ (mod\ m2) \\ \vdots \\ x \equiv a_n\ (mod\ mn) \end{cases} \text{ – имеет решение в } Z\text{, единственное по модулю } m_1m_2 \cdots m_n$$

**Доказательство**

Индукция по $k$. База $k = 2$

- База: строим $\varphi : Z/mnZ \to Z/mZ \times Z/nZ$

  $\overline{a_{mn}} \to (\overline{a_m}, \overline{a_n})$

  $(\overline{a_{mn}} = \overline{b_{nm}} \Rightarrow \overline{a_m} = \overline{b_m})$

  $\varphi$ – гомоморфизм:

  $\varphi(x + y) = \varphi(\overline{a_{mn}} + \overline{b_{mn}}) = \varphi(\overline{a + b_{mn}}) = (\overline{a + b_m}, \overline{a + b_n}) = (\overline{a_m} + \overline{b_m}, \overline{a_n} + \overline{b_n}) = (\overline{a_m}, \overline{a_n}) + (\overline{b_m}, \overline{b_n}) = \varphi(x) + \varphi(y)$

  $\varphi$ – биекция (смотри утверждение перед табличкой $3 \times 5$)

  $$\forall a, b\ \exists x : \begin{cases} x \equiv a\ mod\ m \\ x \equiv b\ mod\ n \end{cases} \text{ и все такие } x \text{ имеют вид } x = x_0 + kmn$$

- Переход $k \to k + 1$

  $m_1, m_2 \cdots m_{k+1}$ попарно взаимнопросты $\Rightarrow (m1m2 \cdots m_k, m_{k+1}) = 1 \Rightarrow$ по базе

  $Z/m_1m_2 \cdots m_{k+1}Z \cong Z/m_1m_2 \cdots m_kZ \times Z/m_{k+1}Z$

  По индукционному предположению $Z/m_1 \cdots m_k \cong Z/m_1Z \times \cdots \times Z/m_kZ$

  Итого $Z/m_1 \cdots m_{k+1}Z \cong Z/m_1 \cdots m_kZ \times Z/m_{k+1}Z \cong (Z/m_1Z \times Z/m_2Z \times \cdots \times Z/m_kZ) \times Z/m_{k+1}Z \cong Z/m_1 \times \cdots \times Z/m_kZ \times Z/m_{k+1}Z$

  **Rem.** $(A \times B) \times C \neq A \times B \times C$

  $((a, b), c) \to (a, b, c)$

- $\varphi$ – сюръективно, т.е. $\forall y_1 \cdots y_n$ $y_i \in Z/m_iZ$

  $\exists z \in Z/m_1 \cdots m_nZ : \varphi(z) = (y_1, y_2 \cdots y_n)$

Возьмем $y_i = \overline{a_1}\ a_i \in Z\ z = \overline{xm_1} \cdots m_n \Rightarrow \begin{cases} \overline{x_{m_1}} = y_1 \\ \overline{x_{m_2}} = y_2 \\ \cdots \end{cases}$, т.е. $\begin{cases} x \equiv a_1\ mod\ m_1 \\ x \equiv a_2\ mod\ m_2 \\ \cdots \end{cases}$

Единственность $x$ по модулю $m_1 \cdots m_n$ – инъективность $\varphi$

"Явная формула"для $\varphi^{-1}$

Найдем $\varphi^{-1}(1_{m_1}, 0_{m_2} \cdots 0_{m_k})$ это $\overline{a}$ : $\begin{matrix} a - 1 \vdots m_1 \\ a \vdots m_2, \cdots, m_k \Leftrightarrow a \vdots m_2 \cdots m_k \end{matrix}$

$a = m_2 \cdots m_k \cdot y;\ m_2 \cdots m_k \cdot y - 1 = m_1 x$

$m_2 \cdots m_k \cdot y - m_1 x = 1$. Далее ищем $y$

$a = a_1\ \varphi(\overline{a_1}) = (1, 0 \cdots 0)$

Аналогично находим $\varphi(\overline{a_i}) = (0, 0 \cdots 1_{m_i} \cdots 0)$

Теперь $\forall \overline{b_1}, \overline{b_2}, \cdots \overline{b_k}\ (b_i \in Z/m_i Z)$

$\varphi(\overline{a_1 b_1} + \overline{a_2 b_2} + \cdots + \overline{a_k b_k}) = \varphi(b\overline{a_1}) + \varphi(b_2\overline{a_2}) + \cdots + \varphi(b_k\overline{a_k}) = b_1\varphi(\overline{a_1}) + b_2\varphi(\overline{a_2}) + \cdots + b_k\varphi(\overline{a_k}) = b_1(1, 0 \cdots 0) + b_2(0, 1, 0 \cdots 0) + \cdots + b_k(0 \cdots 0, 1)$

**Rem.** $\varphi(\overline{3x}) = \varphi(\overline{x} + \overline{x} + \overline{x}) = \overline{3\varphi(x)}$

**Def.** $G$ – группа. $a \in G$, порядок $a$ – $\min k \in N : a^k = e$. Если такого $k$ нет, то порядок $= \infty$. Обозначение: $ord(a)$

**Lm.**

1. $ord(a)$ – количество различных элементов в последовательности $(e, a, a^2, a^3 \cdots)$
2. $ord(a) = \infty \Rightarrow$ все элементы различны
3. $ord(a) = k \in N$, тогда $a^m = a^n \Leftrightarrow m \equiv n\ (mod\ k)$

### Доказательство

1. 2, 3 $\Rightarrow$ 1 – упражнение
2. $ord(a) = \infty\ a^m = a^n$, НУО $m > 0$

   $a^m \cdot a^{m-n} = a^n \cdot e \Rightarrow a^{m-n} = e;\ m - n \in N$, но $ord(a) = \infty$ ???
3. $ord(a) = k\ m, n \in N$

   $m = q_m \cdot k + r_m;\ n = q_n \cdot k + r_n$

   $$\begin{cases} a^m = a^{q_m \cdot k + r_m} = (a^k)^{q_m} \cdot a^{r_m} = a^{r_m} \\ a^n = a^{r_n} \\ r_m = r_n \end{cases} \Rightarrow a^m = a^n \Rightarrow a^{r_m} = a^{r_n} \Rightarrow a^{r_m - r_n} = e\ ???$$

**Th.** Теорема Лагранжа

$G$ – группа, $|G| = n$ ($|G|$ – порядок группы)

$a \in G;\ ord(a) = k \Rightarrow n \vdots k$

### Доказательство

Нарисуем орграф $\forall x \in G : x \to ax$

$\forall x \to$ цикл $x \to ax \to a^2 x \to \cdots \to a^k x = x$

Все элементы $G$ разбились на циклы длины $k \Rightarrow n \vdots k$

**Следствие:** малая теорема Ферма

$G = (Z/pZ)^*;\ |(Z/pZ)^*| = p - 1$

$ord(\overline{a}) = k \Leftrightarrow \overline{a^k} = \overline{1};\ p - 1 \vdots k$

$a^{p-1} = (a^k)^{=}(\overline{1})^l = 1$

В $Z/pZ$ $\begin{matrix} \overline{a^{p-1}} = \overline{1} \\ \overline{a} \neq \overline{0} \end{matrix}$ $a \not\vdots p \Rightarrow a^{p-1} \equiv 1\ (mod\ p) \Leftrightarrow a^{p-1} - 1 \vdots p$

**Th.** Переформулировка теоремы Лагранжа

$G$ – конечная $\Rightarrow a^{|G|} = e$

$e, a, a^2 \cdots$ преиодична с периодом $|G|$, но возможно это не наименьший период
$G = (Z/pZ)^* \Rightarrow a^{p-1} = 1$ в $Z/pZ \Leftrightarrow a^{p-1} \equiv 1 \ (mod\ p)\ (\forall a \not\vdots p)$

Или $a \in Z;\ a^p - a \vdots p \Leftrightarrow a(a^{p-1} - 1) \vdots p \Leftrightarrow \left[\begin{array}{l} a \vdots p \\ a^{p-1} - 1 \vdots p \end{array}\right.$

Что с произвольным $n$? Хотим $a^k \equiv 1\ (mod\ n)$
$(a, n) \neq 1 \Rightarrow (a^k, n) \neq 1 \Rightarrow a^k \not\equiv 1\ (mod\ n)\ (\forall k > 0) \Rightarrow$ вопрос имеет смысл только для $(a, n) = 1 \Rightarrow \overline{a}$ – обратим в $Z/nZ$
По теореме Лагранжа $b \in (Z/nZ)^* \Rightarrow b^{|(Z/nZ)^*|} = 1$
Переформулировка: $(a, n) = 1 \Rightarrow a^{|(Z/nZ)^*|} \equiv 1\ (mod\ n)$ – теорема Эйлера

**Def.** Функция Эйлера $\varphi(n) = |(Z/nZ)^*|$
**Rem.** $\varphi(n) = \{x \in \{0, z \cdots n-1\} | (x, n) = 1\}$
**Ex.** $p$ – простое. Знаем $(Z/pZ)^* = (Z/pZ) \backslash \{0\}$
$\varphi(p) = p - 1$
Как найти $\varphi(n)$? $n = p_1^{a_1} p_2^{a_2} \cdots$
**Rem1.** $p$ – простое $\Rightarrow \varphi(p^k) = \{x \in \{0, 1 \cdots p^k - 1\} | (p^k, x) = 1\} = \{x = 0 \cdots p^k - 1 | x \not\vdots p\} = p^k - \{x = 0 \cdots p^k - 1 | x \vdots p\} = p^k - \frac{p^k}{p} = p^k = p^{k-1}$
**Rem2.** Мультипликативность $\varphi$
$m, n \in N\ (m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$
$\varphi$ – мультипликативная функция
**Remrem.** $\tau(n)$ – количество делителей, $\sigma(n)$ – сумма делителей. Обе эти функции тоже мультипликативны (упражнение)

**Явная формуля для функции Эйлера**
$\varphi(n) = \varphi(p_1^{a_1} \cdots p_k^{a_k}) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1}) = p_1^{a_1}(1 - \frac{1}{p_1}) \cdots p_k(1 - \frac{1}{p_k}) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) = n \prod\limits_{p \in P; p | n} (1 - \frac{1}{p})$
**Ex.** $\varphi(600) = 600 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 160$
**Rem.** $a^{\varphi(n)} = 1\ (\forall a \in (Z/nZ)^*)$
$n \vdots p, q \Rightarrow$ показатель $\varphi(n)$ можно улучшить
$n = 105 = 3 \cdot 5 \cdot 7 \Rightarrow \varphi(n) = 2 \cdot 4 \cdot 6 = 48$
По теореме Эйлера $(a, 105) = 1 \Rightarrow a^{48} \equiv 1\ (mod\ 105)$
На самом деле (применим МТФ) $(a, 105) = 1 \Rightarrow a \not\vdots 3, 5, 7 \Rightarrow \begin{cases} a^2 \equiv 1\ (mod 3) \\ a^4 \equiv 1\ (mod 5) \\ a^6 \equiv 1\ (mod 7) \end{cases} \Rightarrow \begin{cases} a^{12} \equiv 1\ (mod 3) \\ a^{12} \equiv 1\ (mod 5) \\ a^{12} \equiv 1\ (mod 7) \end{cases} \Rightarrow$
$\Rightarrow a^{12} \equiv 1\ (mod 105)$

### Доказательство мультипликативности

Знаем: $(m, n) = 1 \Rightarrow Z/mnZ \cong Z/mZ \times Z/nZ \Rightarrow \varphi(ab) = \varphi(a) \cdot \varphi(b)$
$\varphi$ – изоморфизм. $x$ – обратим $\Leftrightarrow \varphi(n)$ – обратим
$x$ – обратим $\Leftrightarrow \exists y : x \cdot y = 1$. $\varphi(xy) = \varphi(x) \cdot \varphi(y) = 1 = \varphi(1) \Rightarrow \varphi$ – обратим
Обратно: $\varphi(x)$ – обратим. $\varphi(x) \cdot z = 1 \Rightarrow \varphi^{-1}(\varphi(x) \cdot z) = \varphi^{-1}(1)$. $\varphi^{-1}(\varphi(x)) \cdot \varphi^{-1}(z) = \varphi^{-1}(1) \Rightarrow x$ – обратим
**Следствие:** $(Z/mnZ)^* = (Z/mZ \times Z/nZ)^*$
**Утверждение.** $R_1, R_2$ – кольца. $(R_1 \times R_2)^* = R_1^* \times R_2^*$

### Доказательство

$(r_1, r_2) \in R_1 \times R_2$ – обратим $\Leftrightarrow \exists (s_1, s_2) : (r_1, r_2)(s_1, s_2) = 1_{R_1 \times R_2} \Leftrightarrow (r_1 s_1, r_2 s_2) = (1_{R_1}, 1_{R_2}) \Leftrightarrow \begin{cases} \exists s_1 : r_1 s_1 = 1 \\ \exists s_2 : r_2 s_2 = 1 \end{cases} \Leftrightarrow$
$\Leftrightarrow \begin{cases} r_1 \in R_1^* \\ r_2 \in R_2^* \end{cases}$
**Следствие:** $|(Z/mZ \times Z/nZ)^*| = |(Z/mZ)^* \times (Z/nZ)^*| = |(Z/mZ)^*| \cdot |(Z/nZ)^*|$

Итого: $\varphi(mn) = \varphi(m) \cdot \varphi(n)$

Вопрос: $p \in P$. $\exists$ ли $\overline{a} \in Z/pZ : \{\overline{a}, \overline{a^2} \cdots\} = \{\overline{1}, \overline{2} \cdots \overline{p-1}\}$
**Def.** $(G, \cdot)$ – группа; $a \in G$
$< a >= \{a^k | k \in Z\}$ – группа, порожденная элементом $a$
**Утверждение.** Это действительно группа (относительно $\cdot$)

**Доказательство**

- Замкнутость. $x, y \in < a >$
  $x = a^e; y = a^m \Rightarrow xy = a^{e+m} \in < a >$
- Ассоциативность – очев
- $\exists e \in G;\ e = a^0 \in < a >$
- $x \in < a > \Rightarrow x = a^k \Rightarrow x^{-1} = a^{-k} \in < a >$

$< a >$ – подгруппа в $G$. Может быть $< a >= G$ или $< a > \neq G$
**Def.** Если $\exists a \in G :< a >= G \Rightarrow G$ называется циклической
**Th.** $G$ – циклическая

1. $|G| = \infty \Rightarrow G \cong (Z, +)$
2. $|G| = n < \infty \Rightarrow G \cong (Z/nZ, +)$

**Доказательство**

$G =< a >$. Знаем: $ord(a) = k \Rightarrow$ в $< a >$ $k$ элементов. Иначе $(ord(a) = \infty) \Rightarrow$ все $\{a^k | k \in Z\}$ попарно различны

1. Строим гомоморфизм
   $\varphi Z \to G;\ k \to a^k$
   Это биекция (см. выше) и $\varphi(x + y) = a^{x+y} = a^x \cdot a^y = \varphi(x) + \varphi(y)$ – точно гомоморфизм
2. $(k = n)$ $ord(a) = n$. $< a >= \{e, a, a^2 \cdots a^{n-1}\}$
   $(a^n = e;\ a^{-1} = a^{n-1})$
   $\varphi : Z/nZ \to < a >;\ \overline{p} \to a^p$ – биекция и гомоморфизм (упражнение)
   Корректность: $q : \overline{p} = \overline{q} \Rightarrow p - q \,\vdots\, n$
   $p = q + ln \Rightarrow a^p = a^{q+ln} = a^q \cdot (a^n)^l = a^q \Rightarrow a^p = a^q$

**Ex.** $(Z/3Z)^* =< 2 >$: $\overline{2}^2 = 1$ $(ord(\overline{2}) = 2)$
Изоморфизм: $(Z/2Z, +) \to (Z/3Z, \cdot)$
$\overline{0}_2 \leftrightarrow \overline{1}_3$
$\overline{1}_2 \leftrightarrow \overline{2}_3$
$(Z/5Z)^* = \{1, 2, 3, 4\} =< \overline{2} >$ $(ord(2) = 4)$. Поэтому $(Z/5Z)^* \cong (Z/4Z, +)$

**Th.** $p \in P \Rightarrow (Z/pZ)^*$ – циклическая
**Следствие.** $(Z/pZ)^* \cong (Z/(p-1)Z, +)$
$\exists a \in Z :< \overline{a} >= \{1, 2 \cdots p - 1\}$
$a$ называется первообразным корнем по модулю $p$
$a$ – первообразный корень $mod\ p \Leftrightarrow ord(\overline{a}) = p - 1$, т.е. $| < \overline{a} > | = p - 1 = |(Z/pZ)^*|$

**Lm.** $G$ – группа $|G| = N$. $f : G \to G : f(a) = a^k$
Тогда $f_k$ – биекция $\Leftrightarrow (k, N) = 1$

**Доказательство**

Только $\Leftarrow$:
$(k, N) = 1 \Rightarrow \exists x, y : xk + yN = 1 \Rightarrow \forall a \in G;\ a = a^1 = a^{xk+yN} = (a^k)^x \cdot (a^N)^y$ по переформулировке теоремы Лагранжа $= (a^k)^x \Rightarrow f_x$ – обратное к $f_k$

# Алгоритм RSA (шифрование с открытым ключом)

Алиса (А) хочет получать сообщения от Боба (В)
А придумывает $p, q$ – простые (достаточно большие) $N = pq$
$\varphi(N) = (p-1)(q-1)$. А выбирает $x : (x, \varphi(N)) = 1$ и $y : (x - y) \equiv 1\ (mod \varphi(N))$
Тогда как в Lm. $f_x(a) = a^x;\ f_y(a) = a^y$ – взаимно обратные отображения
А сообщает В $x$
В хочет послать А сообщение. $a \in (Z/NZ)^*$
Шифрование: $a \to a^x = b$ и посылает А
А получает $b = a^x$, вычисляет $b^y = a$

Что нужно чтобы дешифровать $b$? Надо знать $y$
$N, x$ известны всем. $xy \equiv 1\ (mod \varphi(N))$
$yx + \varphi(N)z = 1$ – линейное Диофантово уравнение. Легко решается зная $x, \varphi(N)$
Нужно сделать так, чтобы $\varphi(N)$ было сложно узнать

Вопрос: как найти большие простые числа?
$p$ – большое натуральное число. Как проверить, что $p$ – простое?
Рассмотрим $n \in \mathbb{N}$. $n - 1 = p_1^{a_1} \dots p_5^{a_5}$, т.е. $n = \prod p_i^{a_i} + 1$. Простое ли $n$?

**Th.** Тест Люка
Пусть $n = \prod p_i^{a_i} + 1 . a \in \mathbb{Z}$
$$\begin{cases} a^{n-1} = 1\ (mod\ n) \\ a^{\frac{n-1}{p_i}} \neq 1\ (mod\ n) \end{cases} \Rightarrow n \text{ – простое}$$

**Доказательство**

В $(Z/mZ)^*$ $ord(a) = ?$
$$\begin{cases} a^{n-1} \equiv 1 \Leftrightarrow n - 1 \vdots ord(a) \\ a^{\frac{n-1}{p_i}} \neq 1 \Leftrightarrow \frac{n-1}{p_i} \not\vdots ord(a) \end{cases} \Rightarrow n - 1 = ord(a) \Rightarrow |(Z/nZ)^*| \geq |<a>| = n - 1$$
$\varphi(n) \geq n - 1 \Leftrightarrow 1, 2 \dots n - 1$ взаимнопросты с $n \Rightarrow n$ – простое

Вопрос: какая доля $a \in \{1, 2 \dots n\}$ удовлетворяет условию Люка, если $n$ – простое?
$a \in \{1 \dots n - 1\} \Rightarrow \overline{a} \in (Z/nZ)^*$. Какова вероятность: $ord(\overline{a}) = n - 1$?

Знаем: $n$ – простое $\Rightarrow (Z/nZ)^*$ – циклическая. $(Z/nZ)^* = <b>$ $ord(b) = n - 1$
$\forall a \in (Z/nZ)^*\ \exists k : b^k = a;\ k \in \{1, 2 \dots n - 1\}$
**Утверждение:** $ord(a) = n - 1 \Leftrightarrow (k, n - 1) = 1$
**Следствие:** Доля подходящих под тест Люка $a\ = \frac{\varphi(n-1)}{n-1} = p \in [0; 1]$
$$\text{Делаем тест Люка } s \text{ раз} \Rightarrow \left[ \begin{array}{l} \text{попадется хорошее } a \Rightarrow n \text{ – простое} \\ \text{все время плохие } a \Rightarrow (1-p)^s \to 0 \end{array} \right.$$
**Lm.** $ord(x) = n \Rightarrow ord(x^k) = \frac{n}{(n,k)}$ (утверждение: частный случай)
$$(n, k) = d \Rightarrow \begin{cases} n = dn_1 \\ k = dk_1 \end{cases} \Rightarrow (x^k)^{\frac{n}{(n,k)}} = (x^{dk_1})^{n_1} = 1^{n_1} = 1$$
Пусть $(x^k)^l = 1;\ x^{kl} = 1 \Leftrightarrow kl \vdots ord(x) \Leftrightarrow dk_1 l \vdots dn_1 \Leftrightarrow k_1 b \vdots n_1 \Leftrightarrow l \vdots n_1$, т.е. $n_1 = min(l)$

**Нестойкость простых из теста Люка**
Пусть $p, q$ – простые получены тестом Люка, т.е. у $p - 1$ и $q - 1$ маленькие простые множители

$N = pq$. Как зная все разложить $N$?

$a \in N;\ \begin{cases} ord_p(a) = p_1^{b_1} \dots p_k^{b_k} \\ ord_q(a) = p_1^{c_1} \dots p_k^{c_k} \end{cases}$

$\begin{cases} A = min(x | x! \vdots ord_p(a)) \\ B = min(x | x! \vdots ord_q(a)) \end{cases} \Rightarrow A, B$ не очень большие, скорее всего $A \neq B$

Враг считает $d_k = (a^{k!} - 1, n)$. НУО $A < B$. Тогда $d_A = p;\ a := \frac{N}{b}$. Взломано

**Тест Ферма:**
$n \in Z;\ a \in Z;\ a \in \{1 \dots n-1\}$. $n$ тестируем, $a$ – случайное
$a^{n-1} \not\equiv 1\ (mod\ n) \Rightarrow n$ – составное
$a^{n-1} \equiv 1\ (mod\ n) \Rightarrow n$ – может быть простое

$(n = 15;\ n - 1 = 14;\ 4^{14} \equiv 1\ (mod\ 15)$, но 15 не простое)

$a$ – свидетель простотые $mod\ n$, если $a^{n-1} \equiv 1\ (mod\ n)$
**Утверждение:** (упражнение) если не все числа $\{1 \dots n-1\}$ – свидетели, то свидетелей $\leq$ половины
$a$ – свидетель, $b$ не свидетель $\Rightarrow ab$ не свидетель. В этом случае за $s$ тестов $p$(неудачи) $\leq (\frac{1}{2})^s \to 0$
Проблема: $\exists n$ – составные : $\forall a \in (Z/nZ)^*$ – свидетель простоты
Это числа Кармайкла. Наименьшее такое число $n = 561 = 3 \cdot 11 \cdot 17$

$a \not\vdots 3, 11, 17;\ \begin{cases} a^2 \equiv 1\ (mod\ 3) \\ a^{10} \equiv 1\ (mod\ 11) \\ a^{16} \equiv 1\ (mod\ 17) \end{cases} \Rightarrow a \equiv 1\ (mod\ 561) \Rightarrow a^{560} \equiv 1\ (mod\ 561)$, но 561 не простое

**Тест Рабина-Миллера:**
$p \in Z;\ p - 1 = 2^m \cdot l;\ l \not\vdots 2$
$a \in Z;\ a \not\vdots p$. Рассмотрим в $Z/pZ$ последовательность $\overline{a}^l, \overline{a}^{2l} \dots \overline{a}^{2^m l} = a^{p-1} = 1$

**Утверждение:** Если $p$ – простое, то $\left[ \begin{array}{c} \overline{a}^l = 1 \\ \exists k : \overline{a}^{2^k l} = \overline{-1} \end{array} \right. \quad (*)$

**Доказательство**

Пусть $a^l \neq 1;\ a^{p-1} = 1 \Rightarrow \exists k : \overline{a}^{2^k l} \neq 1;\ \overline{a}^{2^{k+1} l} = 1$

$\Rightarrow$ в $Z/pZ$ $x \neq 1;\ x^2 = 1 \Rightarrow (x-1)(x+1) = 0 \Rightarrow \left[ \begin{array}{l} x - 1 = 0 \\ x + 1 = 0 \end{array} \right. \Rightarrow x = -1$

$*$ – условия Рабина-Миллера для числа $a$
Знаем: $\exists a \not\vdots p$. Рабин-Миллер для $a$ не выполнен $\Rightarrow p$ – составные

**Th.** Если все $a = 1, 2 \dots \sqrt[7]{p}$ свидетели Рабина-Миллера $\Rightarrow p$ – простое
**Th.** Если все $a = 1, 2 \dots c \cdot \log^2 p$ свидетели $\Rightarrow p$ – простое. (следует из гипотезы Римана)
**Th.** $n$ – составное $\Rightarrow$ свидетелей Рабина-Миллера $\leq \frac{\varphi(n)}{4}$
**Следствие:** делаем $s$ ходов. $p$(неудачи) $= (\frac{1}{4})^s \to 0$

# Квадратичные вычеты

$Z \to Z/nZ \to Z/pZ$. Как решать уравнения в $Z/pZ$?

1. Линейные $\overline{ax} = \overline{b} \Leftrightarrow ax \equiv b\ (mod\ p) \Leftrightarrow ax - py = b$

2. Квадратные $ax^2 + bx + c = 0;\ a \neq 0$

   $x^2 + sx + q = 0$. Если $p \neq 2$, то

   $(x + \frac{s}{2})^2 + (q - \frac{s^2}{4}) = 0 \Leftrightarrow y^2 = k$, где $y = x + \frac{s}{2};\ -k = q - \frac{s^2}{4}$

   Как понять, что $\exists y : y^2 \equiv k$ в $Z/pZ$

   Или для каких $p$ $\exists y : (y^2 - k \vdots p)$

   Если такой $y$ существует, $k$ называется квадратичным вычетом по модулю $p$. $(k \neq 0)$

Символ Лежандра $\binom{a}{p} = \left[\begin{array}{r} 1,\ a\text{– квадратичные вычет} \\ -1,\ a\text{– не квадратичные вычет} \\ 0,\ a \vdots p \end{array}\right.$

**Утверждение:** $\exists$ ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных неравенства

**Доказательство**

$1, 2 \ldots p-1$

$1^2, 2^2 \ldots (p-1)^2$

Сколько различный вычетов во второй строке? Заметим: $x^2 = y^2 \Rightarrow (x-y)(x+y) = 0 \Leftrightarrow \left[\begin{array}{l} x = y \\ x = -y \end{array}\right. \Rightarrow$ при возведении в квадрат вычеты склеиваются, попадая $\Rightarrow$ ровно $\frac{p-1}{2}$ квадратов $\Rightarrow p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ не квадратов

Мультипликативность: $\forall a, b. \binom{ab}{p} = \binom{a}{p}\binom{b}{p}$

**Доказательство**

$\binom{ab}{p} = 0 \Leftrightarrow ab \vdots p \Leftrightarrow \left[\begin{array}{l} a \vdots p \\ b \vdots p \end{array}\right. \Leftrightarrow \left[\begin{array}{l} \begin{pmatrix} a \\ p \end{pmatrix} = 0 \\ \begin{pmatrix} b \\ p \end{pmatrix} = 0 \end{array}\right.$

$\binom{a}{p}\binom{b}{p} = 1 \Rightarrow \begin{cases} a = x^2 \\ b = y^2 \end{cases} \Rightarrow ab = (xy)^2 \Rightarrow \binom{ab}{p} = 1$

$\binom{a}{p} = 1;\ \binom{b}{p} = 1 \Rightarrow \exists x : a = x^2;\ b \neq y^2\ \forall y$

Пусть $\begin{cases} ab = z^2 \\ a = x^2 \end{cases} \Rightarrow b = (\frac{z}{x})^2$ ????

$\binom{a}{p} = -1;\ \binom{b}{p} = -1$

$b_1, b_2 \ldots b_{\frac{p-1}{2}}$ – квадраты, все остальные не квадраты

Идем $ab_1, ab_2 \ldots ab_{\frac{p-1}{2}}$ – не квадраты (все, т.к. их $\frac{p-1}{2}$) $\Rightarrow$ все остальные квадраты

$\{ab_1, ab_2 \ldots ab_{p-1}\} = \{1, 2 \ldots p-1\}$

**Утверждение:** Квадратичный закон взаимности

Если $p, q$ – нечетные простые $\Rightarrow \binom{p}{q}\binom{q}{p} = (-1)^{\frac{p-1}{2} \cdots \frac{q-1}{2}}$

$R$ – коммутативное кольцо с 1

$f(x) = 3x^2 + 2x$ имеет смысл в любом кольце с 1, т.к. $f(x) = (1+1+1) \cdot x \cdot x + (1+1) \cdot x$

**Ex.** $g, f : Z/pZ \to Z/pZ$

$\begin{cases} f(x) = x \\ g(x) = x^p \end{cases} \Rightarrow$ по МТФ одна и та же функция, но многочлены различные

$x^2 + 2x + 5 \to (1, 2, 5)$

## Формальные степенные ряды

**Def.** Пусть $R$ – коммутативное кольцо с 1. Кольцом формальных степенных рядов $R[[x]]$ называется множество $f : Z_{\geq 0} \to R$; $\{a_0, a_1, a_2 \ldots | a_i \in R\}$ с операциями $+, \cdot$

Ряд: $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$

$(a_0, a_1, a_2 \ldots) + (b_0, b_1, b_2 \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots)$

$(a_i)\cdot(b_i)=(c_i)_{i=0}^{\infty};\ c_i=\sum\limits_{k=0}^{i}a_kb_{i-k}$ – правило свертки

**Th.** $R[[x]]$ – коммутативное кольцо с 1

**Доказательство**

Очев – аксиомы сложения: $(0,0\dots)=0_{R[[x]]}$
$1_{R[[x]]}=(1,0,0\dots)$
$(a+b)\cdot c$ – очев (покоординатно)
$ab=ba:(ab)_i=\sum\limits_{k=0}^{i}a_ib_{i-k}=\sum\limits_{l=0}^{i}a_{i-l}b_l=\sum\limits_{l=0}^{i}b_la_{i-l}=(ba)_i$
Ассоциативность: $(f\cdot g)\cdot h=f(g\cdot h);\ f,g,h\in R[[x]]$
$f=(a_0,a_1,a_2\dots a_i\dots);\ f_i=a_i$
$((f\cdot g)\cdot h)_n=\sum\limits_{k=0}^{n}(fg)_kh_{n-k}=\sum\limits_{k=0}^{n}(\sum\limits_{i=0}^{k}f_ig_{k-i})h_{n-k}=\sum\limits_{k=0\dots n;i=0\dots k}f_ig_{k-i}h_{n-k}=\sum\limits_{p,q,r\geq0;p+q+r=n}(f_pg_q)h_r=$
$\sum\limits_{p,q,r\geq0;p+q+r=n}f_p(g_qh_r)=\sum\limits_{p,q,r\geq0;p+q\leq n}f_p(g_qh_{n-p-q})=\sum\limits_{r=0}^{n}f_p(\sum\limits_{q=0}^{p}g_qh_{(n-p)-q})=\sum f_p(gh)_{n-p}=(f(gh))_n$

**Lem.** $\exists$ инъективный гомоморфизм колец
$i:\begin{matrix}R\to R[[x]]\\ a\to(a,0,0\dots)\end{matrix}$

**Доказательство**

Нужно доказать $\begin{cases}\text{инъективность}\\ i(x+y)=i(x)+i(y)\\ i(xy)=i(x)\cdot i(y)\\ i(1)=1\end{cases}$ – все очев
В умножении $(a,0,0\dots)\cdot(b,0,0\dots)=(ab,0,0\dots)$

**Def.** $x=(0,1,0,0\dots)$
**Lem.** $a\in R\begin{cases}ax=(0,a,0,0\dots)\\ x^2=(0,0,1,0,0\dots)\\ x^k=(0,0,0\dots1,0,0\dots)\end{cases}$

$(a_0,a_1,a_2\dots a_k,0,0\dots)=a_0+a_1x+a_2x^2+\dots a_kx^k$ – следствие из леммы и правила сложения
**Def.** $f\in R[[x]]$ называется многочленом, если $\exists N:\forall n>N\ f_n=0$
**Обозначение:** множество многочленов обозначается $R[x]$
**Lem.** $R[x]$ – подкольцо в $R[[x]]$

**Доказательство**

$0,1\in R[x]$ – очев
$(a_n)\in R[x]\Rightarrow(-a_n)\in R[x]$ – тоже очев
$(b_i),(a_i)\in R[x]\Rightarrow(b_i+a_i)\in R[x]\ \begin{cases}\exists N_1:a_n=0;\ n>N_1\\ \exists N_2:b_n=0;\ n>N_2\end{cases}\Rightarrow(a+b)_n=0;\ n>max(N_1;N_2)\ (a\cdot b)_n=0=$
$=\sum\limits_{i=0}^{n}a_ib_{n-i};\ n>N_1,N_2\Rightarrow\left[\begin{matrix}i>N_1\\ n-i>N_2\end{matrix}\right.\Rightarrow a_ib_{n-i}=0\ \forall i\Rightarrow(ab)_n=0$

**Th.** $S$ – коммутативное кольцо; $f:R\to S$ – гомоморфизм (e.g. $R=S;f=id$); $s\in S$. Тогда $\exists!f_s:R[x]\to S$ продолжающий $f$
$f_s|_R=f;\quad f_s\circ i=f;\quad f_s(x)=s$

**Доказательство**

$g \in R[x] \Rightarrow g = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$
Положим $f_s(g) = f(a_0) + f(a_1)s + f(a_2)s^2 + \ldots f(a_n)s^n$
$f_s(gh) = f_s(g) \cdot f_s(h)$ – муторная проверка
Сложение – очев проверка
Единственность – очев
**Rem.** $f_s$ называется гомоморфизм эвалюоации
**Rem.** $R = S$; $f \to f(s)$ – значение многочлена в точке $S$
$f \in R[x];\ P(f) : R \to R :\ a \to f(a)$ – полиномиальная функция, заданная $f$
Знаем: может быть такое, что $f_1 \neq f_2$, но $P(f_1) = P(f_2)$ (e.g. $x^p$ и $x$ в $Z/pZ$)

Степень многочлена: $f = \sum\limits_{i \in Z_{\geq 0}} a_ix^i$
$deg(f) = max\{i | a_i \neq 0\};\ f \neq 0$
$deg(0) = -\infty$

Свойства степени:

1. $deg(f + g) \leq max(deg(f), deg(g))$

   $deg(f + g) = max(deg(f), deg(g))$ если $deg(f) \neq deg(g)$

2. $deg(fg) = deg(f) + deg(g)$

   $f = \sum a_ix^i;\ g = \sum b_jx^j$

   Тогда $(fg)_s = 0$ при $s > n + m$

   $(fg)_{n+m} = a_{n+m}b_0 + a_{n+m-1}b_1 + \ldots + a_nb_m + a_{n-1}b_{m+1} \ldots = a_nb_m$

   Итого: $(fg)_{n+m} = a_nb_m \neq 0 \Rightarrow deg(fg) = deg(f) + deg(g)$ – но верно только если $R$ – область целостности, т.к. нет делителей нуля

   Далее $R$ – область целостности, еще лучше: $R = K$ – поле

**Следствие:** $R$ – область целостности $\Rightarrow R[x]$ – область целостности

**Th.** О делении с остатком
$K$ – поле, $f, g \in K[x] (g \neq 0)$, тогда $\exists! q, r \in K[x] : f = gq + r;\ deg(r) < deg(g)$
**Def.** $a$ – корень $f$, если $f(a) = 0$
**Th.** Теорема Безу: остаток от деления $f$ на $(x - a)$ равен $f(a)$. В частности $a$ – корень $f \Leftrightarrow f \vdots x - a$

### Доказательство

По теореме о делении с остатком
$f = (x - a)q + r;\ deg(r) < deg(x - a) = 1 \Rightarrow \left[\begin{matrix} deg(r) = 0 \\ r = 0 \end{matrix}\right. \Leftrightarrow r = c \in K$
$f(x) = (x - a)q(x) + k$
$f(a) = (a - a)q(a) + k = k$
TODO
$f = ax^n + f_1;\ f \circ deg(f_1) < n$
$g = bx^m + g_1;\ deg(g_1) < m$
$\tilde{f} = f - \frac{a}{b}x^{n-m}g = ax^n + f_1 - ax^n - \frac{a}{b}x^{n-m}g_1 = f_1 - \frac{a}{b}x^{n-m}g_1$
$deg(\tilde{f}) < n$ по и.п. $\exists \tilde{q}, \tilde{r} : \tilde{f} = g \cdot \tilde{q} + \tilde{r};\ deg(\tilde{r}) < deg(g)$
Тогда $f = \tilde{f} + \frac{a}{b}x^{n-m}g = g(\tilde{q} + \frac{a}{b}x^{n-m}) + \tilde{r}$
Положим $q = \tilde{q} + \frac{a}{b}x^{n-m};\ r = \tilde{r}$

**Th.** $k$ – поле, $f \in k[x],\ deg(f) = n \in Z \Rightarrow f$ имеет не более $n$ корней

### Доказательство

Индукция по n. База $n = 1$ – очев
$n \to n + 1$. $\deg(f) = n + 1$

1. У $f$ 0 корней. $0 \leq n+1$
2. У $f$ есть корень $a \Rightarrow f = (x-a)\tilde{f}$

   $b$ – корень $f \Leftrightarrow (b-a)\tilde{f}(b) = a \Leftrightarrow \left[\begin{aligned} &b-a=0 \\ &\tilde{f}(b)=0 \end{aligned}\right. \Leftrightarrow \left[\begin{aligned} &b=a \\ &b\text{– корень?} \end{aligned}\right.$

   По и.п. $deg(\tilde{f}) = n$. У $\tilde{f}$ не больше $n$ корней, у $f \leq n+1$ корня

**Th.** О формальном и функциональном равенстве

1. $k$ – поле. $f, g \in k[x];\ a_1 \dots a_n \in k;\ n > max(deg(f), deg(g))$

   $f(a_i) = g(a_i) \forall i \Leftrightarrow f = g$
2. $k$ – бесконечно, $f(a) = g(a) \forall a \in k \Rightarrow f = g$

   $1 \Rightarrow 2$ : возьмем любые $a_1 \dots a_n \in k : n > max(deg(f), deg(g))$

**Доказательство**

1. $h := f - g;\ deg(h) \leq max(deg(f), deg(g)) < n$

   При этом $h(a_i) = d(a_i) - g(a_i) = 0;\ a_1 \dots a_n$ – корни $h,\ n > deg(h) \Rightarrow h = 0 \Leftrightarrow f = g$

**Rem.** $f, g \in Z/pZ[x];\ deg(f), deg(g) < p \Rightarrow$ по предыдущей теореме $f \neq g$ как функции
$|\{f | degf < p\}| = |\{a_0 + a_1x + \dots a_{p-1}x^{p-1}\}| = p^p$

Функций: $\begin{cases} f(0) = b_0 \\ f(1) = b_1 \\ \vdots \\ f(p-1) = b_{p-1} \end{cases} \Rightarrow$ всего $p^p$

**Lm.** $a_1, a_2 \dots a_k$ – корни $f : a_i \neq a_j \Rightarrow f \vdots (x-a_1)(x-a_2)\dots(x-a_k)$

# Интерполяция

**Def.** $k$ – поле. Интерполяционные данные $\begin{array}{c|c} x & x_1 \dots x_n \in k \\ \hline f(x) & y_1 \dots y_n \in k \end{array}$ $x_i \neq x_j$

Интерполяционная задача: построить $f \in k[x]$ такую, что $f(x_i) = y_i \forall i$

**Th.**

1. $\forall$ интерполяционная задача имеет решение
2. Оно единственно при ограничении $deg(f) < n$ (а вообще бесконечно много)

**Доказательство**

2. Пусть $f_1, f_2$ – два решения. $deg(f_i) < n$

   По теореме о формальном и функциональном равенстве $f_1 = f_2$ $(f_1(x_i) = y_i = f_2(x_i))$

1. Рассмотрим $L_i(x) = \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)}$

   $L_i = \frac{\prod\limits_{j \neq i}(x-x_j)}{\prod\limits_{j \neq i}(x_i-x_j)}$

   $L_i(x_i) = 1$; при $i \neq j$ $L_i(x_j) = 0$

   $deg(L_i) = n - 1$

   Положим $f = \sum y_i L_i$

   $\forall k\ f(x_k) = \sum y_i L_i(x_k) = y_k L_k(x_k) + \sum y_i L_i(x_k) = y_k$

   Итог: $f = \sum\limits_{i=1}^{n} \frac{y_i \prod\limits_{j \neq i}(x-x_j)}{\prod\limits_{j \neq i}(x_i-x_j)}$ – интерполяционная формула Лагранжа

**Rem.** Это все КТО:

Интерполяционная задача $\Leftrightarrow \begin{cases} f \equiv y_1 \ (mod\ x - x_1) \\ \vdots \\ f \equiv y_n \ (mod\ x - x_n) \end{cases}$

Вернемся к теории чисел
**Th.** $(Z/pZ)^* =< a >$. $\exists a : \{\overline{a}, \overline{a^2}, \overline{a^3} \dots\} = \{\overline{1}, \overline{2} \dots\}$. $a$ – первообразный корень по модулю $p$
Надо доказать: $\exists a \in (Z/pZ)^* : ord(a) = p - 1$
**LmA.** $\forall n \in N \quad \sum\limits_{d|n} \varphi(d) = n$
**Доказательство LmA:**
$\{1, 2, \dots, n\} = A_{d_1} \bigcup A_{d_2} \dots;\ A_d = \{x \le n | (x, n) = d\}$
$|A_d| = |\{dy \le d \cdot \frac{n}{d} | (dy, d\frac{n}{d}) = d\}| = |\{y \le \frac{n}{d} | (y, \frac{n}{d}) = 1\}| = \varphi(\frac{n}{d})$
Тогда $n = |\{1 \dots n\}| = \sum\limits_{d|n} |A_d| = \sum\limits_{d|n} \varphi(\frac{n}{d}) = \sum\limits_{x|n} \varphi(x)$

**LmB.** $\forall d$ – делителя $n$ в $(Z/pZ)^*$ есть либо 0, либо $\varphi(d)$ элементов порядка $d$
**Доказательство LmB:**
Пусть $a \in (Z/pZ)^* : ord(a) = d$
$a^d = 1;\ 1, a, a^2 \dots a^{d-1}$ попарно различны
Заметим: $ord(b) = d \Rightarrow b^d = 1 \Rightarrow b \in \{1, a, a^2 \dots a^{d-1}\}$, так как иначе у многочлена $x^d - 1$ $d$ корней в $Z/pZ$
$b = a^k;\ ord(b) = d;\ b^l \ne 1$ при $l < d \Leftrightarrow a^{kl} \ne 1$ при $l < d \Leftrightarrow kl \not\vdots d$ при $l < d \Leftrightarrow (k, d) = 1 - \varphi(d)$ вариантов

**Доказательство (Th.)**

Докажем: d – делитель $p - 1 \Rightarrow$ в $(Z/pZ)^*$ ровно $\varphi(d)$ элементов порядка $d$ (в частности $d = p - 1 \Rightarrow$ есть элементы порядка $p - 1$)
По LmA. $p - 1 = \sum\limits_{d|p-1} \varphi(d)$, но $p - 1 = |(Z/pZ)^*| = |\bigcup\limits_{d|p-1} B_d| = \sum |B_d|$, где $B_d = \{a | ord(a) = d\}$
$p - 1 = \sum\limits_{d|p-1} |B_d| = \sum\limits_{d|p-1} \varphi(d) \Rightarrow |B_d| = \varphi(d)$. В частности $|B_{p-1}| = \varphi(p-1) > 0$

Хотим ОТА для многочленов ...
**Def.** Область целостности $R$ называется евклидовым кольцом, если $\exists \varphi : R \backslash \{0\} \to Z_{\ge 0}$ (евклидова норма), такая, что $\forall a, b \in R, b \ne 0\ \exists q, r$" $a = bq + r \left[ \begin{array}{l} \varphi(r) < \varphi(b) \\ \quad r = 0 \end{array} \right.$
**Смысл.** В евклидовом кольце можно делать алгоритм евклида (понижая $\varphi$)

**Def.** $R$ – область целостности. $R$ – евклидово, если $\exists \varphi : R \backslash \{0\} \to Z_{\ge 0}$ – евклидова норма
$\forall a, b \in R, b \ne 0;\ \exists q, r : a = b \cdot q + r \left[ \begin{array}{l} \quad r = 0 \\ \varphi(r) < \varphi(b) \end{array} \right.$
**Th.** В евклидовом кольце любой идеал главный

**Доказательство**

$I$ – идеал в $R;\ I \ne \{0\}$ (иначе $I =< 0 >$)
Рассмотрим $i \in I : \varphi(i)$ – минимальна
Тогда $\forall a \in I\ a = q \cdot i + r \left[ \begin{array}{l} \varphi(r) < \varphi(i) \\ \quad r = 0 \end{array} \right.$
Но $r = a - q \cdot i \in I \Rightarrow \varphi(r) \ge \varphi(i)!! \Rightarrow r = 0$, т.е. $a = qi \forall a \in I$, т.е. $I \in < i > \Rightarrow I =< i >$

**Def.** Область целостности в которой любой идеал главный, называется областью главных идеалов (ОГИ)
**Д-ли:** $\forall$ евклидово кольцо
**Rem.** Обратное неверно (сложно)
**Ex.** Пусть $R = Z[x]$, тогда $R$ – не ОГИ
$I =< 2, x >= \{f \in Z[x] | f(0) \vdots 2\}$ – идеал

$I \neq < f >$, т.к. $\left[\begin{array}{l} 2 \vdots f \\ x \vdots f \end{array}\right. \Rightarrow f = \pm 1$, но $\pm 1 \in I$!!! $(2, x) = 1$, но $\nexists g, h : 2 \cdot g + x \cdot h = 1$
$R = Q[x], R[x], Z/pZ[x]$ – все ок, т.к. это поля $\Rightarrow K[x]$ евклидово $\Rightarrow$ ОГИ

**Def.** $R$ – область целостности, $a \vdots b$, если $\exists c : a = bc$
**Rem.** $a \vdots c,\ c \neq 0 \Rightarrow$ частное в определении однозначно (т.к. в области целостности верен закон сохранения)
$Z/4Z,\ 2 = 2 \cdot 1 = 2 \cdot 3$????
**Def.** $a \in R \Rightarrow a$ называется неразложимым, если

1. $a \neq 0,\ a \notin R^*$
2. $a = bc \Rightarrow \left[\begin{array}{l} b \in R^* \\ c \in R^* \end{array}\right.$

**Def.** $a, b$ называются ассоциированными ($a \sim b$), если выполнено одно из определений

1. $a \vdots b,\ b \vdots a$
2. $a = b\varepsilon;\ \varepsilon \in R^*$

**Rem.** В $Z$ $a \sim b \Leftrightarrow |a| = |b|$
**Rem.** Это отношение эквивалентности (очев из первого определения)
**Упражнение:** $3 \Rightarrow 1, 2$ у $a, b$ одинаковые делители
$3'$: у $a, b$ одинаковые кратные

**Def.** Область целостности $R$ называется факториальной, если любой $a \in R \backslash \{0\}$ представляется в виде произведения не разложимых единственным образов с точностью до порядка множителей и ассоциированности
**Ex.** $a = p_1 p_2 p_3;\ p_1, p_2, p_3$ – неразложимые. $\varepsilon, \mu, \alpha \in R^*$
$a = (\varepsilon p_2 \mu)(o_3 \mu^{-1} \alpha^{-1})(\varepsilon^{-1} \alpha p_1);\ \varepsilon p_2 \mu \sim p_2$ – неразложимый (упр) и т.д.
**Th.** ОГИ – факториальна
Ключевые свойства:

1. $\begin{cases} (a, b) = 1 \\ ac \vdots b \end{cases} \Rightarrow c \vdots b$
2. $p$ – неразложимый

   $ab \vdots p \Rightarrow \left[\begin{array}{l} a \vdots p \\ b \vdots p \end{array}\right. \Rightarrow$ единственность разложения

**Доказательство**

Единственность доказывается по той же схеме, что и в $Z$
Существование – неочев /без доказательства/
У нас $R = K[x]$ – существование разложения очевидна (индукция по $deg(f)$)

Что значит в $K[x]$ $f \sim g$? $f = \varepsilon g,\ \varepsilon \in K[x]^*$
**Lem.** $K[x]^* = K \backslash \{0\}$. $deg(f) > 0,\ \forall g\ deg(fg) \geq deg(f) > 0$ или $fg = 0$ $(fg \neq 1)$
Поэтому $f \sim g \Leftrightarrow \exists k \in K^* : f = kg$
$deg(f) = 0,\ f = k \sim 1$, для $f$ разложение пустое ($deg(f) > 0$ – непустое)

**Def.** $f$ называется уникальным, если $\exists n = deg(f) : f = x^n + \sum\limits_{i=0}^{n-1} a_i x^i$
В $\forall$ классе ассоциативности $\exists!$ уникальный многочлен
Итого: $\forall f \in K[x]$ $\exists! a \in K,\ p_1, p_2 \ldots p_l$ – уникальные неразложимые: $f = a p_1 p_2 \ldots p_3$
$p_1, p_2 \ldots p_l$ – единственные с точностью до перестановки множителей

# Производная

**Def.** $R$ – коммутативное кольцо: $D : R \to R$ называется дифференциированием, если

1. $\forall f, g \in R\ D(f+g) = D(f) + D(g)$
2. $\forall f, g \in R\ D(f \cdot g) = f \cdot D(g) + g \cdot D(f)$ – правило Лейбница

**Def.** $R$ – кольцо, $f \in R[x] : f = \sum a_n x^n$ тогда по определению $D(f) = f' = \sum n a_n x^{n-1}$ ($n \cdot a_n = a_n + a_n + \ldots + a_n$ ($n$ раз))
**Def.** $f \in R[x]$. Положим $D(f)(x) = \frac{f(x)-f(y)}{x-y}|_{x=y}$
Упражнение: $def1 \Leftrightarrow def2$
$\frac{ax^n - ay^n}{x-y} = a\frac{(x-y)(x^{n-1}+x^{n-2}y+\ldots+y^{n-1})}{x-y}|_{x=y} = na \cdot y^{n-1}$
**Def./Th.** $K$ – бесконечное поле $f \in K[x],\ a \in K,\ \exists q, r : f = (x-a)^2 \cdot q + r\ (deg(r) < 2)$
$f = (x-a)^2 \cdot q(x) + k(x-a) + m_a\ (x = a;\ m_a = f(a))$
**Утв.** отображение $a \to K_a$ – полиномиальная функция, соответствующий многочлен называется производной (а и менно $f'$ из Def1. задает эту функцию)
**Утв.** $f = (x-a)^2 q_f(x) + f'(a)(x-a) + f(a);\ g = (x-a)^2 q_g(x) + g'(a)(x-a) + g(a)$
Сложим: $f + g = (x-a)^2(q_f + q_g) + (f'(a) + g'(a))(x-a) + f(a) + g(a)$
$f \cdot g = (x-a)^2((x-a)^2 q_f q_g + q_f g'(a)(x-a) + q_g f'(a)(x-a) + f'(a)g'(a)) + (f'(a)g(a) + f(a)g'(a))(x-a) + f(a)g(a)$, но коэффициенты при $x - a$ равен $(fg)'(a)$
Пусть $K$ – поле, $f \in K[x];\ a$ – корень $f$
$a$ – корень кратности $l$, если $V_{(x-a)}(f) = l$, т.е. $f \vdots (x-a)^l,\ f \not\vdots (x-a)^{l+1}$, $f = (x-a)^l \tilde{f} : \tilde{f}(a) \neq 0$
$a$ – кратный корень, если $l > 1$ (иначе простой)
**Th.** $f \in K[x],\ a$ – корень кратности $l$ ($l \geq 1$), тогда

1. $a$ – корень кратности $\geq l - 1$ в многочлене $f'$
2. Если $1 + 1 + \ldots + 1 \neq 0$ в $K \Rightarrow a$ – корень кратности $= l - 1$ в $f'$
3. $a$ – кратный корень $f \Leftrightarrow a$ – корень $gcd(f, f')$

**Доказательство**

1. $f = (x-a)^l \tilde{f};\ \tilde{f}(a) \neq 0$
   $f' = ((x-a)^l)'\tilde{f} + (x-a)^l \tilde{f}' = l(x-a)^{l-1}\tilde{f} + (x-a)^l \tilde{f}' = (x-a)^{l-1}(l\tilde{f} + (x-a)\tilde{f}') \Rightarrow a$ – корень кратности хотя бы $l - 1$
2. $1 \cdot l \neq 0$ в $K$, т.е. $l \neq 0$ в $K \Rightarrow l\tilde{f} \neq 0 \Rightarrow (l\tilde{f}' + (x-a)\tilde{f}')(a) \neq 0$
   т.е. $f' = (x-a)^{l-1} g,\ g(a) \neq 0 \Rightarrow$ кратность ровно $l - 1$

**Ex.** $Z/pZ\ f = x^p$, 0 – корень кратности $p$
$f' = px^{p-1} = 0$ – корень кратности $\infty\ 0 \vdots x^n \forall n$

**Def.** $K$ – поле. Характеристика $K$ – $char(K) = \begin{cases} ord_{(K,+)}(1), \text{ если оно не } \infty \\ 0 \end{cases}$
**Ex.** $char(Q) = char(Z) = 0;\ char(Z/pZ) = p$
**Th.** $char(K) = 0$ или простое число

**Доказательство**

Пусть $n = pq,\ p, q > 1$

Если $n$ единиц $= 0 \Rightarrow$ т.к. $K$ – поле $\Rightarrow$ О.Ц. $\Rightarrow \left[\begin{array}{l} p = 0 \\ q = 0 \end{array}\right. \Rightarrow n$ – не минимальное

**Rem.** Любое поле характеристики 0 содержит подполе, изоморфное $Q$. Поле характеристики $p$ содержит подполе, изоморфное $Z/pZ$

**Th.** $K$ – поле, $a \in K;\ f \in K[x]$, тогда $\exists! a_0, a_1, a_2 \ldots a_n;\ n = degf : f = \sum a_i(x-a)^i;\ f = \sum a_i(x-0)^i = \sum a_i x^i$

**Доказательство**

Индукция по $degf$. База очев
Переход: $n \to n+1$
$f = (x-a)q + f(a)$ по и.п. $q = \sum\limits_{i=0}^{n} b_i(x-a)^i$
$f = (x-a)\sum b_i(x-a)^i + a_0 = \sum b_i(x-a)^{i+1} + a_0$, положим $a_i = b_{i-1}$ при $i > 0$

**Th.** Формула Тейлора:
$K$ – поле, $f \in K[x],\ char(K) = 0$ или $char(K) > degf$
Определим последовательность многочленов: $f^{(0)} = f;\ f^{(n+1)} = (f^{(n)})'$
Тогда $f = \sum \frac{f^{(k)}(a)}{k!}(x-a)^k$

**Доказательство**

Знаем: $f = \sum a_i(x-a)^i$ $(*)$. Хотим $a_i = \frac{f^{(i)}(a)}{i!}$
$((x-a)^k)' = k(x-a)^{k-1}$
Тогда $f = (x-a)^k;\ f^{(1)} = k(x-a)^{k-1};\ f^{(k)} = k!(x-a)^0 = k!;\ f^{(l)} = 0,\ l > k$
Применим к $*$ дифференцирование $k$ раз и эвалюируем в $a$
$f^{(k)}(a) = \sum((a_i(x-a)^i))^{(k)}(a)$
При $i < k:\ ((a_i(x-a)^i))^{(k)}(a) = 0$
При $i > k:\ ((a_i(x-a)^i))^{(k)} = c \cdot (x-a)^{i-k}$. Эвалюация в $a$ дает 0
При $i = k:\ (a_i k!)(a) = a_i k!$
Итого: $f^{(k)}(a) = a_k k! \Rightarrow a_k = \frac{f^{(k)}(a)}{k!}$

# Расширения полей и комплексные числа

Пусть $K$ – поле, $f \in K[x],\ f$ – неразложим, $degf > 1$
Надо $K = Q;\ f = x^2 - 2$
$Q \to Q(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in Q\};\ Q \to R$ – новые поля
$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ – разложение!!!
Хотим уметь строить новое поле $L \supset K$ такое, что в $L$ у $f$ есть корень $\Rightarrow$ раслкадывается на множители
Конструкция: положим $g \equiv h\ (mod\ f)$, если $g - h \,\vdots\, f$
Это отношение эквивалентности и можно перейти к $K[x]/f$ – множество классов эквивалентности
$K[x]/f$ – кольцо вычетов по модулю $f$
**Th.** Упражнение: $f$ – неразложимый многочлен $\Rightarrow K[x]/f$ – поле
$g = f \cdot q + r;\ degr < degf$
$\overline{g} = \overline{r} = \{\overline{a_0 + a_1x + \ldots + a_{n-1}x^{n-1}} | a_i \in K\}$
Все $\overline{a_0}$ – различны и $\overline{a_0} + \overline{a_0'} = \overline{a_0 + a_0'}$ и $\overline{a_0} \cdot \overline{a_0'} = \overline{a_0 \cdot a_0'}$
Можно считать, что $K[x]/f$ содержит $K$ как подполе

$L = K[x]/f$. В $L$ $f$ имеет корень:
$f = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$
$\overline{0} = \overline{f} = \sum \overline{a_i} \cdot \overline{x}^i = \sum \overline{a_i}(\overline{x})^i = \sum a_i\overline{x}^i = f(\overline{x})$
$f$ имеет корень в $L:\ f = (x - \overline{x})(\ldots)$
**Ex. (основной)** $K = R;\ f = x^2 + 1$ – неразложим
$R[x]/(x^2+1) = \{\overline{ax+b} | a, b \in R\}$
$\overline{ax+b} + \overline{cx+d} = \overline{(a+c)x + (b+d)}$
$\overline{ax+b} \cdot \overline{cx+d} = \overline{(ax+b)(cx+d)} = \overline{acx^2 + (ad+bc)x + bd}$ делим на $x^2+1$
Получаем $\overline{acx^2 + ac - ac + (bc+ad)x + bd} = \overline{ac(x^2+1)} + \overline{(bc+ad)x - ac + bd} = \overline{(bc+ad)x - ac + bd}$

$R[x]/(x^2+1) \cong R \times R$ $(\overline{a+bx} \leftrightarrow (a,b))$ со следующими операциями
$(a,b) + (c,d) = (a+c, b+d)$
$(a,b) \cdot (c,d) = (ac - bd, ad + bc)$

$\overline{x} \to (0,1)$
$\overline{x^2} = -1 \to (-1,0);\ \overline{x} = i$
Итого: $C = R[x]/(x^2+1) = \{a+bi|a,b \in R\}$ – поле комплексных чисел

$R = \{a + 0 \cdot i|a \in R\} \subset C$ – подполе $C$
В общем случае $Z = a + bi;\ a = Re(z),\ b = Im(z)$ – вещественная и мнимая часть соответственно
$i$ – мнимая единица
$x^2 + 1 = x^2 - (-1) = x^2 - i^2 = (x-i)(x+i)$

**Следствие.** Любой квадратный трехчлен из $R[x]$ раскладывается на линейные множители в $C$. $f = (x-c)^2 - D = (x - c - \sqrt{D})(x - c + \sqrt{D})$
$D = -k;\ k > 0 \Rightarrow \sqrt{D} = i\sqrt{k}$

**Th.** Основная теорема алгебры: $\forall f \in C[x]\ f = c(x-a_1)\dots(x-a_n)$ – имеет $n$ комплексных корней с учетом кратности

Знаем: существует биекция $R \times R \leftrightarrow$ точки на плоскости
А еще есть биекция $C \leftrightarrow$ точки на плоскости
А еще есть биекция $C \leftrightarrow$ вектора, отложенные из 0
Вот как-то так и думайте, а по-другому не думайте

**Def.** $|a + b_i| = \sqrt{a^2+b^2}$ – модуль комплексного числа
$z \to |\overrightarrow{0x}| = \sqrt{a^2+b^2}$
Симметричный относительно $\overrightarrow{0x}$ вектор $\to a - bi$
**Def.** $\overline{a+bi} = a - bi$ – сопряженное число

Свойства модуля и сопряжения:

1. $\overline{\overline{z}} = z$
2. $z + \overline{z} = 2Re(z)$
3. $z \cdot \overline{z} = |z|^2$

   Резюмируем что-то: $z, \overline{z}$ – корни многочлена $x^2 - 2ax + (a^2+b^2) \in R[x]$
4. $|z_1 z_2| = |z_1| \cdot |z_2| \Leftrightarrow |z_1 z_2|^2 = |z_1|^2 \cdot |z_2|^2 \Leftrightarrow z_1\overline{z_1}z_2\overline{z_2} = (z_1 z_2)(\overline{z_1 z_2})$ – следует из 6
5. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
6. $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

**Rem.** 3) $\Rightarrow C$ – поле, т.к. $z \neq 0 \Rightarrow |z| \neq 0 \Rightarrow z^{-1} = \frac{\overline{z}}{|z|^2}$

$\varphi \in R/z_\varphi = \cos\varphi + i\sin\varphi;\ |z_\varphi| = 1$
Утверждение: $\varphi \to z_\varphi$ – гомоморфизм $(R,+) \to (C,\cdot)$, т.е. $z_{\varphi_1} \cdot z_{\varphi_2} = z_{\varphi_1+\varphi_2}$