

Алгебра и теория чисел

Иванова Ольга Юрьевна¹

08.09.2023 - ...

¹"Записал Сергей Киселев, Гараев Тагир"

Оглавление

1	Множества	2
1.1	Операции над множествами	2
1.2	Отображения	7
1.3	Бинарные отношения	16
1.4	Множество с алгебраическими операциями	23
1.5	Группы	25
1.6	Группы	25
1.7	Кольца и поля	26
2	Теория чисел	28
2.1	Алгоритм Евклида	28
2.2	Алгоритм Евклида	29
2.3	Линейное представление НОД	30
2.4	Простые числа	30
2.5	Основная теорема арифметики	32
2.6	Степень вхождения простого числа	33
3	Сравнения и классы вычетов	34

Глава 1

Множества

Лекция 1: Операции над множествами

08.09.2023

1.1 Операции над множествами

Обозначение. $x \in A$ означает, что элемент x принадлежит множеству A .

$x \notin A$ означает, что элемент x не принадлежит множеству A .

Определение 1. \emptyset , пустое множество - множество, не содержащее ни одного элемента.

Определение 2. Множество B называют подмножеством A , если любой элемент B принадлежит A .

Обозначение. $B \subset A$

Пример. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Операции.

1. Пересечение множеств A и B - это множество из элементов принадлежащих A и B .

Обозначение. $A \cap B$

2. Объединение множеств A и B - множество из элементов A или B .

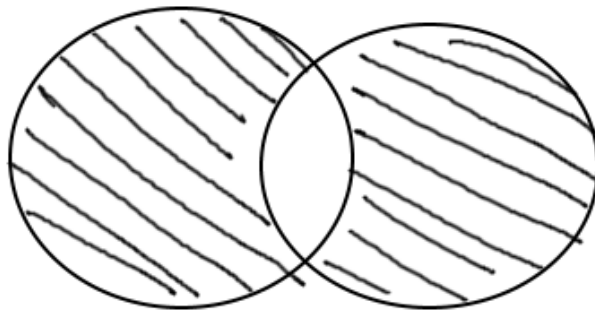
Обозначение. $A \cup B$

3. Разность множеств A и B - множество элементов A , не принадлежащих B .

Обозначение. $A \setminus B$

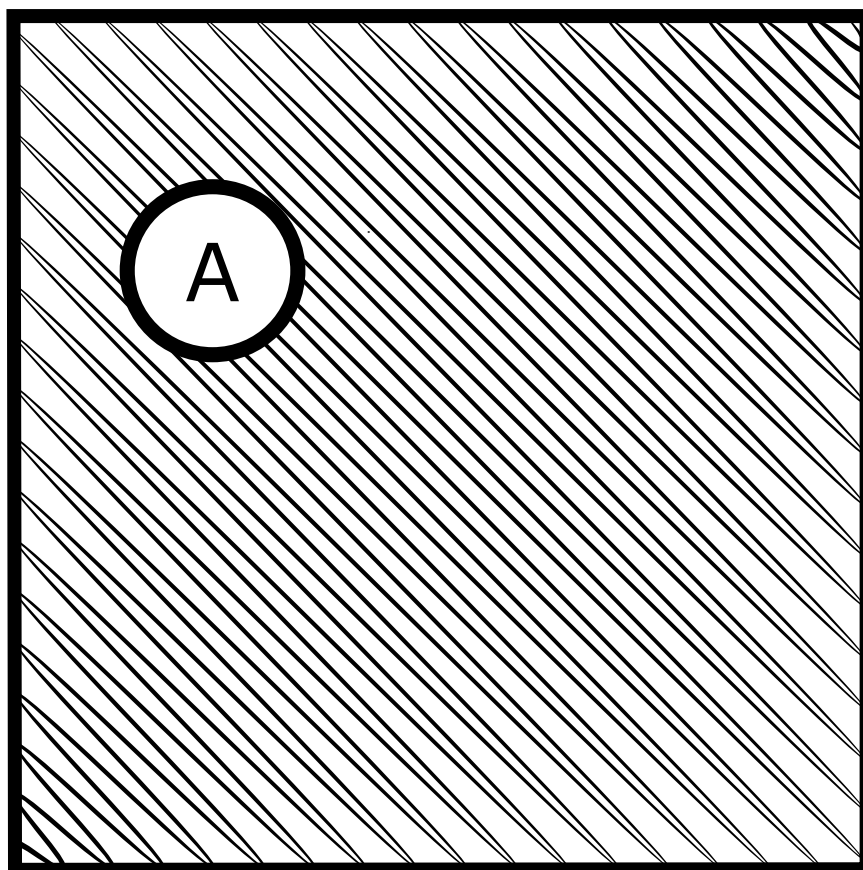
4. Симметрическая разность

Пример. $A \Delta B = (A \setminus B) \cup (B \setminus A)$
 $A \Delta B = (A \cup B) \setminus (A \cap B)$



5. Дополнение

Если предположить, что все множества являются подмножествами некоторого универсального множества, дополнение множества A - это множество элементов U , не принадлежащих A .



Пример. $U = \mathbb{Z}$

A - множество чётных чисел

\overline{A} - множество нечётных чисел

Порядок действий

1. Дополнение
2. Пересечение
3. Объединение, разность, симметрическая разность

Приоритет слева направо.

Пример. $U = \{1, 2, 3, 4, 5\}$ $A = \{1, 2, 3\}$ $B = \{3, 4\}$ $C = \{4, 5\}$

$A \cup B \cap \overline{C} \setminus \overline{B}$

1. $\overline{C} = \{1, 2, 3\}$
2. $\overline{B} = \{1, 2, 5\}$
3. $B \cap \overline{C} = \{3\}$

$$4. A \cup B \cap \overline{C} = \{1, 2, 3\}$$

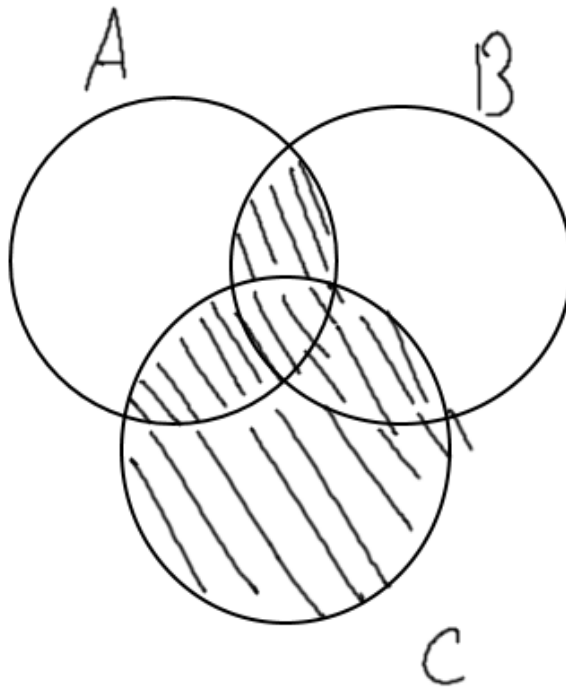
$$5. A \cup B \cap \overline{C} \setminus \overline{B} = \{3\}$$

$$6. \dots = \{1, 2, 4, 5\}$$

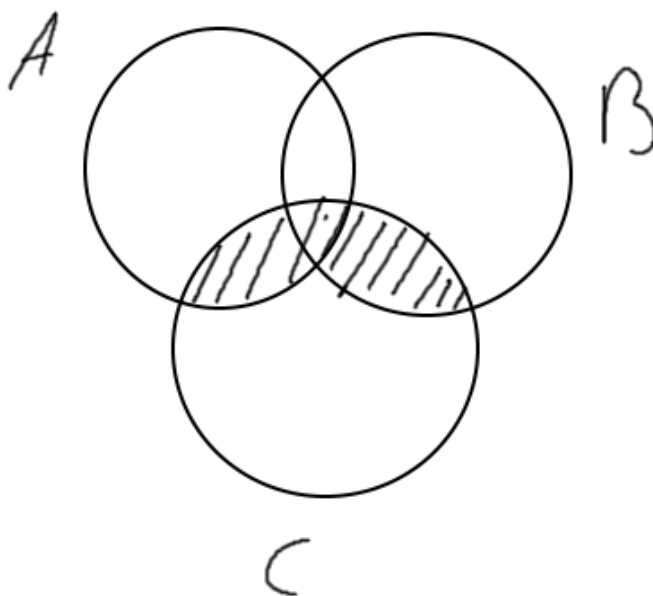
Свойства:

1. Дистрибутивность

$$(a) (A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$



$$(b) (A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$



Доказательство. Положим $D = (A \cap B) \cup C$

$$E = (A \cup C) \cap (B \cup C)$$

Докажем, что $C \subset E$

Пусть $x \in D$, тогда выполняется

(a) $x \in A \cup B$ или

(b) $x \in C$

Если выполнено 1, то $x \in A \cup B \Rightarrow x \in A \Rightarrow x \in A \cup C \in A \cap B \Rightarrow x \in B \Rightarrow x \in B \cup C \Rightarrow x \in (A \cup C) \cap (B \cup C)$

Если выполнено 2, то $x \in C \Rightarrow x \in A \cup C \Rightarrow x \in (A \cup C) \cap (B \cup C)$

$$x \in C \Rightarrow x \in B \cup C$$

$$x \in E \Rightarrow x \in A \cup C \text{ и } x \in B \cup C$$

Случай 1. $x \notin C$

- $x \notin C, x \in A \cup C \Rightarrow x \in A$

$$\bullet x \notin C, x \in B \cup C \Rightarrow x \in B$$

$$\Rightarrow x \in A \cap B = .x \in B$$

Случай 2. $x \in C$

$$\Rightarrow x \in (A \cap B) \cup C \Rightarrow x \in D$$

□

2. Законы де Моргана

$$(a) \overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$(b) \overline{A \cap B} = \overline{A} \cup \overline{B}$$

Прямым или декартовым произведением множеств A и B называют множество упорядоченных пар (a, b) , где $a \in A, b \in B$

Обозначение. $A \times B$

Пример. 1. $A = \{1, 2\}, B = \{x, y\}$

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$$

2. $A = \{1, 2\}, B = \{1\}$

$$A \times B = \{(x, y) | x, y \in \mathbb{R}\}$$

3. $A = B = \mathbb{R}$

$$A \times B = \{(x, y) | x, y \in \mathbb{R}\}$$

Св-во: между элементами множеств $(A \times B) \times C$ и $A \times (B \times C)$ есть взаимно однозначное соответствие.

Определение 3. $A \times B \times C$ - Это $(A \times B) \times C$

$$A^n = A \times A \times \dots A$$

Пример. $0, 1^3$ элементов $(0,0,0), (0,0,1), \dots, (1,1,1)$

1.2 Отображения

Определение 4. Отображением или функцией из множества X в множество Y называют правило, которое каждому элементу множества X сопоставляет ровно один элемент из множества Y .

Пример. 1. $X = \{a, b, c, d\} Y = \{1, 2, 3\}$

$$f(a) = 1$$

$$f(b) = 2$$

$$f(c) = 1$$

$$f(d) = 1$$

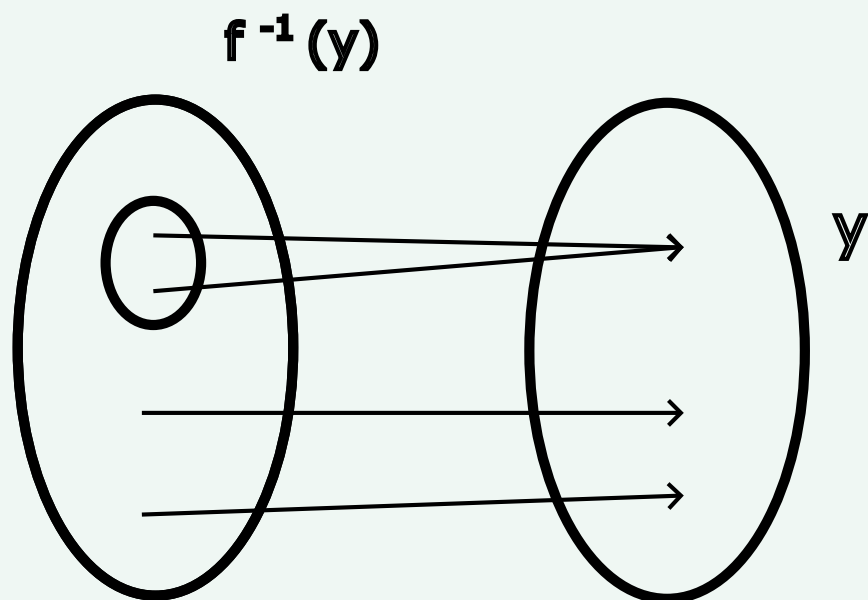
$$2. X = Y = \mathbb{R}$$

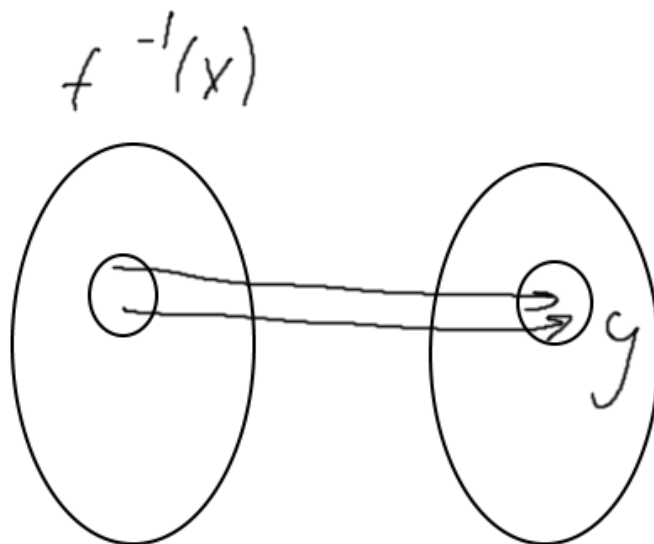
$$f(x) = x^2 =$$

Определение 5. Образом отображения f называют множество элементов $f(x)$ т.к. $\{f(x) | x \in X\}$

Обозначение. $Im f, f(X)$

Определение 6. Прообразом элемента $y \in Y$ называют множество элементов множества X , которые переходят в y , т.е.
 $\{x \in X | f(x) = y\}$



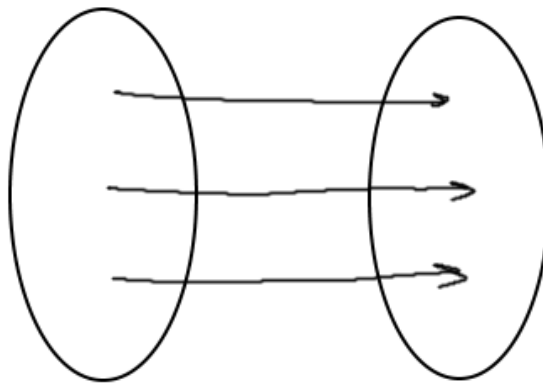


Обозначение. $f^{-1}(y)$

Если $y_1 \subset y$, то

$$f^{-1}(y_1) = \{x \in X \mid f(x) \in y_1\}$$

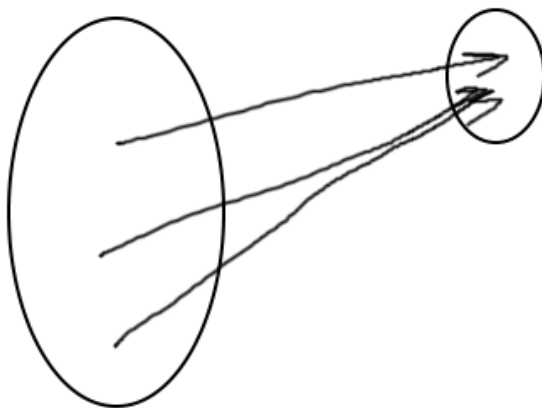
Определение 7. Отображением f называют инъективным, если прообраз любого элемента содержит не более одного элемента.



Др. названия:

- f - инъекция
- f является отображением в

Определение 8. Отображение f называется сюръективным, если если прообраз любого элемента содержит хотя бы один элемент.



Др. названия:

- f - сюръекция
- f является отображением на

Определение 9. Отображение f называется биективным, если прообраз любого элемента состоит ровно из одного элемента.

Др. названия:

- f - биекция
- f - взаимно однозначное отображение

Замечание. f биекция $\Leftrightarrow f$ - инъекция и сюръекция.

Пример. $f : \mathbb{Z} \rightarrow \mathbb{Z}$

1. $f(x) = x + 1$ - биекция
2. $f(x) = x^2$ - не инъекция, не биекция

$$f^{-1}(4) = \{2, -2\}$$

$$f^{-1}(5) = \emptyset$$

$$\alpha \subset 2$$

3. $f(x) = 2x$ - инъекция, не сюръекция

$$f^{-1} = \emptyset$$

$$x_1 \neq x_2 \Rightarrow 2x_1 \neq 2x_2$$

4. $f(x) = \left[\frac{x}{2}\right]$ не инъекция

$$\left[\frac{0}{2}\right] = \left[\frac{1}{2}\right]$$

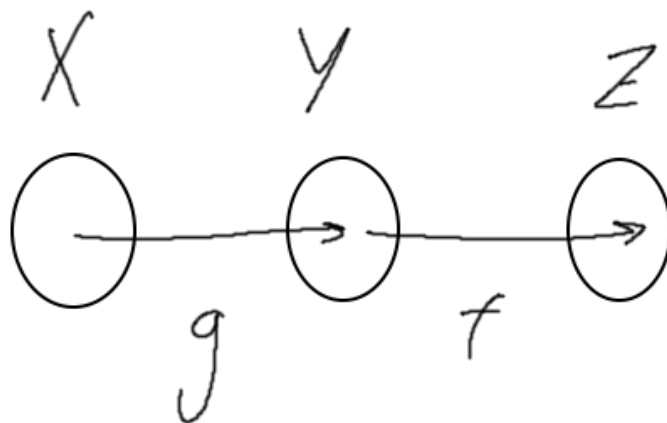
$$2n \in f^{-1}(n)$$

\Rightarrow

$$f^{-1}(n) \neq \emptyset$$

Определение 10. Тожественное отображение $e_x : x \rightarrow x, e_x(x) = x$

Определение 11. Пусть $g : X \rightarrow Y, f : Y \rightarrow Z$



отображение композиция fog определяется как
 $(fog)(x) = f(g(x))$

Пример. $X = Y = \mathbb{Z} = \mathbb{R}$

$$f(x) = x + 1, y(x) = x$$

$$(fog)(x) = x^2 + 1$$

$$(gof)(x) = (x + 1)^2$$

Замечание. $(fog)oh = fo(goh)$

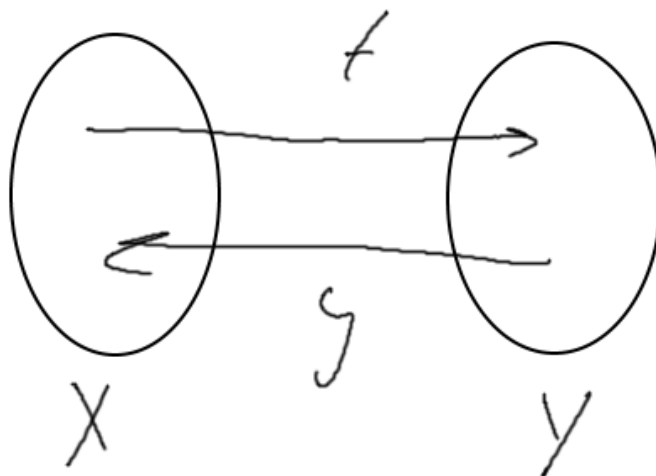
Обозначение. $fogoh$

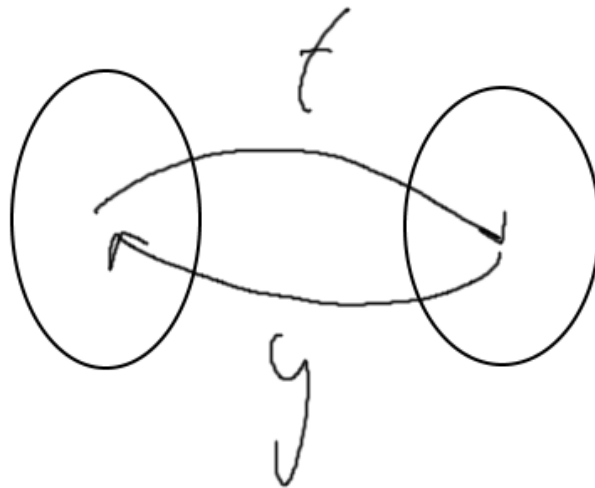
Определение 12. Пусть $f : X \rightarrow Y, g : Y \rightarrow X$

Отображение g называют обратным к отображению f , если

$$fog = e$$

$$gof = e$$





Пример. $X = Y = [0; +\infty]$
 $f(x) = x^2, y(x) = \sqrt{x}$

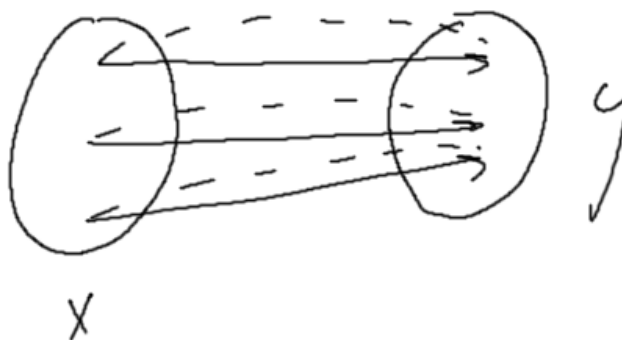
Определение 13. Обратное отображение к f обозначается f^{-1}
(Корректность, т.е. единственность отображения обратных -
ниже)

Теорема 1. (Существование обр. отображения)

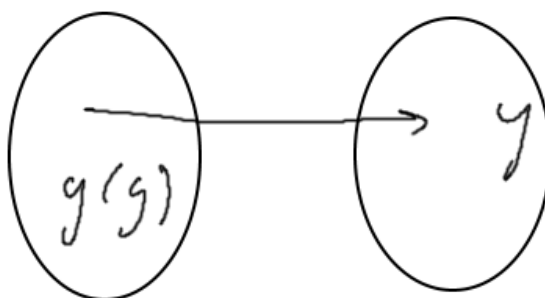
Обратное отображение к f существует тогда и только тогда, когда f является биекцией.

Доказательство. 1. Доказать, что если f биекция, то существует y , обратное к f

Пусть $y \in X \exists! x$, такой, что $f(x) = y$



Положим $y(y) = x$



Теорема 2. (Единственности обратного отображения)

Пусть f - Биекция $X \rightarrow Y$. Тогда не существует различных отображений y_1, y_2 являющихся обратными к f .

Доказательство. Доказательство: Упражнение! □

Лекция 2: Бинарные отношения

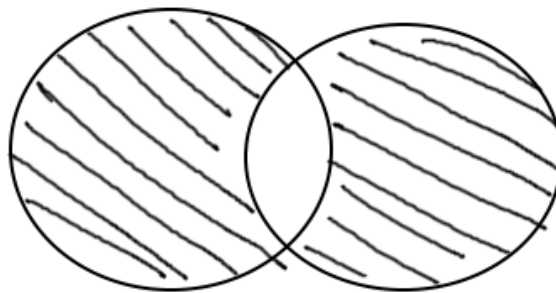
15.09.2023

1.3 Бинарные отношения

Определение 14. Бинарным отношением между множествами X и Y называют подмножество $X \times Y$

Обозначение. Пусть задано $w \subset X \times Y$. Тогда, условие $(x, y) \in w$ записывается как xwY

Обозначение. Если $X = Y$, то говорят, что w - отношение на X .



Доказательство. Пусть g_1, g_2 - отображения к \mathbb{R} .

$$q_1 \neq q_2$$

$$\exists g : g, (g) \neq g = (g)$$

$$x_i = y_1(y), x_2 := g_2(y)$$

$$f(x_1) = f(g_1(y)) = g = f(g_2(y)) = f(x_2)$$

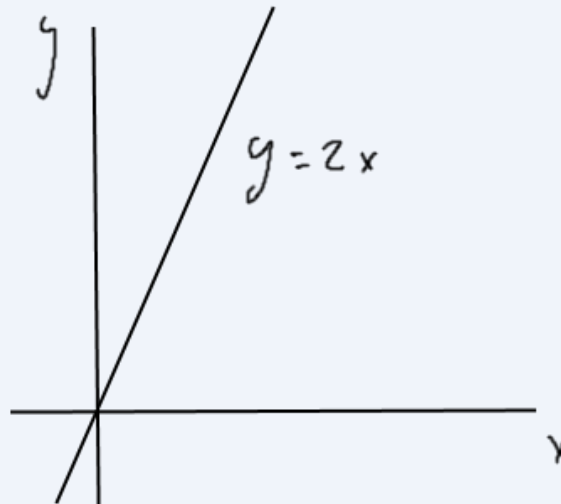
$$f(x_1) = f(x_2)$$

$$x_1 \neq x_2$$

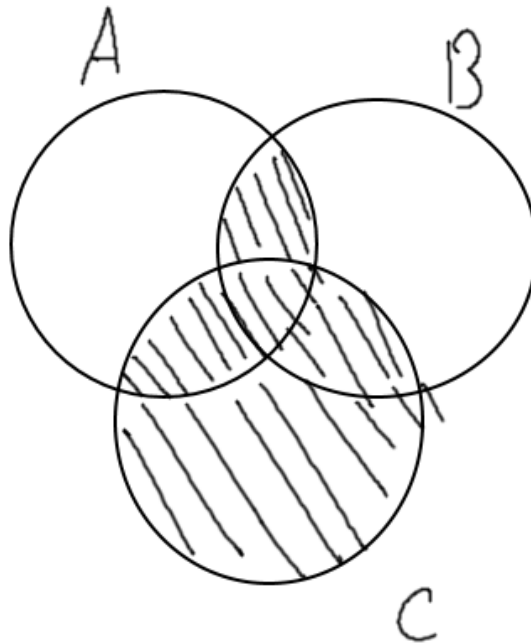
□

Пример. 1. $f(x) = 2x$

xwy , если $g = f(x)$



2. xwy , если $x^2 = y$



Определение 15. Бинарное отношения w на X называется

1. Рефлексивным, если xwy и ywz
2. Симметричным, если из того что xwy и ywz следует, что xwf

Пример. 1. $=, \leq$ - рефлексивное

$<$, параллельно на множестве прямых - не рефлексивно

2. $=, ||$ - симметрично

$leq, <$ - не симметрично

3. $=, <, \dot{<}$ - транзитивно

\perp - на множестве прямых - не транзитивно

Определение 16. Бинарное отношение на множестве X называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Обозначение. Обычно обозначается \sim .

Пример. 1. $=$ на \mathbb{R}

2. Множество \mathbb{Z} $a \sim b$, если $a - b \in 5\mathbb{Z}$

Обозначение. \equiv

3. Множество прямых на плоскости $l_1 \sim l_2$, если $l_2 \parallel l_1'$, если $L_1 = l_2$

4. Пусть множество \mathcal{L} - это множество направленных отрезков $\overline{AB} \sim \overline{CD}$, если $|\overline{AB}| = |\overline{CD}|$, $AB \parallel CD$.

5. $f(x), g(x)$ - функции $f \sim g$, если $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$

Определение 17. Пусть на X задано отношение эквивалентности. Классом эквивалентности x называется множество элементов $\{y \in X \mid y \sim x\}$.

Обозначение. $\bar{x}, [x], ((x))$

Примечание. Черта над x должна быть немного загнута вниз слева. Также первый вариант обозначения является основным.

Пример. $\mathbb{R}, x \sim y, x - y \in \mathbb{Z}$

$$x = 0, 1$$

$$0, 1; 1, 1; -0.9 \in \bar{x}$$

$$\bar{x} = \{y \mid \{y\} = \{x\}\}$$

Пример. $1, 1 \in \overline{0, 1}$

$$0, 1 \in \overline{1, 1}$$

$$\{y\} = 0, 1$$

5 классов эквивалентности:

$$5k$$

$$5k + 1$$

$$5k + 2$$

$$5k + 3$$

$$5k + 4$$

Теорема 3. (Разбиение на классы эквивалентности) На множестве X задано отношение эквивалентности. Тогда, множество X разбивается на классы эквивалентности, т.е. X является объединением не пересекающихся подмножеств, каждое из которых является классом эквивалентности некоторого элемента.

Пример. 1. \equiv_5

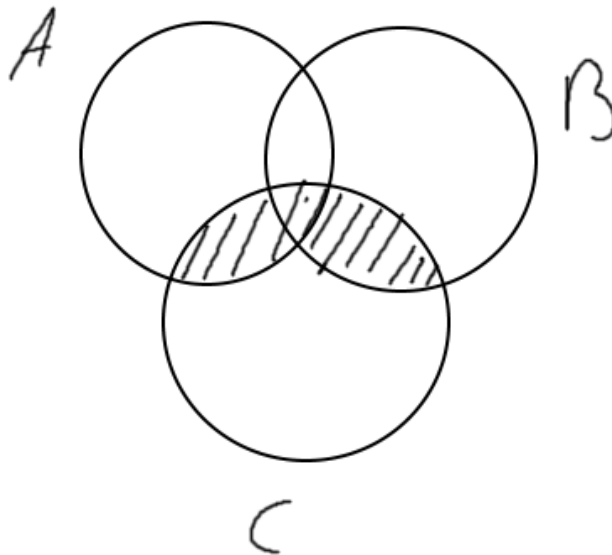
$a \sim b$, если $a - b \vdots 5$

2. = в каждом классе 1 элемент

3. Направленные отрезки $\overline{AB} \sim \overline{CD}$, если $|\overline{AB}| = |\overline{CD}|$,
 $AB \uparrow\uparrow CD$

Класс эквивалентности - вектор.

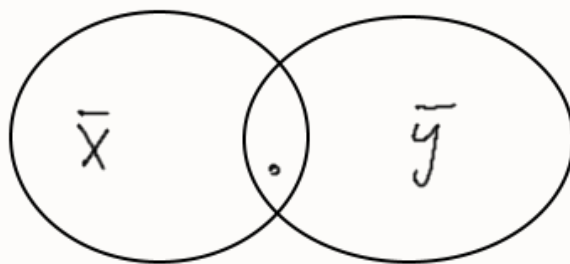
4. $\mathbb{R} a \sim b$, если $\alpha - \beta = 2\pi k$



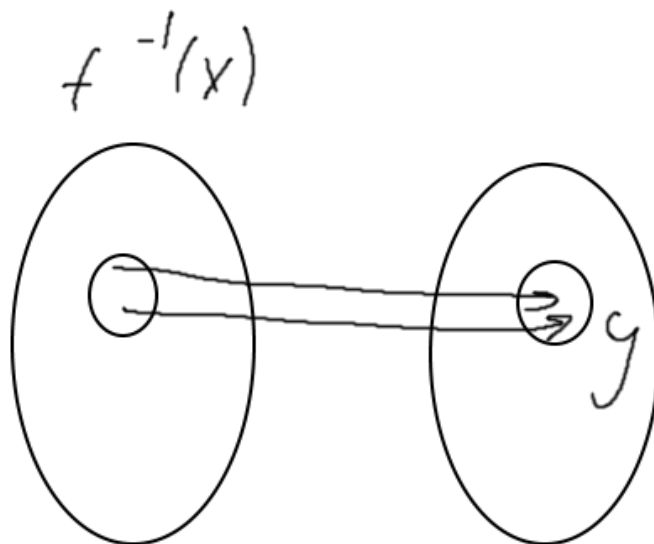
Доказательство. 1. Докажем, что любой элемент X принадлежит некоторому классу эквивалентности.

$X \in \overline{X}$, т.к. $\sim ???$, $X \sim X$

2. Докажем, что классы не пересекаются



т.е. докажем, что если $\exists z \in \bar{x} \cap \bar{y}$, то $\bar{x} = \bar{y}$

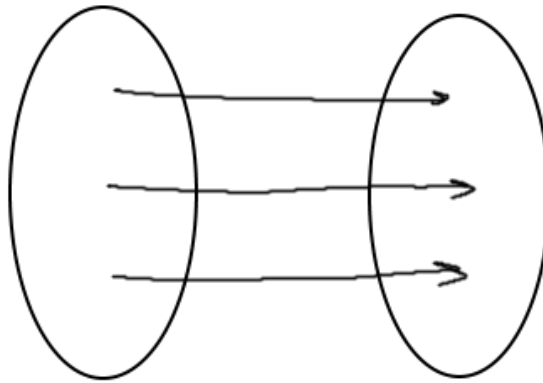


$$z \in x \Rightarrow z \sim x \Rightarrow (\text{симм}) x \sim z$$

$$z \in \bar{y} \Rightarrow z \notin Y$$

$$x \notin z, z \notin y \Rightarrow (\text{тр}) x \notin y \Rightarrow x \in y \Rightarrow x \in \bar{y}$$

$$\text{аналогично } y \in \bar{x}$$



$$x = \bar{y}$$

Докажем, что $\bar{x} \subset y$

Пусть $\exists f \in \bar{x} \Rightarrow f \sim x$

$f \sim x, x = y \Rightarrow f \sim y$

Аналогично $\bar{y} \subset \bar{x}$

$$\bar{x} = \bar{y}$$

□

1.4 Множество с алгебраическими операциями

Определение 18. X - множество бинарной алгебраической операции на X Называется отображением $X \times X \rightarrow X$

Обозначение. 1. Буква, например $f : X \times X \rightarrow X$ пишут $f(x, y)$ или xfy

2. Спец. символ: $+$, \cdot , 0 , $*$ Пишут $x + y$, $x \cdot y$
часто вместо $x \cdot y$, $x * y$ пишут xu

Пример. 1. $X = \mathbb{Z}$

Определить $+$, \cdot , $-$

2. X - множество отображений $\mathbb{Z} \rightarrow \mathbb{Z}$,

операция - композиция.

3. X - множество векторов

Обозначение. Множество X с операцией V обозначается $(V, *)$

Определение 19. Бинарная операция $*$ на X Называется

1. Ассоциативной, если $(x * y * z) = x * (y * z) \forall x, y, z$

2. Коммутативной, если $x * y = y * x \forall x, y$

Пример. 1. $+$, \cdot - коммутативные, ассоциативные

$X : y$ на $\mathbb{R} \setminus \{0\}$ не ассоциативно, не коммутативно

$x - y$ на \mathbb{R}

x - векторное произведение

2. ассоциативны, не коммутативны \circ - композиция для отображения

$\mathbb{Z} \rightarrow \mathbb{Z}$

Обозначение. Пусть $*$ - ассоциативно

Тогда пишут $a * b * c$, $a * b * c * d$

Используют обозначение степени, например $a^4 = a * a * a * a$

Если операция обозначается $+$, пишут

$4a = a + a + a + a$

Пример. 1. $(\mathbb{Z}, \cdot) e = 1$

2. $(\mathbb{Z}, +) e = 0$

3. $(2\mathbb{Z}, \cdot)$ нет ? элемента, множества четных чисел

Замечание. Если операция обозначается $+$, то нейтральный элемент обозначается 0 .

Свойство. (единственности единичного элемента)

На x задана операция $*$. Тогда существует не более одного единичного элемента.

Доказательство. Пусть e_1, e_2 - единичные, т.е.

$\forall x \ e_1 + x = x, x + e_1 = x \ e_2 * x = x, x * e_2 = x$

$$e_2 = (\text{ед. эл.})e_1 * e_2 = (\text{ед.эл.})e_1 \Rightarrow e_1 = e_2$$

□

Определение 20. Полугруппой называется множество с заданной на нем бинарной ассоциативной операцией.

Определение 21. Моноидом называется полугруппа, в которой есть нейтральный элемент

- Пример.**
1. $(\mathbb{Z}, +)$ - моноид
 2. (\mathbb{Z}, \cdot) - моноид
 3. $(2\mathbb{Z}, \cdot)$ - полугруппа, не моноид
 4. $(\mathbb{Z}, -)$ - вектор $\subset x$ - не полугруппа

1.5 Группы

Определение 22. Множество G с бинарной операцией $*$ называется группой, если выполнены следующие условия.

1. Операция $*$ ассоциативна, т.е. $(a * b) * c = a * (b * c) \forall a, b, c$
2. \exists единица $e : a * e = e * a = a \forall a$
3. $\forall a \exists$ Обратный элемент $a' \in G$ такой, что $a * a^{-1} = a^{-1} * a = e$

Обозначение. Если операция обозначается -1 , то единичные элементы обозначаются o , а обратный элемент a обозначается $-a$.

Определение 23. Пусть $(G, *)$ - группа, если $*$ коммутативна, то группа G называется коммутативной или абелевой.

Лекция 3: Группы, кольца, поля и теория чисел

22.09.2023

1.6 Группы

- Пример.**
1. $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$ - абелева группа
аналогично с $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}_+^*$
 2. $(\mathbb{R}, +)$ - абелева
 3. пусть X - множество, G - множество биекций $X \Rightarrow X$, \circ - композиция, тогда G - группа

4. Группа движений плоскости, операция - \circ
5. пусть X - множество, тогда $(2^X, \Delta)$ - группа (доказать)

Свойство. (сокращение), G - группа, $a, b, c \in G$

1. если $ac = bc \Rightarrow a = b$
2. если $ca = cb \Rightarrow a = b$

Доказательство. $ac = bc \xRightarrow{\exists c^{-1}} (ac)c^{-1} = (bc)c^{-1} \xRightarrow{\text{ассоц.}} a(cc^{-1}) = b(cc^{-1}) \Rightarrow ae = be \Rightarrow a = b$ Q.E.D. □

Определение 24. Группы G и H - изоморфны, если \exists биекция из G в H , т.ч. $\forall x, y \in G : f(x \cdot y) = f(x) * f(y)$ где \cdot - операция G , $*$ - операция H

Обозначение. $G \cong H$, f - изоморфизм

Пример. $G(\mathbb{R}, +) \cong H(\mathbb{R}_+^*, \cdot)$ $f(x) = 2^x$ - изоморфизм:

$$\begin{aligned} f(x + y) &= 2^{x+y} \\ f(x)f(y) &= 2^x \cdot 2^y \end{aligned}$$

1.7 Кольца и поля

Замечание. в теории чисел все числа по умолчанию целые

Определение 25. число a делится на b , если: $\exists c : a = bc$

Свойство. 1. $a : c, b : c \Rightarrow a + b : c, a - b : c$

Доказательство. $a : c \Rightarrow a = kc \wedge b : c \Rightarrow b = mc$

$$a = kc \wedge b = mc \Rightarrow \begin{cases} a + b = (m + k)c : c \\ a - b = (m - k)c : c \end{cases} \quad \text{Q.E.D.} \quad \square$$

2. $\forall k : a : b \Rightarrow ak : b$

3. $a : b \wedge b : c \Rightarrow a : c$

4. $a : b \Rightarrow |a| \geq |b| \vee a = 0$

Доказательство. $a = bc \Rightarrow \begin{cases} c = 0, \text{ значит } a = 0 \\ c \neq 0, \text{ значит } |c| \geq 1 \end{cases}$

значит, $|a| = |c||b| \geq |b|$ Q.E.D. □

$$5. \forall a : a : 1$$

$$6. \forall a : 0 : a$$

Определение 26. НОД (a_1, a_2, \dots, a_k) - наибольшее число, на которое делятся a_1, a_2, \dots, a_k
Обозначается как: (a_1, a_2, \dots, a_k)

Определение 27. НОК (a_1, a_2, \dots, a_k) - наименьшее число, которое делится на a_1, a_2, \dots, a_k
Обозначается как: $[a_1, a_2, \dots, a_k]$

Теорема 4. Если не все числа a_1, a_2, \dots, a_k равны нулю, но НОД существует.

Доказательство. Пусть A - множество всех общих делителей, тогда $1 \in A \Rightarrow A \neq \emptyset$

A ограничено сверху, т.к. $\forall \text{делитель} \leq |a_i|$, где a_i - любое ненулевое число, значит, в множестве A есть наибольший элемент Q.E.D. \square

Теорема 5. Если все числа a_1, a_2, \dots, a_k не равны нулю, но НОК существует.

Доказательство. Пусть A - множество всех общих кратных, тогда $a_1, a_2, \dots, a_k \in A \Rightarrow A \neq \emptyset$

A ограничено снизу числом 0, значит, в множестве A есть наименьший элемент Q.E.D. \square

Глава 2

Теория чисел

2.1 Алгоритм Евклида

Теорема 6. (деление с остатком) Пусть $b \in \mathbb{N}, a \in \mathbb{Z}$, тогда $\exists! q, r$:

$$\begin{cases} a = bq + r, \\ 0 \leq r \leq b - 1 \end{cases}$$

Доказательство. 1. Пусть $A = \{a - bx : x \in \mathbb{Z}\}$

Среди элементов A есть хотя бы один неотрицательный:

- . если $a \geq 0$, то $a \in A$
- . если $a < 0$, то $a - ab = a(1 - b) \in A$

Пусть r - наименьший неотрицательный элемент в A . Проверим, что он подходит.

$r = a - bx \Rightarrow a = bx + r$, x можно взять в качестве q

Предположим, что $r \geq b$, тогда:

$r - b = a - b(x + 1) \in A \Rightarrow r$ - не наименьший элемент в $A \Rightarrow r \leq b - 1$

2. Докажем единственностью Пусть $a = bq_1 + r_1 = bq_2 + r_2$;

$0 \leq r_1, r_2 \leq b - 1$

$b(q_1 - q_2) = r_2 - r_1 \Rightarrow (r_2 - r_1) : b \Rightarrow \begin{cases} r_2 - r_1 = 0 \\ |r_2 - r_1| \geq b \end{cases}$ - противоречие: $r_1, r_2 \leq b - 1$

Значит, $r_1 = r_2 \Rightarrow q_1 = q_2$ Q.E.D.

□

Определение 28. (Алгоритм Евклида) даны числа $a, b \in \mathbb{N}, a \geq b$

1. если $a : b$ - конец алгоритма, результат = b
2. если же не делится, то алгоритм применяется к паре (b, r) , где r - остаток от деления a на b

Пример. $a = 22, b = 6$

1. $22 = 3 \cdot 6 + 4 : (22, 6) \rightarrow (6, 4)$
2. $6 = 1 \cdot 4 + 2 : (22, 6) \rightarrow (4, 2)$
3. $4 = 2 \cdot 2$ - конец, ответ: 2

Замечание. (Запись с формулами:)

$$\begin{array}{lll}
 a = bq_0 + r_1 & 0 \leq r_1 < b \\
 b = r_1q_1 + r_2 & 0 \leq r_2 < r_1 \\
 r_1 = r_2q_2 + r_3 & 0 \leq r_3 < r_2 \\
 \vdots & \vdots & \vdots \\
 r_{k-2} = r_{k-1}q_{k-1} + r_k & 0 \leq r_k < r_{k-1} \\
 \vdots & \vdots & \vdots \\
 r_{n-2} = r_{n-1}q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
 r_{n-1} = r_nq_n, \text{ ответ: } r_n
 \end{array}$$

Лекция 4

29.09.2023

2.2 Алгоритм Евклида

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

Доказательство. M_1 - множество общих делителей a, b

M_2 - множество общих делителей $a + kb, b$

докажем, что $M_1 = M_2$

1. $M_1 \subset M_2$

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

2. $M_2 \subset M_1$

$$\exists d \in M_2 \Rightarrow a + kb : d, b : d \Rightarrow a = (a + kb) - kb : d \Rightarrow d \in M_1$$

□

Теорема 7. (Алгоритм Евклида) для любых a, b алг. Евклида заканчивается за конечное число шагов, и его результат равен $\text{НОД}(a, b)$

Доказательство. 1. Алгоритм заканчивается:

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

2. Результат равен $\text{НОД}(a, b)$

если $a : b$, то $\text{НОД}(a, b) = b$

если $a \nmid b$, то итог алгоритма не меняет НОД :

$$\text{НОД}(a, b) = \text{НОД}(a, -bq, b)$$

□

2.3 Линейное представление НОД

Теорема 8. (Линейное представление НОД) Пусть $a, b \in \mathbb{N}$

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

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

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

Докажем:

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

Докажем, что $a, b : d$

Пусть $a \nmid d$. Делим a на d с остатком:

$$a = dq + r, 0 < r < d$$

$$r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy) \in M$$

$0 < r < d, r \in M \Rightarrow d$ - не наименьший положительный, противоречие

аналогично, $b : d$

Докажем, что если k - общий делитель a и b , то $k : d$:

$$d = ax + by$$

$$a : k \Rightarrow ax : k \wedge b : k \Rightarrow by : k \Rightarrow ax + by : k$$

□

Замечание. Линейное представление можно найти с помощью алгоритма Евклида

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

2.4 Простые числа

Определение 29. числа a и b - взаимно простые, если $(a, b) = 1$

Определение 30. Числа a_1, a_2, \dots, a_k называются взаимно простыми в совокупности, если $(a_1, a_2, \dots, a_k) = 1$

Определение 31. Числа a_1, a_2, \dots, a_k называются попарно взаимно простыми, если любые два из них - взаимно простые

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

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

Доказательство. \Rightarrow : по теореме о линейном представлении НОД
 \Leftarrow : Пусть $d = (a, b), d \neq 1$. Тогда $ax + by : d, 1 \nmid d$. противоречие, \square

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

Доказательство. (Индукция) База $k = 2$. Докажем, что если a_1, a_2 взаимно просты с b , то $a_1 a_2$ взаимно просто с b . По лемме (2): $\exists x_1, y_1, x_2, y_2 : a_1 x_1 + b y_1 = 1, a_2 x_2 + b y_2 = 1$. Перемножим:

$$(a_1 a_2)(x_1 x_2) + b(a_1 x_1 y_2 + y_1 a_2 x_2 + b y_1 y_2) = 1$$

Получили линейное представление 1 через $a_1 a_2$ и $b \Rightarrow a_1 a_2, b$ - взаимно просты

Переход $k \rightarrow k + 1$

$a_1, a_2, \dots, a_k, a_{k+1}$ взаимно просты с b

a_1, a_2, \dots, a_k взаимно просты с $b \xrightarrow{\text{ИП для } k} a_1 \cdot a_2 \cdot \dots \cdot a_k$ \square

Свойство. 1. Пусть $ab : c$, a и c взаимно просты. Тогда $b : c$

2. Пусть $a : b, a : c$, b и c взаимно просты. Тогда $a : bc$

Доказательство. 1. $\exists x, y : ax + cy = 1$. Умножим на b :

$$(ab)x + bcy = b$$

\vdots_c

$$ab : c \text{ — по условию } \Rightarrow abx : c \wedge bcy : c \Rightarrow b : c$$

2. $a = bk, a = cm, \exists x, y : bx + cy = 1$. Умножим на k :

$$k = \underset{a}{bkx} + cyk = ax + cyk = cmx + cyk : c \Rightarrow k : c$$

$$k = cz, a = bk = (bc)z : bc$$

\square

Определение 32. Число p называется простым, если $p > 1$ и у p нет натуральных делителей, кроме 1 и p

Определение 33. Число n называется составным, если $n > 1$ и n - не простое

Обозначение. множество простых чисел - P

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

Доказательство. 1. \Rightarrow : $a \notin P$, тогда у a есть делитель $b : b \neq 1, b \neq a \Rightarrow 1 < b < a$

$$\exists c : a = bc, c = \frac{a}{b}, \frac{a}{b} < c < \frac{a}{1}$$

$$2. \Leftarrow: a = bc, 1 < b < a \Rightarrow \text{у } a \text{ есть делитель } \neq 1, \neq a \Rightarrow a \notin P$$

□

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

Доказательство. (Индукция)

1. База $n = 2$, делителя 2
2. Переход. Предположим, что $n > 2, \forall k : 1 < k < n$ у k есть простой делитель. Докажем, что у n есть простой делитель

- (а) случай 1: n - простое $\Rightarrow n$ - простой делитель n
- (б) случай 2: n - составное \Rightarrow у n есть делитель, $n = km, 1 < k, m < n$

По индукции: $\exists p \in P : k : p \Rightarrow n : p$

□

Теорема 9. (Евклида) Множество простых чисел бесконечно

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

Положим $N = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$, Тогда по лемме у N есть некий простой делитель, Np_1, p_2, \dots, p_k , т.к. $\Rightarrow 1 : p_i$ - невозможно

Значит N - простое. Противоречие.

□

Теорема 10. (Дирихле) Пусть $(a, m) = 1$. Тогда \exists бесконечно много простых чисел вида $a + km$ (Доказательство слишком сложное)

2.5 Основная теорема арифметики

Теорема 11. Любое натуральное число, большее 1 можно представить в виде произведения простых чисел. С точностью представления до порядка сравнения.

Доказательство. 1. Существование: Индукция

- (а) База $n = 2, 2 = 2$ - разложение
- (б) Переход: Предположим, что все числа, меньшие n , раскладываются в произведение простых. Докажем для n .
 - i. случай 1: n - простое, $n = n$ - разложение
 - ii. случай 2: n - составное, тогда $\exists p : p \in P, n : p, 1 < p < n$

$1 < \frac{n}{p} < n$ По инд. предположению $\frac{n}{p}$ можно разложить:
 $\frac{n}{p} = p_1 p_2 \cdot \dots \cdot p_k \Rightarrow n = p \cdot p_1 p_2 \cdot \dots \cdot p_k \Rightarrow$ существование
 доказано.

2. Единственность.

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

Далее: $q_1 \neq p_1, q_2 \neq p_1, \dots, q_m \neq p_1 \Rightarrow q_1, p_1$ - взаимно простые,
 q_2, p_1 - взаимно простые,

\vdots

q_m, p_1 - взаимно простые,

Значит, $n = q_1 \cdot \dots \cdot q_m \cdot p_1$, при этом $n = p_1 \cdot \dots \cdot p_k : p_1$ - противоречие, единственность доказана. \square

Свойство. Пусть $p \in P, a_1, \dots, a_k : p$, тогда для некоторого $a_i : p$

Доказательство. Пусть не делится, тогда:

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

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

\vdots

$$\text{Получаем: } \underbrace{a_1 \cdot a_2 \cdot \dots \cdot a_k}_{\text{делится на } p} = \underbrace{p_{11} \cdot p_{12} \cdot \dots}_{\text{не делится на } p} \Rightarrow \text{противоречие.} \quad \square$$

Лекция 5

06.10.2023

2.6 Степень вхождения простого числа

Определение 34. $v_p(n)$ — степень вхождения $p \in P$ в разложение n на простые множители.

Т.е. $v_p(n) = k$, если $n : p^k$ и $n \nmid p^{k+1}$.

Пример. $v_2(12) = 2, v_2(15) = 0, v_2(16) = 4$.

Свойство. 1. $v_p(nm) = v_p(n) + v_p(m)$.

2. $a, b \in \mathbb{N}$. Тогда $a = b \Leftrightarrow v_p(a) = v_p(b)$

3. $a : b \Leftrightarrow v_p(a) \geq v_p(b) \forall p \in P$

4. $v_p((a, b)) = \min(v_p(a), v_p(b))$ $v_p([a, b]) = \max(v_p(a), v_p(b))$

Глава 3

Сравнения и классы вычетов

Определение 35. $m \in \mathbb{N}$. Числа a и b называют сравнимыми по модулю m , если $a - b : m$.

Обозначение. $a \equiv b \pmod m$ $a \equiv b$.

Теорема 12. Сравнение по модулю m — отношение эквивалентности.

Доказательство. 1. $a \equiv a \pmod m \Leftrightarrow a - a : m \Leftrightarrow 0 : m$ — рефлексивное.

2. $a \equiv b \pmod m \Rightarrow (a - b) : m \Rightarrow (-1)(a - b) : m \Rightarrow b - a : m \Rightarrow b \equiv a \pmod m$ — симметричное.

3. $a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow (a - b) : m, (b - c) : m \Rightarrow (a - b) + (b - c) : m \Rightarrow a - c : m \Rightarrow a \equiv c \pmod m$ — транзитивное. \square

Определение 36. $a \in \mathbb{Z}, m \in \mathbb{N}$. Классом вычетов по модулю m называется множество $\bar{a}_m = \{b \in \mathbb{Z} \mid a \equiv b \pmod m\}$.

Определение 37. Набор чисел называется полной системой вычетов по модулю m , если в него входят по одному представителю из каждого класса вычетов

Пример. $m = 5$. Полные системы вычетов:

$\{0, 1, 2, 3, 4\}$
 $\{-2, -1, 0, 1, 2\}$
 $\{5, 11, -13, 3, 4\}$

Свойство. (Арифметические свойства сравнений)

Пусть $a \equiv b \pmod m$ и $c \equiv d \pmod m$, тогда:

$$1. a + c \equiv b + d \pmod m$$

$$a - c \equiv b - d \pmod m$$

$$2. ac \equiv bd \pmod m$$

Доказательство. 1. $(a + c) - (b + d) = \underbrace{(a - b)}_{\vdots m} + \underbrace{(c - d)}_{\vdots m} \Rightarrow$

$$\Rightarrow a + c \equiv b + d \pmod m$$

Аналогично для разности.

$$2. ac - bd = ac - bc + bc - bd = c \underbrace{(a - b)}_{\vdots m} + b \underbrace{(c - d)}_{\vdots m} \Rightarrow ac \equiv bd \pmod m$$

□

Замечание. $2 \equiv 12 \pmod{10}$, $1 \not\equiv 6 \pmod{10}$

Свойство. (Решение линейного сравнения)

Пусть $a, b \in \mathbb{Z}, m \in \mathbb{N}, (a, m) = 1$, Тогда:

1. Сравнение $ax \equiv b \pmod m$ имеет решение.

2. Если x_1, x_2 — решения, то $x_1 \equiv x_2 \pmod m$.

Пример. $3x \equiv 2 \pmod 5$

$x_0 = 4$ — решение, множество решений: $x \equiv 4 \pmod 5$

Доказательство. Докажем первое, затем второе.

$$1. (a, m) = 1 \Rightarrow \exists u, v : au + mv = 1 \Rightarrow$$

$$\Rightarrow au \equiv 1 \pmod m \Rightarrow a(bu) \equiv b \pmod m$$

$$x = bu \text{ — решение.}$$

$$2. \begin{cases} ax_1 \equiv b \pmod m \\ ax_2 \equiv b \pmod m \end{cases} \Rightarrow ax_1 \equiv ax_2 \pmod m \Rightarrow a(x_1 - x_2) \vdots m \Rightarrow$$

$$x_1 - x_2 \vdots m \Rightarrow x_1 \equiv x_2 \pmod m$$

□

Определение 38. Определим сложение и умножение на множестве классов вычетов по модулю m :

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Пример. $m = 5$

$$\begin{aligned}\bar{2} + \bar{3} &= \bar{5} = \bar{0} \\ \bar{2} \cdot \bar{3} &= \bar{6} = \bar{1}\end{aligned}$$

Теорема 13. (Кольцо вычетов) Пусть $m > 1, m \in \mathbb{N}$. Рассмотрим классы вычетов по модулю m .

1. Сумма и произведение определены корректно, т.е. результат не зависит от выбора представителей.
2. Классы вычетов образуют коммутативное и ассоциативное кольцо с единицей.
3. Кольцо классов вычетов является полем $\Leftrightarrow m$ — простое.

Доказательство. Приведем доказательство только для суммы, для произведения доказательство строится аналогично.

$$1. \begin{cases} a_1, a_2 — \text{представители одного класса} \\ b_1, b_2 — \text{представители одного класса} \end{cases} \Rightarrow \begin{cases} a_1 \equiv a_2 \pmod{m} \\ b_1 \equiv b_2 \pmod{m} \end{cases} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m} — a_1 + b_1 \text{ и } a_2 + b_2 \text{ в одном классе.}$$

$$2. \text{ Нейтральный по сложению: } \bar{0} : \bar{0} + \bar{x} = \overline{x + 0} = \bar{x}$$

$$\text{Нейтральный по умножению: } \bar{1} : \bar{1} \cdot \bar{x} = \overline{1 \cdot x} = \bar{x}$$

Свойства ассоциативности и коммутативности очевидны. Докажем, например, ассоциативность:

$$(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \overline{xy} \cdot \bar{z} = \overline{xyz} = \bar{x} \cdot \overline{yz} = \bar{x} \cdot (\bar{y} \cdot \bar{z})$$

3. ассоциативное коммутативное кольцо с единицей является полем $\Leftrightarrow \forall \bar{a} \neq \bar{0}$ есть обратный по умножению.

(a) Пусть $m \in P, \bar{a} \neq \bar{0}$

$$\bar{a} \neq \bar{0} \Rightarrow a \nmid m \Rightarrow_{m \in P} (a, m) = 1$$

Из решения линейного сравнения следует, что $\exists x : ax \equiv 1 \pmod{m} \Rightarrow \bar{a} \cdot \bar{x} = 1 \Rightarrow \bar{x} = \bar{a}^{-1}$

(b) Пусть $m \notin P$. Тогда $\exists a, b : m = ab, 1 < a, b < m$

Докажем, что $\nexists \bar{a}^{-1}$

Предположим, что есть, тогда: $\bar{x} = \bar{a}^{-1}$

$$\bar{b} = 1 \cdot \bar{b} = \bar{x} \cdot \bar{a} \cdot \bar{b} = \bar{x} \cdot \overline{ab} = \bar{x} \cdot \bar{m} = \bar{x} \cdot \bar{0} = \bar{0} — \text{противоречие.}$$

□

Обозначение. Кольцо вычетов по модулю m обозначается \mathbb{Z}_m или $\mathbb{Z}/m\mathbb{Z}$.

Теорема Вильсона и малая теория Ферма

Теорема 14. (Теорема Вильсона) Пусть $p \in P$, тогда $(p-1)! \equiv -1 \pmod p$.

Доказательство. 2 случая:

1. случай $p = 2$: $(p-1)! = 1 \equiv -1 \pmod 2$

2. случай $p > 2$: Рассмотрим поле \mathbb{Z}_p

(а) Нужно доказать, что $(p-1)! = 1 \in \mathbb{Z}_p$.

- $1, 2, \dots, p-1$ - ненулевые элементы \mathbb{Z}_p .
- у каждого элемента есть обратный по умножению.

(б) Докажем, что $x = \bar{x}^{-1}$ выполнено только при $x = 1, x = p-1$:

$$x = \bar{x}^{-1} \Leftrightarrow x \cdot x = \bar{x}^{-1} \cdot x \Leftrightarrow x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$$

$$\Leftrightarrow \begin{matrix} \text{обл. целост.} \\ \Leftrightarrow \end{matrix} \begin{cases} x-1=0 \\ x+1=0 \end{cases} \Leftrightarrow \begin{cases} x=1 \\ x=p-1 \end{cases}$$

(с) Все элементы, кроме 1 и $p-1$ распадаются на пары, обратные друг другу:

$$1 \cdot 2 \cdot \dots \cdot (p-1) = 1 \cdot (p-1) \cdot (x_1 \cdot \bar{x}_1^{-1}) \cdot (x_2 \cdot \bar{x}_2^{-1}) \cdot \dots = p-1 = 1$$

□

Лемма 4. Пусть $p \in P$. Тогда $\forall a \in \mathbb{Z}_p, a \neq 0$ набор элементов:

$0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a$ — перестановка элементов $0, 1, \dots, p-1$.

Другая формулировка:

Если $a \nmid p$, то $0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a$ — полная система вычетов по $\pmod p$.

Доказательство. Докажем, что элементы $0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a$ — различны.

Предположим, что не различны, тогда $\exists i, j : i \neq j, i \cdot a = j \cdot a \Rightarrow (i-j) \cdot a = 0 \Rightarrow i = j$ — противоречие.

$0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a$ — p шт. различных элементов в $\mathbb{Z}_p \Rightarrow$ это все элементы \mathbb{Z}_p . □

Пример. $p = 5, a = 3$

$$\{0 \cdot 3, 1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3\} = \{0, 3, 6, 9, 12\}$$

Теорема 15. (Малая теорема Ферма) Пусть $p \in P, a \in \mathbb{Z}, a \not\equiv 0 \pmod{p}$. Тогда $a^{p-1} \equiv 1 \pmod{p}$.

Доказательство. Рассмотрим наборы $0, 1, \dots, p-1$ и $0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a$ — совпадающие по лемме 4

Выкинем 0 из наборов, тогда $1, \dots, p-1$ — перестановка $1 \cdot a, \dots, (p-1) \cdot a$.

Перемножим:

$$1 \cdot 2 \cdot \dots \cdot (p-1) = (1 \cdot a) \cdot (2 \cdot a) \cdot \dots \cdot ((p-1) \cdot a)$$

$$1 \cdot 2 \cdot \dots \cdot (p-1) = a^{p-1} \cdot 1 \cdot 2 \cdot \dots \cdot (p-1)$$

$$1 = a^{p-1} \quad \text{в } \mathbb{Z}_p$$

□