

Теория чисел и основные алгебраические структуры

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

Аксиома индукции. $A \subset \mathbb{N}; A \neq \emptyset \Rightarrow$ 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 $a \neq \emptyset$)

Пусть a_0 - наименьшее плохое, значит $a_0 - 1$ - хорошее, можно разделить с остатком

$$a_0 - 1 = b \cdot q + r, 0 \leq r < b, \text{ тогда}$$

$$a_0 = (b \cdot q + r) + 1, r + 1 < b$$

$$a_0 = b \cdot (q + 1), \text{ т.е. } a_0 - \text{хорошее}$$

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'

$$a = b \cdot q + r$$

$$a = b \cdot q' + r'$$

$$a - a = b \cdot q + r - b \cdot q' - r'$$

$$0 = b \cdot (q - q') + (r - r')$$

$$r' - r = b \cdot (q - q'), q \neq q', |q - q'| \geq 1$$

$$|b \cdot (q - q')| \geq |b|$$

$$r', r \in [0; |b| - 1]$$

$$|r - r'| < |b| - 1 \text{ Противоречие } \Rightarrow q = q', r = r'$$

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

Rem. $0 : \forall x \in \mathbb{Z} 0 = 0 \cdot x$

Основные свойства делимости:

1. $0 : a$

2. $a:\dot{1}$
3. $a, b:\dot{c} \Rightarrow a + b:\dot{c}$
4. $a, k:\dot{c} \Rightarrow k \cdot a:\dot{c}$
5. $a:\dot{a}$
6. $a:\dot{b}, b:\dot{a} \Rightarrow a = \pm b$
7. $a:\dot{b}, b:\dot{c} \Rightarrow a:\dot{c}$
8. $ac:\dot{bc}, c \neq 0 \Rightarrow a:\dot{b}$

Доказательство

3. $a:\dot{c} \Rightarrow \exists q_a : a = q_a \cdot c$
 $b:\dot{c} \Rightarrow \exists q_b : b = q_b \cdot c$
 $a + b = (q_a + q_b) \cdot c$
6. $a = bx$
 $b = ay$
 $a = a y x$
 $a = a(xy) \Rightarrow \begin{cases} a = 0, b \neq 0 \\ a \neq 0, xy = 1 \Rightarrow x, y = \pm 1, a = \pm b \end{cases}$
8. $ac:\dot{bc}, c \neq 0$
 $ac = bc \cdot x$
 $c \cdot a = c \cdot bx \Rightarrow a = bx \ (a:\dot{b})$

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. $I \neq \emptyset$
2. $a, b \in I \Rightarrow a + b \in I$
3. $a \in I, k \in \mathbb{Z} \Rightarrow a \cdot k \in I$

Ех. 1 $c \in \mathbb{Z}$

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

Ех. 2 $c_1, c_2 \dots c_k \in \mathbb{Z}$

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

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 $I = \langle b \rangle$

$$\langle b \rangle \subset I, b \in I, k \cdot b \in I$$

$a \in I$ делим с остатком

$$a = bq + r, 0 \leq r < b$$

$$r = a - bq \quad b \in I \Rightarrow -bq \in I \Rightarrow a - bq \in I \Rightarrow r \in I$$

$r \in \mathbb{N}$ - противоречие (b - наименьшее) $\Rightarrow r \notin \mathbb{N} \Rightarrow r = 0$

В частности $\forall a, b \in \mathbb{Z} \exists d : \langle a, b \rangle = \langle d \rangle$

Def. $a, b \in \mathbb{Z}$ НОД(a, b) = $\gcd(a, b) = (a, b)$ - такое $d \in \mathbb{Z}$, что:

$$1. \quad a : d, b : d$$

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

Rem. НОД определен однозначно с точностью до знака

Доказательство

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

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

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

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

$$3. \quad ax + by = c \text{ имеет решение} \Leftrightarrow c : d$$

Доказательство 1

Рассмотрим $I = \langle a, b \rangle$ - по предыдущей теореме он главный

$$\langle d \rangle = \langle a, b \rangle$$

$$d = d \cdot 1 \in I \Rightarrow d \in \langle a, b \rangle, \text{ т.е. } \exists x, y : ax + by = d$$

$$d = (a, b) \begin{cases} a : d \Rightarrow ax : d' \\ b : d \Rightarrow by : d' \end{cases} \Rightarrow d : d'$$

$$a = a \cdot 1 + b \cdot 0 \in \langle a, b \rangle = \langle d \rangle \Leftrightarrow a : d$$

Аналогично $b : d$

Доказательство 3

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

\Leftarrow : Пусть $c : (a, b) = d$, 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. $(a, b) = (a, b - a)$

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

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

Алгоритм Евклида:

1. $a = bq + r_1$
 $b = r_1q + r_2$
 \dots
2. $(a, b) = (r_1, b) = (r_1, r_2) \dots, \exists i \in \mathbb{N} : r_i = 0$
3. $(a, b) = \dots = (r_k, r_k + 1) = (r_k, 0) = r_k$

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

Доказательство

Рассмотрим идеал $\langle a_1, a_2 \dots a_k \rangle \exists d : \langle d \rangle = \langle a_1 \dots a_k \rangle$. 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

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

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

Lm. об отбрасывании взаимнопростого множителя

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

Доказательство

$$ab = cx$$

$$ay + cz = 1 \Rightarrow aby + cbz = b : c$$

Def. $p \in \mathbb{Z}$. p называется простым, если

1. $|p| > 1$
2. $p \neq xy \mid x, |y| < |p|$

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

$$\textbf{Lm. } p - \text{ простое} \Leftrightarrow ab : p \Rightarrow \begin{cases} a : p \\ b : p \end{cases}, |p| > 1$$

Доказательство

$$\Leftarrow p = xy \Rightarrow xy : p \Rightarrow \begin{cases} x : p \\ y : p \end{cases} \Rightarrow \begin{cases} |x| \geq p \\ |y| \geq p \end{cases}$$

$$\Rightarrow \text{Пусть } p - \text{ простое, } ab : p$$

$$\begin{cases} (a, p) = 1 \Rightarrow b : p \\ (a, p) = p \Rightarrow a : p \end{cases}$$

Основная теорема арифметики

$$x \in \mathbb{Z}, x \neq 0$$

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

$$\varepsilon = \text{sgn}(n)$$

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

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

2. Это разложение единственное с точностью до порядка сомножителей

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

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

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

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

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

Доказательство

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

1. Существование:

Пусть есть плохие n (множество плохих непусто)

n_0 - наименьшее плохое

- n_0 - простое

$$p_1 = n_0, s = 1$$

$$n_0 = p_1 \quad ?? \Rightarrow n_0 \text{ - хорошее}$$

- n_0 - составное $\Rightarrow n_0 = n_1 n_2 \quad n_1, n_2 < n_0$

$$n_1, n_2 \text{ - хорошие} \Leftrightarrow \begin{cases} n_1 = p_1 p_2 \dots p_k, p_i \text{ - простое} \\ n_2 = q_1 q_2 \dots q_s, q_i \text{ - простое} \end{cases} \Rightarrow n_0 = n_1 n_2 = p_1 p_2 \dots p_k q_1 q_2 \dots q_s \Rightarrow n_0 \text{ - хорошее}$$

2. Единственность:

Пусть есть плохие n

n_0 - наименьшее из плохих

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

$$p_1 p_2 \dots p_k = n_0 \overset{\cdot}{:} q_1 \Rightarrow \begin{bmatrix} p_1 \overset{\cdot}{:} q_1 \\ p_2 \dots p_k \overset{\cdot}{:} q_1 \end{bmatrix} \Rightarrow \begin{bmatrix} p_1 \overset{\cdot}{:} q_1 \\ p_2 \overset{\cdot}{:} q_1 \\ p_3 \dots p_k \overset{\cdot}{:} q_1 \end{bmatrix} \Rightarrow \dots \Rightarrow \begin{bmatrix} p_1 \overset{\cdot}{:} q_1 \\ p_2 \overset{\cdot}{:} q_1 \\ \dots \\ p_k \overset{\cdot}{:} q_1 \end{bmatrix}$$

$$\exists p_i \overset{\cdot}{:} q_1$$

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

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

$n = \varepsilon p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, p_1 < p_2 < \dots < p_k$ - каноническое разложение

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}, \text{ почти все } v_p(n) = 0$$

$v_p(n)$ - степень 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 $a \nmid p^n, a \mid p^{n+1}$

Доказательство

1. Напишем разложения:

$$a = p^{v_p(a)} \cdot \prod_{q \neq p} q^{v_q(a)}$$

$$b = p^{v_p(b)} \cdot \prod_{q \neq p} q^{v_q(b)}$$

$$ab = p^{v_p(a)+v_p(b)} \cdot \prod_{q \neq p} q^{v_q(a)+v_q(b)}$$

$$a = p^n x, b = p^m y$$

$$\text{НУО } n \geq m$$

$$a+b = p^m p^{n-m} x + p^m y = p^m (p^{n-m} x + y) \mid p^m = p^{\min(n,m)}$$

$$n \neq m \quad p^{n-m} x \nmid p \Rightarrow p^{n-m} x + y \nmid p \Rightarrow p^m (p^{n-m} x + y) \nmid p^{m+1}$$

$$m = v_p(a+b)$$

Следствия из ОТА

Утверждение: $a = \prod_{p_i \in \mathbb{P}} p_i^{a_i}, b = \prod_{p_i \in \mathbb{P}} p_i^{b_i}$

Тогда

- $a \mid b \Leftrightarrow a_i \geq b_i \forall i$
- $\exists c : a = c^k \Leftrightarrow a_i \mid k \forall i$
- Число a имеет $\tau(a) = \prod (a_i + 1)$ натуральных делителей

Доказательство

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

- $$b_1 \in \{0, 1 \dots a_1\}$$

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

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

- $c \mid a, c \mid b$
- $c' \mid a, c' \mid b \Rightarrow c' \mid c$

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

$$1. \min(a_i, b_i) \leq a_i$$

$$\prod_{p_i^{a_i}} p_i^{a_i} : \prod_{p_i^{\min(a_i, b_i)}} p_i^{\min(a_i, b_i)}, \text{ т.е. } a, b : \prod_{p_i^{\min(a_i, b_i)}} p_i^{\min(a_i, b_i)}$$

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

2. НОК - аналогично

Отступление

Решаем диофантовы уравнения

$x^2 - y^2 = 100 \Rightarrow (x - y)(x + y) = 2^2 \cdot 5^2 \Rightarrow$ 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. Нейтральный 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 (?)

- $a * x = b * x$

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

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

$$a * e = b * e$$

$$a = b$$
- $a * x = b$

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

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

$$e * x = a^{-1} * b$$

$$x = a^{-1} * b$$
- $x * a = b$

$$\dots$$

$$x = b * a^{-1}$$

Главный пример ассоциативной, но не коммутативной операции – композиция

$$f : A \rightarrow B$$

$$\{(a, f(a)) \mid \begin{matrix} a \in A \\ f(a) \in B \end{matrix}\}$$

$$g : B \rightarrow C$$

$$b \in B; g(b) \in C$$

$$a \rightarrow f(a) \rightarrow g(f(a)) \in C$$

$$g \circ f : A \rightarrow C$$

$$(g \circ f)(x) = g(f(x)) \quad \forall x \in A$$

Rem. Если $C \neq A$, то $f \circ g$ не существует

$$A \rightarrow B \rightarrow C \rightarrow D$$

$$h \circ (g \circ f) : A \rightarrow D$$

$$(h \circ g) \circ f : A \rightarrow D$$

$$\text{и } h \circ (g \circ f) = (h \circ g) \circ f$$

$$\forall a \in A \quad (h \circ (g \circ f))(a) = h(g \circ f)(a) = h(g(f(a))) = ((h \circ g) \circ f)(a)$$

Def. M – множество

$$End(M) = \{f : M \rightarrow M\}$$

Тогда на $End(M)$ определена бинарная ассоциативная операция \circ

$$f, g : M \rightarrow M; f \circ g : M \rightarrow M \rightarrow M$$

$End(M)$ замкнуто относительно композиции

Аксиомы:

1. Ассоциативность есть

$$2. id_m(x) = x \quad \forall x \in M$$

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

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

$$\text{Т.е. } f \circ id = f \text{ и } id \circ f = f$$

id_m – нейтральный элемент

Rem. Если в определение группы взять только аксиомы 1 и 2, то G – моноид. $End(M)$ – моноид

$$fix \quad f(x) = a$$

$$g(f(x)) = f(a) = fix$$

$$g \circ f \neq id_m \quad \forall g$$

Th. $f : M \rightarrow M$ имеет обратное $\Leftrightarrow f$ – биекция

Т.е. $\forall y \in M \quad f(x) = y$ 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

$$S(M) \subset End(M)$$

$$S(M) = \{f \in End(M) \mid f \text{ – биекция}\}$$

$S(M)$ – симметрическая группа на множестве M , группа относительно \circ

Rem. id – биекция; $id^{-1} = id$

$$M = \{1, 2 \dots n\}$$

$S(M) = S_n$ – 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

$$\bullet \quad a + b = b + a$$

- $(a + b) + c = a + (b + c)$
 - $\exists 0 : a + 0 = a$
 - $\forall a \exists (-a) : a + (-a) = 0$
5. $a \cdot (b + c) = a \cdot b + a \cdot c$ – дистрибутивность
 $(b + c) \cdot a = b \cdot a + c \cdot a$
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 $\Rightarrow \forall a, b \neq 0 \dot{a} \dot{b}$

$$a = b \cdot \frac{a}{b} = b(a \cdot b^{-1})$$

Значит бессмысленны понятия простых, разложения на простые

Кольца вычетов

$M, \{(a, b)\} \subset M \times M$ – отношения 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 – отношения эквивалентности

$a \in M$

$\bar{a} = \{b \in M | aRb\}$ – класс эквивалентности a

Th. Любые два класса эквивалентности $\bar{a}, \bar{b} : \begin{cases} \bar{a} \cap \bar{b} = \emptyset \\ \bar{a} = \bar{b} \end{cases}$

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

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

Доказательство

P: $a - a = 0 \dot{n} \Rightarrow a = a$

C: $a \equiv b \Rightarrow a - b \dot{n} \Rightarrow b - a \dot{n} \Rightarrow b \equiv a$

$$\text{T: } \begin{cases} a \equiv b \\ b \equiv c \end{cases} \Rightarrow \begin{cases} a - b \equiv 0 \\ b - c \equiv 0 \end{cases} \Rightarrow a - c = (a - b) + (b - c) \equiv 0 \Rightarrow a \equiv c$$

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

Доказательство

\Leftarrow Упражнение

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

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

Элементы \mathbb{Z}/\equiv – вычеты (классы вычетов) по модулю n

$$\bar{3} = \{3; 3 \pm n; 3 \pm 2n \dots\}$$

Из Rem $\Rightarrow |\mathbb{Z}/\equiv| = n$

$$\mathbb{Z}/\equiv = \{\bar{0}; \bar{1} \dots \overline{n-1}\}$$

Обозначается $\mathbb{Z}/n\mathbb{Z}$

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

$$1. (a + c) - (b + d) = (a - b) + (c - d) \equiv 0$$

$$2. ac \equiv bc, \text{ т.к. } ac - bc = c(a - b) \equiv 0$$

$$ad \equiv bd, \text{ т.к. } ad - bd = d(a - b) \equiv 0$$

По транзитивности $ac \equiv bc \equiv bd$

$$a \equiv b \Leftrightarrow \bar{a} = \bar{b} \text{ в } \mathbb{Z}/n\mathbb{Z}$$