Основы комбинаторики и теории чисел

Сергей Григорян

7 января 2025 г.

Содержание

1 Лекция 1

1.1 Инфа

Лектор: Даниил Владимирович Мусатов (ему писать по поводу логики) и Райгородский Андрей Михайлович.

`telega: @musatych`

Об отсутствии на КР писать в тг заранее

Задачи на КР:

- Тестовые 0.8 (Или отдельно написано)
- Обычные (можно пересдать (1(на КР)/0.8(На след. КР)/0.5(В ДЗ)))

Задачи на ДЗ:

- Перешедшие с КР (0.5)
- Обычные (1)
- Дополн. (1.5)

Замечание. *Чтобы получить доп. задачу, нужно решить* ***все*** *обычные задачи по какой-то теме.*

1.2 Основные понятия теор. множеств

Обозначение. $x \in A \iff$ ***элемент*** *x принадлежит* ***мн-ву*** *A.*

Определение 1.1. **Пустое мн-во** $\emptyset$ - мн-во, не содержащее ни одного эл-та.

Определение 1.2. A **подмн-во** B $(A \subset B) \iff$

$$\forall x (x \in A \Rightarrow x \in B).$$

Замечание. $\forall A \colon \emptyset \subset A$

Замечание.

$$\forall x (x \in \emptyset \Rightarrow x \in A).$$

Свойство отношения подмножества:

- **Рефлексивность**: $A \subset A$
- **Транзитивность**: $A \subset B, B \subset C \Rightarrow A \subset C$ -
- **Антисимметричность**: $A \subset B, B \subset A \Rightarrow A = B$

Определение 1.3 (Равенство мн-в)**.** $A = B \iff$, если A и B содержат одни и те же эл-ты.

Запись конечного мн-ва: $\{a, b, c\}$

Замечание. *Из опр. рав-ва следует, что* ***кратность и порядок записи не важен****:*

Пример. $\{a, b, c\} = \{a, c, b, b, b, a\}$

Замечание. *Отличие* $\in$ *и* $\subset$ *:*

$$A = \{a, \{b\}, c, \{c\}\}.$$

$$\{a\} \subset A, \{a\} \notin A.$$

$$\{b\} \not\subset A, \{b\} \in A, \{\{b\}\} \subset A.$$

$$\{c\} \subset A, \{c\} \in A.$$

$$\{d\} \notin A, \{d\} \notin A.$$

Конструкция нат. чисел на основе мн-в
$0 = \emptyset$
$1 = \{\emptyset\}$
$2 = \{\emptyset, \{\emptyset\}\}$
$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
$n + 1 = \{0, 1, 2, \cdots, n\}$

Операции над мн-вами

1. Объединение: $A \cup B = \{x\colon x \in A \vee x \in B\}$
2. Пересечение: $A \cap B = \{x\colon x \in A \wedge x \in B\}$
3. Разность: $A \backslash B = \{x\colon x \in A \wedge x \notin B\}$

4. Дополнение: $\overline{A} = \{x \colon x \notin A\}$

5. Симметрическая разность: $A \triangle B = \{x \colon (x \in A \vee x \in B) \wedge (x \notin A \cap B)\}$

<u>Утверждение</u> 1.1.

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

Доказательство. В одну сторону:

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

1. $x \in A \Rightarrow x \in A \cup B$ и $A \cup C \Rightarrow x \in A \cup B \wedge x \in A \cup C$

2. $x \in B \cap C \Rightarrow x \in B \wedge x \in C \Rightarrow x \in A \cup B \wedge x \in A \cup C \Rightarrow x \in (A \cup B) \cap (A \cup C)$

$\square$

1.3 Упорядоченные пары и кортежи

$$(a, b), a - \text{ 1-ый эл-т}, b - \text{ 2-ой эл-т}$$

Требование: $(a, b) = (c, d) \iff a = c \wedge b = d$

<u>Определение</u> 1.4 (Упрощенное определение Куратовского)**.**

$$(a, b) = \{\{a, b\}, a\}.$$

$$(a, a) = \{\{a\}, a\}.$$

1.4 Парадокс Рассела

Определим I**:**

$$\{\{\{\cdots a \cdots\}\}\} = I \Rightarrow I \in I, \text{(беск. кол-во скобок)}.$$

$$(I, I) = \{\{I\}, I\} = I.$$

Рассмотрим: $M = \{x \colon x \notin x\}$

$$M \overset{?}{\in} M.$$

- Пусть $M \in M$. Тогда $x \notin x$ верно для $x = M$. Тогда $M \notin M$. Но тогда $x \notin x$ неверно для $x = M$. Противоречие.

- Аналогично $M \notin M \Rightarrow$ получаем парадокс.

Аксиома 1.1 (Аксиома фундированности)**.** *Не сущ. беск цепочки:*

$$A_1 \ni A_2 \ni A_3 \ni \cdots$$

Замечание. *Это запрещает мн-во I и $M \in M$, а также даёт однозначную интерпретацию (a, b)*

Если $\{a, b\} \in a$, то возникает беск. цепочка:

$$\{a, b\} \ni a \ni \{a, b\} \ni a \cdots .$$

Определение 1.5. Кортежи - расширение пары на много эл-ов.

Пример. $(a, b, c, d) = (a, (b, (c, d)))$ - *кортеж*

Определение 1.6. Декартово произведение мн-в A, B:

$$A \times B = \{(a, b)\colon a \in A, b \in B\}.$$

2 Лекция 2

2.1 Отображения и соответствия

Определение 2.1. Соответствие (или **многозначная ф-ция**, или **точечно-множ. отображение**) - подмн-во декартова произведения мн-в A и B.

$F \subset A \times B$ - соответствие между A и B

Замечание. ***Непустозначное соответствие:*** $\forall x, \exists y\colon (x, y) \in F$

Картинки графика и двудольного графа

Определение 2.2. Отображение - однозначное соотв.

$$\forall x, \exists! y\colon (x, y) \in f$$

$\forall$- для любого, $\exists!$ – существует единственный

Определение 2.3. Частично определённая ф-ция:

$$\forall x\colon (\neg\exists y\colon (x,y)\in F)\vee(\exists! y\colon (x,y)\in F)$$

Определение 2.4. Инъекция - отображение, т. ч. $\forall x, y(x\neq y\to f(x)\neq f(y))$

Определение 2.5. $f(x)$ - тот элемент $z\colon (x,z)\in f$

Определение 2.6. $F(x)$ - образ $x \iff F(x)=\{z\colon (x,z)\in F\}$

Определение 2.7. Инъективные соответствия:

$$\forall x, y(x\neq y\to F(x)\cap F(y)=\emptyset)$$

Определение 2.8. Сюрьекция - отображение, т. ч. $\forall y, \exists x(y=f(x))$

Определение 2.9. Сюрьективное соответствие:

$$\forall y, \exists x\colon (x,y)\in F$$

Или по другому: $\forall y, \exists x\colon y\in F(x)$

Определение 2.10. Биекция - отображение, которое одновременно сюрьекция и инъекция.

Биекция = отображение + сюрьекция + инъекция

Замечание. *Отдельного понятия биективного соответствия нет.*

Определение 2.11. Обратное соответствие $F\subset A\times B$ - $F^{-1}\subset B\times A$:

$$(x,y)\in F \iff (y,x)\in F^{-1}$$

Теорема 2.1. ***F* - *Биекция*** $\iff$ ***F* - *взаимнооднозначное соответствие*** *(т. е. F и F^{-1} - отображения)*

Замечание. ***Частично опред. ф-ция + непустознач. соотв = отображение***

Доказательство.

- F явл. инъективным соответствием $\iff$ $F^{-1}-$ частично опред. ф-ция.
- F явл. сюрьективным соответствием $\iff$ $F^{-1}-$ непустозначное соотв.

$\square$

2.2 Образ и прообраз

Определение 2.12. Пусть $S \subset A$. Тогда образ S:

- Для отображения: $f(S) = \{f(x) | x \in S\}$
- Для соотв.: $F(S) = \bigcup_{x \in S} F(x)$

Определение 2.13. Пусть $T \subset B$. Тогда прообраз T:

- Для отображения: $f^{-1}(T) = \{x | f(x) \in T\}$
- Для соотв.: $F^{-1} = \{x | F(x) \cap T \neq \emptyset\}$

Утверждение 2.1. $F(S \cap Q) \subset F(S) \cap F(Q)$

Доказательство. Пусть $y \in F(S \cap Q) \Rightarrow \exists x \in S \cap Q \colon y \in F(x)$:

$$\begin{cases} \exists x \in S \colon y \in F(x) \\ \exists x \in Q \colon y \in F(x) \end{cases} \Rightarrow \begin{cases} y \in F(S) \\ y \in F(Q) \end{cases} \Rightarrow y \in F(S) \cap F(Q)$$

□

Утверждение 2.2 (Обратное.)**.** *Если F - инвективно, то*

$$F(S) \cap F(Q) \subset F(S \cap Q)$$

Доказательство.

$$y \in F(S) \cap F(Q) \Rightarrow$$

$$\begin{cases} y \in F(S) \\ y \in F(Q) \end{cases} \Rightarrow \begin{cases} \exists x_1 \in S \colon y \in F(x_1) \\ \exists x_2 \in Q \colon y \in F(x_2) \end{cases} \Rightarrow x_1 \neq x_2 \Rightarrow \text{Нарушает инъективность}$$

$$\Rightarrow x_1 = x_2 = x \Rightarrow \exists x \in S \cap Q \colon y \in F(x)$$

□

2.3 Композиция

Определение 2.14. Композиция отображений $f \circ g$, опр. так:

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

Определение 2.15. Композиция соотв. $F \circ G$

$$\begin{cases} F : B \to C \\ G : A \to B \end{cases} \Rightarrow F \circ G(x) = F(G(x))$$

Причём $G(x)$ - это мн-во значений $\Rightarrow F(G(x))$ - образ $G(x)$
Или, эквив.: $(x, z) \in F \circ G \iff \exists y((x, y) \in G \wedge (y, z) \in F)$

Свойства композиции:

1) **Ассоциативность:** $F \circ (G \circ H) = (F \circ G) \circ H$

2) **Отсутствие** коммутативности (в общем случае): $F \circ G \neq G \circ F$

Обозначение. ***Тождественное отображение:***

$$id_A : A \to A$$

$$id_A(x) = x$$

$$G : A \to B \Rightarrow G \circ id_A(x) = id_B \circ G(x) = G(x)$$

Утверждение 2.3. *Если $F : A \to A$ - биекция, то:*

$$F \circ F^{-1} = id_A = F^{-1} \circ F$$

Обозначение. ***Мн-во всех отображений из** A **в** B будем называть B^A*

Утверждение 2.4. *Если $|A| = n$ и $|B| = k$, то $|B^A| = k^n$*

Теорема 2.2. *Пусть A, B, C - мн-ва. Тогда:*

1) $A^C \times B^C \sim (A \times B)^C$

2) $A^{B \cup C} \sim A^B \times A^C, B \cap C \neq \emptyset$

3) $A^{B \times C} \sim (A^B)^C$

Доказательство. 1)

$$\begin{cases} f : C \to A \\ g : C \to B \end{cases} \longleftrightarrow h : C \to A \times B, h(x) = (f(x), g(x))$$

2)

$$\begin{cases} f : B \to A \\ g : C \to A \end{cases} \longleftrightarrow h : B \cup C \to A \Rightarrow h(x) = \begin{cases} f(x), x \in B \\ g(x), x \in C \end{cases}$$

3)

$$\begin{cases} f : B \times C \to A \\ g : C \to A^B \end{cases} \Rightarrow g(x) : B \to A \Rightarrow g(x)(z) = f(z, x)$$

$\square$

3 Лекция 3

3.1 Мощности мн-в

3.1.1 Парадоксы

Парадокс Галилея:

Все нат. числа	$\not\supseteq$	полные квадаты
n	$\longleftrightarrow$	n^2

Гранд-отель Гильберта:

1	2	3	4	5	6	7	...

1) Все места заняты, нужно подселить постояльца:

<u>Решение</u>.

Новый	$\to$	*0*
i	$\to$	$(i+1)$

2) Есть своб. места, **хотим занять все комнаты имеющимися постояльцами**:

<u>Решение</u>. *Если мн-во занятых комнат бесконечно, то:*

0	*1*	*0*	*0*	*1*	*1*	*0*	*1*	*0*	...

(1 - занято, 0 - свободно) $\Rightarrow$
Переносим 1 в самый ранний 0 для всех 1

3) 2 гранд-отеля, полностью заняты. Один закрылся, как всех заселить?

<u>Решение</u>.

0	*1*	*2*	*3*	*4*	*5*	...

a	b	c	d	e	f	...

$\Rightarrow$

0	a	*1*	b	*2*	c	...

4) Гранд-авеню, гранд-отелей. Цель: переселить всех в один отель:

<u>Решение</u>.

Отель 0: $\mapsto$ *неч. номера*

Отель 1: $\mapsto$ *номера, кот.* $\vdots 2$, $\not\vdots 4$

Отель 2: $\mapsto$ *номера, кот.* $\vdots 4$, $\not\vdots 8$

Отель k: $\mapsto$ *номера, кот* $\vdots 2^k$, $\not\vdots 2^{k+1}$

3.1.2 Счётных мн-в

<u>Определение</u> 3.1. A и B **равномощны** ($A \cong B$), если $\exists$ биекция $f : A \to B$

<u>Определение</u> 3.2. A наз-ся **счётным**, если $A \cong \mathbb{N}$

<u>Утверждение</u> 3.1. *1)* A *счётно* $\Rightarrow A \cup x$ *счётно*

2) Любое подмн-во счётного мн-ва конечно или счётно

3) A, B *счётны* $\Rightarrow A \cup B$ *счётно*

4) $A_0, A_1, \dots$ *- сч.* $\Rightarrow \bigcup_{i=0}^{\infty} A_i$ *- сч.*
или: A, B *- сч.* $\Rightarrow A \times B$ *- сч.*

Доказательство. 1) $f : A \to \mathbb{N}$ - биекция

$$g : A \cup \{ x \} \to \mathbb{N}:$$

$$\begin{cases} g(x) = 0 \\ g(y) = f(y) + 1, y \in A \end{cases}$$

2)

$$f : A \to \mathbb{N}, \text{- биекция}; B \subset A$$

$$g : B \to \mathbb{N}; g(x) = \# \{ y \in B \mid f(y) < f(x) \}$$

3)

$$f : A \to \mathbb{N}; g : B \to \mathbb{N}$$

$$h : A \cup B \to \mathbb{N}; h(x) = \begin{cases} 2f(x), x \in A \\ 2g(x) + 1, x \in B \end{cases}$$

4)

$$f : A \to \mathbb{N};$$

$$g : B \to \mathbb{N};$$

$$h : A \times B \to \mathbb{N}; h(x, y) = 2^{f(x)} * (2g(y) + 1) - 1$$

□

3.1.3 Отношение равномощности

Утверждение 3.2. *Общие св-ва равномощности:*

1) ***Рефлексивность**: $A \cong A$*
   (т. к. id_A - биекция)

2) ***Симметричность**: $A \cong B \iff B \cong A$*
   (f - биекция $\iff$ f^{-1} - биекция)

3) ***Транзитивность**: $A \cong B, B \cong C \Rightarrow A \cong C$*
   (т. к. композиция биекций - биекция)

3.1.4 Сравнимость по мощности

Обозначение. • *Нестрогая: AB, если $\exists B' \subset B, A \cong B'$*

(A не более мозно чем B)

- *Строгая: AB, если $AB, A \ncong B$*

  (A менее мощно чем B)

Утверждение 3.3. *Св-ва сравнимости по мощ-ти:*

1) *Рефлексивность: AA; Антирефлексивность: $A \not A$*

2) *Транзитивность: $AB, BC \Rightarrow AC$*

   Для строгой сравнимости:

   Доказательство.

$$AB, BC \Rightarrow AC$$

$$AC \text{ - из предыдущего}$$

Нужно: $A \cong C$ ☐

Теорема 3.1 (Теорема Кантора-Бернштейна)**.**

$$AB, BA \Rightarrow A \cong B$$

Доказательство. 1) Пусть $f : A_0 \to B_1 \subset B_0$ - биекция
$g : B_0 \to A_1 \subset A_0$ - биекция

2) $B_{i+1} = f(A_i)\,; A_{i+1} = g(B_i)$

3) $C_i = A_i \backslash A_{i+1}; D_i = B_i \backslash B_{i+1}$

4) $C = \bigcap_{i=0}^{\infty} A_i; D = \bigcap_{i=0}^{\infty} B_i$

Утверждение 3.4. *$C_i \cong D_{i+1}$, т. е. $f : C_i \to D_{i+1}$ - биекция*
Почему? Потому что:

$$C_i = A_i \backslash A_{i+1}; f(A_i) = B_{i+1}, f(A_{i+1}) = B_{i+2}$$

$f(A_i \backslash A_{i+1}) =$ (*т. к. f - биекция*) $f(A_i) \backslash f(A_{i+1}) = B_{i+1} \backslash B_{i+2} = D_{i+1} = f(C_i)$

Утверждение 3.5.

$$D_i \cong C_{i+1} \, (\textit{симметричо})$$

Следствие.

$$C_0 \cong C_2 \cong C_4 \cong C_6 \cong \dots$$

$$C_0 \cong D_1 \cong D_3 \cong D_5 \dots$$

Утверждение 3.6.

$$C \cong D$$

Доказательство. f - биекция
Пусть $x \in \bigcap_{i=0}^{\infty} A_i \Rightarrow \forall i, x \in A_i \Rightarrow \forall i, f(x) \in B_{i+1} \Rightarrow f(x) \in \bigcap_{i=0}^{\infty} B_i$
Т. е. $f(C) \subset D$**:**

Инъекция - наследуется

Сюрьекция: $y \in \bigcap_{i=0}^{\infty} B_i \Rightarrow \forall i, y \in B_{i+1} \Rightarrow \forall i, f^{-1}(y) \in A_i \Rightarrow f^{-1}(y) \in C$ □

$$A = C \cap C_0 \cap C_1 \cap C_2 \cap C_3 \cap \dots$$

$$B = D \cap D_1 \cap D_2 \cap D_3 \cap D_4 \dots$$

При этом:

$$\begin{cases} C \cong D \\ \begin{cases} C_0 \cong D_1 \\ C_1 \cong D_0 \end{cases} \\ \begin{cases} C_2 \cong D_3 \\ C_3 \cong D_2 \end{cases} \\ \vdots \end{cases} \Rightarrow A \cong B$$

□

4 Лекция 4

Обозначение. $\{0,1\}^{\mathbb{N}}$ - *это*

1) *Мн-во подмножеств* $A \subset \mathbb{N}$
2) *Мн-во ф-ций* $f : \mathbb{N} \to \{0,1\}$

3) Мн-во $A \leftrightarrow f_A\colon N \to \{0,1\}$

$$f_A(x) = \begin{cases} 1, x \in A \\ 0, x \notin A \end{cases}$$

Замечание. *Бесконечная двоичная дробь:*

$$\underline{a_1 a_2 \dots a_n} 01111\dots = \underline{a_1 a_2 \dots a_n} 10000\dots$$

Задача 4.1. Показать:

$$[0,1] \cong \{0,1\}^{\mathbb{N}} \setminus \{\text{посл-ти с 1 в периоде}\}$$

Доказательство. Конструктивно: Picture

□

Теорема 4.1. A *- беск.,* B *- сч.* $\Rightarrow A \cup B \cong A$

Следствие.

$$[0,1] \cong \{0,1\}^{\mathbb{N}}$$

Лемма 4.2. *В любом бесконечном мн-ве есть счётное подмн-во*

Доказательство. A - беск. мн-во
$a_0 \in A, a_1 \in A \setminus \{a_0\}, \dots$
$a_{n+1} \in A \setminus \{a_0, a_1, \dots, a_n\}$ A - беск., сл-но на каждом шаге возможен выбор нового эл-та □

Теперь **докажем теорему:**

Доказательство. A - беск. $\Rightarrow C \subset A$, C - счётно

$$\begin{cases} C \cong \mathbb{N} \\ B \cong \mathbb{N} \end{cases} \Rightarrow C \cup B \cong \mathbb{N} \cong C$$

$$A \cup B = (A \setminus C) \cup C \cup B \cong (A \setminus C) \cup C \cong A$$

□

Теорема 4.3 (Кантора)**.** $[0,1]$ - *несчётен (или:* $\{0,1\}^{\mathbb{N}}$ *несчётно)*

Доказательство. Пусть $\{\,0,1\,\}^{\mathbb{N}}$ - счётно, тогда α_i - i-ая бинарная последовательность:

α_0	$\underline{0}0000\ldots$
α_1	$1\underline{1}111\ldots$
α_2	$01\underline{0}11\ldots$
$\vdots$	$\vdots$

Воспользуемся диагональным методом Кантора:. Возьмём диагональную п-ть:

$$d_i = \alpha_i^i, d = 010\ldots$$

$$d_i' = 1 - \alpha_i^i, d' = 101\ldots$$

Если $d' = (\alpha_k)^k$, то $(d_k)^k = ((d_k)^k)' = 1 - (\alpha_k)^k$, что невозможно $\Rightarrow$ противоречие. $\square$

Теорема 4.4 (Общая теорема Кантора)**.** $\forall A\colon A2^A$

Доказательство. Пусть $\phi : A \to 2^A$ - биекция
$\phi(x)$ - подмн-во A
Корректен ли вопрос о том, что $x \in \phi(x)$?
Расм. $M = \{\, x \mid x \notin \phi(x)\,\}$
Т. к. ϕ - биекция $\Rightarrow$ сущ. $m = \phi^{-1}(M)$. Т. е. $\phi(m) = M$
Рассм. 2 случая:

1)

$$m \in M \Rightarrow m \in \phi(m) \Rightarrow x \notin \phi(x) - \text{ ложно при } x = m \Rightarrow m \notin M$$

2)

$$m \notin M \Rightarrow m \notin \phi(m) \Rightarrow x \notin \phi(x) \text{ - истино, при } x = m \Rightarrow m \in M$$

Получаем противоречие. $\square$

Определение 4.1. A **континуально**, если $A \cong \{\,0,1\,\}^{\mathbb{N}}$

Теорема 4.5. *A - континуально $\Rightarrow$ A^2 - континуально*

Пример.

$$[0,1] \cong [0,1]^2$$

Следствие.

$$(\{0,1\}^{\mathbb{N}})^2 = \{0,1\}^{\mathbb{N}}$$

$$(\alpha,\beta) \leftrightarrow \gamma = \alpha_0\beta_0\alpha_1\beta_1\alpha_2\beta_2\dots$$

$$[0,1] \cong \mathbb{R} \Rightarrow \mathbb{R} \text{ - \textit{континуально}}$$

По индукции:

$$\mathbb{R}^k \cong \mathbb{R}$$

Верно и $\mathbb{R}^{\mathbb{N}} \cong \mathbb{R}$

Доказательство. Док-во конструктивно ИЛИ:

$$\mathbb{R}^{\mathbb{N}} \cong (\mathbb{R}^{\mathbb{N}})^{\mathbb{N}} \cong 2^{\mathbb{N}\times\mathbb{N}} \cong \mathbb{R}$$

□

4.1 Бинарные отношения

Определение 4.2. Отношение - любое $R \in A \times A$

Обозначение. *Отношение* R *между* a *и* b*:*

1) $(a,b) = R$

2) $R(a,b)$

3) aRb

Различные виды отношений:

1) Рефлексивные: $\forall a\colon aRa$

   Пример. $=, \leq, \subset, \cong, \sqsubset$

2) Антирефлексивные: $\forall a\colon \neg(aRa)$

   Пример. $<, \in, ||$

3) Симметричные: $\forall a, \forall b(aRb \to bRa)$

   Пример. $\cong, ||, =, \equiv_k$

4) Антисимметричные: $\forall a, \forall b((aRb \land bRa) \to a = b)$

<u>**Пример.**</u> $\leq, <, >, \sqsubset, \sqsubset, \subset$

5) Транзитивность:

$$\forall a, b, c((aRb \land bRc) \to aRc)$$

<u>**Пример.**</u> $=, \cong, \equiv_k, \leq, \subset, \sqsubset$

6) Антитранзитивность:

$$\forall a, b, c((aRb \land bRc) \to \neg(aRc))$$

$$|a - b| = 1 \text{ (На } \mathbb{R})$$

7) Полнота: $\forall a, b(aRb \lor bRa)$

<u>**Пример.**</u> $\leq$, *(теор. Цермело)*

Наборы св-в:

1) Отнош. эквивалентности: рефлексивность, симметричность, транзитивность.

   <u>**Пример.**</u> $\equiv_k, (\parallel$ *или* $=), \sim$ *(подобие $\triangle$-ов)*

   Общий вид: $f \colon A \to B, x \sim y$, если $f(x) = f(y)$

2) Отношение нестрогого частичного порядка, рефлексивность, антисимметричность, транзитивность:

   <u>**Пример.**</u> $\subset, \leq, \vdots, \sqsubset, \dots$

3) Отнош. строгого част. п-ка: антирефл., антисимметричность, транзитивность

4) Отнош. лин. порядка: нестрогий частичный порядок + полнота

5) Препорядки: рефлексивность, транзитивность

6) Полные предпорядки: полнота + транзитивность

5 Лекция 5

5.1 Отношения эквивалентности ($\sim$)

Определение 5.1. Отношение эквив. - отношение с св-вами:

1) Рефлексивность: $x \sim x$

2) Симметричность: $x \sim y \Rightarrow y \sim x$

3) Транзит.: $x \sim y, y \sim z \Rightarrow x \sim z$

Определение 5.2. Класс эквив.: $K_x = \{ y \mid y \sim x \}$

Теорема 5.1 (О разбиении на классы эквив.)**.** *Если задано отн. экв.* $\sim$ *на* A*, то* A *можно представить как:*

$$A = \bigsqcup_{i \in I} A_i,$$

т. ч.:

1) *Каждая* A_i *-* K_x *для некот.* x

2) $i \neq j \Rightarrow A_i \cap A_j = \emptyset$

3) $y, z \in A_i \Rightarrow y \sim z$

4) $y \in A_i, z \in A_j, i \neq j \Rightarrow y \not\sim z$

Доказательство. Рассм. всевозм. мн-ва, явл-ся классами эквив-ти. Докажем выполн. св-в для них. Для этого докажем леммы I-IV

Лемма 5.2 (I)**.** $x \in K_x$

Доказательство.

$$x \sim x \Rightarrow x \in \{ y \mid y \sim x \} \Rightarrow x \in K_x$$

□

Следствие.

$$\bigsqcup_{x \in A} K_x = A$$

Лемма 5.3 (II).

$$y \in K_x, z \in K_x \Rightarrow y \sim z$$

Доказательство.

$$\begin{cases} y \in K_x \Rightarrow y \sim x \\ z \in K_x \Rightarrow x \sim z \text{ - симметричность} \end{cases} \Rightarrow y \sim z \text{ - транзитивность}$$

□

Лемма 5.4 (III).

$$K_x \neq K_t \Rightarrow K_x \cap K_t = \emptyset$$

Доказательство. Докажем контрапозицию:

$$K_x \cap K_t \ni w \Rightarrow K_x = K_t$$

$$\Rightarrow \begin{cases} w \sim x \\ w \sim t \end{cases} \Rightarrow \begin{cases} w \sim x \\ t \sim w \end{cases} \Rightarrow t \sim x$$

Если $y \in K_t \Rightarrow y \sim t \Rightarrow y \sim x \Rightarrow y \in K_x$, т. е. $K_t \subset K_x$. Аналогично, получаем $K_x \subset K_t \Rightarrow K_x = K_t$ □

Лемма 5.5 (IV).

$$K_x \neq K_t, y \in K_x, z \in K_t \Rightarrow y \not\sim z$$

Доказательство.

$$\begin{cases} y \in K_x \Rightarrow x \sim y \\ y \in K_t \Rightarrow z \sim t \end{cases}$$

Из $y \sim z$, то, по транзитивности, $x \sim t \Rightarrow K_x = K_t$!!!. Т. к. это противоречие, то $y \not\sim z$ □

□

Определение 5.3. Фактормножество $A/_\sim$ - мн-во классов эквив.

Теорема 5.6. *Если $\sim$ - отн. эквив. на A, то сущ. B и $f : A \to B$, т. ч.:*

$$x \sim y \iff f(x) = f(y)$$

Доказательство.

$$B = A/_\sim$$
$$f(x) = K_x$$

□

5.2 Отношение порядка ($\leq$)

Определение 5.4. Отношение порядка - отношение со св-вами:

- Нестрогий порядок $\leq$:
  1) Рефлекивность: $x \leq x$
  2) Антисимм.: $x \leq y \wedge y \leq x \Rightarrow x = y$
  3) Транзтивность: $x \leq y \wedge y \leq z \to x \leq z$
  4) (Для линейных порядков) Полнота: $(x \leq y \vee y \leq x)$
- Строгий порядок $<$:
  1) Антирефлексивность: $\neg(x < x)$
  2) Антисимметричность: $\neg(x < y \wedge y < x)$
  3) Транзитивность: $(x < y \wedge y < z) \to x < z$
  4) (Для линейных порядков) Трихотомичность:

$$x < y \vee y < x \vee x = y$$

Пример. *1) Стандартный числовой порядок в* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

2) $\vdots$ *на* $\mathbb{N}$ *(в том числе включая* 0*)*

$$x \vdots y \iff \exists z \colon x = y \cdot z$$

3) $\subset$ *на* 2^A

4) $\sqsubset, \sqsupset, (substring)$ *на* $\{0, 1\}^n$

5) Асимптот. порядок на ф-циях $f < g$, *если* $\exists N \forall n > N \colon f(n) < g(n)$

6) Пор-ки на $\mathbb{R}^2$*:*

a) Лексикографический:

$$(x_1, y_1) \leq (x_2, y_2) \iff \left[\begin{array}{l} x_1 < x_2 \\ x_1 = x_2 \wedge y_1 \leq y_2 \end{array}\right.$$

b) Покоординатный:

$$(x_1, y_1) \leq (x_2, y_2) \iff \begin{cases} x_1 \leq x_2 \\ y_1 \leq y_2 \end{cases}$$

Диаграмма Хассе: граф на пл-ти, т. ч. вершины, соед. рёрбрами, не находятся на одном уровне (Picture)

Рассм.: $(\{0, 1, \ldots, 9\}, \vdots)$
$x \leq y \iff$ Есть восходящий путь из x в y

Определение 5.5. Наибольший эл-т - Больше всех

$$x \text{ - наиб. } \iff \forall y \colon y \leq x$$

Определение 5.6. Макс. эл-т - больше него нет

$$x \text{ - макс. } \iff \neg \exists y \colon y > x$$

Для лин. порядка - это одно и то же

Для част. порядка - может быть разное, т. е.:

$$\forall y (y \leq x \vee y \text{ не сравним с } x)$$

- макс. эл-т для част. порядка.

Наименьший и **минимальный** - аналогично.

В конечном непустом мн-ве всегда есть макс. и мин.

В конечном мн-ве **единственный** макс. является наибольшим.

Для беск. мн-в всё, что выше, конечно неверно. (picture)

Определение 5.7. Упорядоченное мн-во - пара из мн-ва и порядка на нём.

Обозначение. *Пишут так: $(A, \leq_A)$, сокращённо УМ*

Операции над УМ:

1) Сложение:

$$(A, \leq_A) + (B, \leq_B) = (C, \leq_C)$$

$$C = A \sqcup B$$

$$x \leq y \iff \left[\begin{array}{l} x, y \in A\colon x \leq_A y \\ x, y \in B\colon x \leq_B y \\ x \in A, y \in B \end{array}\right.$$

При этом оно:

- Ассоциативно: $A + (B + C) = (A + B) + C$
- **Некоммутативно:** $A + B \neq B + A$

2) Умножение:

$$(A, \leq_A) \cdot (B, \leq_B) = (C, \leq_C)$$

$$C = A \times B$$

$$(a_1, b_1) \leq_C (a_2, b_2) \iff \left[\begin{array}{l} b_1 <_B b_2 \\ b_1 = b_2, a_1 \leq_A a_2 \end{array}\right.$$

6 Лекция 6

6.1 Плотный порядок. Изоморфизм

Отношение частичного порядка:

1) $x \leq x$ - рефлексивность

2) $(x \leq y \wedge y \leq x) \Rightarrow x = y$ - антисимметричность

3) $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$ - транзитивность

Отношение линейного порядка:

4) $\forall x, y\colon x \leq y \vee y \leq x$

Упор. мн-во $(A, \leq_A)$
Наибольший эл-т - $M\colon \forall x, x \leq M$.
Наименьший эл-т - $m\colon \forall x, x \geq m$
Максимальный эл-т - $M\colon \neg\exists x\colon x > M$ (или $\forall x\colon x \leq M \vee$($x$ не сравним с M))
Минимальный эл-т $m\colon \neg\exists x\colon x < m$

Определение 6.1. Плотный порядок:

$$\forall x, y(x < y \to \exists z \colon x < z < y)$$

Утверждение 6.1. *Плотный порядок - либо тривиальный (т. е. разлные эл-ты не сравнимы), либо опр. на бесконечном мн-ве.*

Определение 6.2. Изоморфизм упор. мн-в $(A, \leq_A)$ и $(B, \leq_B)$ - это такая биекция $f : A \to B$, что:

$$\forall x, y \colon (x \leq_A y \iff f(x) \leq_B f(y))$$

Пример.

$$(\{\, n \mid 30 \vdots n \,\}, \vdots) \text{ и } (2^{\{\, a,b,c \,\}}, \subset)$$

Пример.

$$(\mathbb{Q} \cap (0,1), \leq) \text{ и } (\mathbb{Q} \cap (0,+\infty), \leq)$$

$$x \mapsto \frac{1}{1-x} - 1$$

Теорема 6.1. *Любые два счётных плотно, линейно упоряд. мн-ва без наиб. и наим. эл-тов изоморфны:*

Пример.

$$\mathbb{Q}, \mathbb{Q}_2 = \{\, \frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N} \,\}, \mathbb{Q}[\sqrt{2}] = \{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q} \,\},$$

$\mathbb{A}$ - *корни мн-ов с целыми коэфф-ми*

Доказательство.

$$A = \{\, a_0, a_1, \dots \,\}, B = \{\, b_0, b_1, \dots \,\}$$

Построим **инъекцию** f:

1) Построим $a_0 \to b_0$

2) Б. О. О. $a_1 > a_0$. Т. к. в B нет наибольшего, то есть $b_i \colon b_i > b_0$. Тогда добавим $a_1 \to b_i$

3) Пусть для $a_k, k \leq n-1$ соединения проведены. Проведём для a_n. Рассм. три случая:

I) $a_n < a_k, \forall k \leq n-1$. Тогда отобразим его в b_p: $b_p < b_i, \forall i$ из использованных ранее.

II) $a_n > a_k, \forall k \leq n-1$. Тогда отобразим его в b_p: $b_p > b_i, \forall i$ из использованных ранее.

III) Иначе у a_n есть использованные ранее соседи a_i и a_j. Т. к. A и B - лин. упор.: $\exists p$: $f(a_i) < b_p < f(a_j)$. Добавим $a_n \to b_p$

Как добиться, чтобы постр. ф-ция была сюрьекцией? Варианты:

1) Каждый раз брать эл-т B с наим номером из подходящих.

2) Действовать по очереди: сначала брать эл-т A с наим. номером, кот. ещё не рассмотрен, и отправлять в B. Затем эл-т B с наим. номером, кот. ещё не рассм, и отправлять в A. И т. д.

□

6.2 Предпорядки

Определение 6.3. Предпорядок (Предпочтения) - отношение, обладающее рефлексивностью и транзитивностью.

Определение 6.4. Полный предпорядок (Рациональные предпочтения) - предпорядок + любые два сравнимы. (или полн. + транз.)

Обозначение.

$$a \succsim b \text{ - предпор.}$$

$$a \sim b \iff (a \succsim b \wedge b \succsim) \text{ - отношение безразличия}$$

$$a \succ \iff (a \succ b \wedge \neg(b \succ a)) \text{ - строгий предпорядок}$$

Нетранзитивно: $a \succ b \succ c \succ a$

Теорема 6.2 (Структурная теорема о предпорядке на мн-ве A)**.**

1) Отношение безразличия - это отношение эквив-ти на A

2) На эл-ах $A/_\sim$ можно ввести отношение
$S \leq T$, если $\exists x \in S, y \in T$: $x \precsim y$
Это отнош. будет част. пор. на $A/_\sim$

3) $\leq$ *лин. пор.* $\iff$ $\precsim$ *- полон.*

Доказательство.

- 1) Рефл.: $a \precsim a \Rightarrow (a \precsim a \wedge a \precsim a) \Rightarrow a \sim a$

  2) Симм.:

  $$a \sim b \iff (a \precsim b \wedge b \precsim a) \iff (b \precsim a \wedge a \precsim b) \iff b \sim a$$

  3) Транзитивность:

  $$\begin{cases} a \sim b \\ b \sim c \end{cases} \iff \begin{cases} a \precsim b \wedge b \precsim a \\ b \precsim c \wedge c \precsim b \end{cases} \iff \begin{cases} a \precsim c \\ c \precsim a \end{cases} \Rightarrow a \sim c$$

- 1) Рефл $S \neq \emptyset \Rightarrow \exists x \in S \Rightarrow$ т. к. $x \precsim x \Rightarrow S \leq S$

  2) Транз. $R \leq S \leq T$:

  $$\begin{cases} x \in R \\ y, z \in S \\ t \in T \\ x \precsim y \\ z \precsim t \end{cases} \Rightarrow y \precsim z \Rightarrow x \precsim t \Rightarrow R \leq T$$

  3) Антисимм.:

  $$S \leq T, T \leq S$$

  $$\begin{cases} x \in S, y \in T \Rightarrow x \precsim y \\ z \in T, t \in S \Rightarrow z \precsim t \\ x \sim t \\ y \sim z \end{cases} \Rightarrow y \sim z \precsim t \sim x \Rightarrow y \precsim x \Rightarrow x \sim y \Rightarrow S = T$$

- $\Leftarrow$) S, T - классы

  $$x \in S, y \in T:$$

  Если $x \precsim y \Rightarrow S \leq T$
  Если $y \precsim x \Rightarrow T \leq S$

$\Rightarrow$) Даны x, y:

$$x \in S, y \in T, \text{ б. о. о. } S \leq T$$

$$\Rightarrow \exists z \in S, t \in T : z \precsim t$$

$$x \sim z \precsim t \sim y \Rightarrow x \precsim y$$

S - класс эквив., T - класс эквив.

□

6.2.1 Агрегирование предпорядков

A - мн-во, $\precsim_1, \ldots, \precsim_n$ - препорядки $\Rightarrow$
$F : (\precsim_1, \precsim_2, \ldots, \precsim_n) \mapsto \precsim$

Определение 6.5. Агрегирование по больш-ву:

$$x \trianglelefteq y, \text{ если } \#\{\, i \mid x \precsim_i y \,\} \leq \#\{\, i \mid y \precsim_i x \,\}$$

Парадокс Кондорсе:

$$\begin{cases} a \precsim_1 b \precsim_1 c \\ b \precsim_2 c \precsim_2 a \\ c \precsim_3 a \precsim_3 b \end{cases} \Rightarrow a \trianglelefteq b \trianglelefteq c \trianglelefteq a$$

Теорема 6.3. *Любое полное отношение может быть реализовано как результат агрегирование предпорядков*

Доказательство. Эл-ты $x, y, a_1, a_2, \ldots, a_{n-2}$. Также есть два предпорядка $\prec$ и $\prec'$, т. ч.:

$$x \prec y \prec a_1 \prec \ldots \prec a_{n-2}$$

$$a_{n-2} \prec' a_{n-3} \ldots a_2 \prec a_1 \prec x \prec y$$

□

7 Лекция 7

7.1 База

Сложение, умножение.
Прицнип Дирихле.
$\{ a_1, \dots, a_n \}$
Сочетания: без и с повторениями.
Размещения: без и с повторениями.
C_n^k - число сочет. без повтор. (или $\binom{n}{k}$)
$\overline{C_n^k}$ - число сочет. с повт.

Теорема 7.1.

$$\overline{A_n^k} = n^k$$

$$A_n^k = n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}$$

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$$

$$\overline{C_n^k} = C_{n+k-1}^k$$

Доказательство. Для док-ва последнего, сделаем биекцию:

$$\text{k-сочет с повтор.} \longleftrightarrow \text{п-сть из 0 и 1 длины } n+k-1 \text{ с } k \text{ ед-цами.}$$

Пример.

$$n = 26, \{ a, b, c, \dots \}, k = 4, \{ m, a, m, a \}$$

$$\underset{a}{110}\,\underset{b}{0}\,\underset{c}{0}\dots0\underset{m}{110}\dots\underset{y}{0}\,\underset{z}{0}$$

□

$$V = \{ \overline{x} = (x_1, \dots, x_8) \colon \forall i, x_i \in \{ -1, 0, 1 \}, x_1^2 + \dots x_8^2 = 4 \}$$

$$|V| = C_8^4 \cdot 2^4 = 1120$$

$$(\overline{x}, \overline{y}) = x_1 y_1 + \dots + x_8 y_8$$

Рассм. произв. $W \subset V \colon \forall \overline{x}, \overline{y} \in W \colon (\overline{x}, \overline{y}) \neq 0$

Утверждение 7.1. $\forall W: \ |W| \leq 140$

Задача 7.1. $\{1, 2, \ldots, 30\}$
$M_1, \ldots, M_{15}$ - различные 5-сочет.
Можно ли покрасить числа 1, .., 30 в 2 цвета, чтобы все M_i были неоднoцветными?

Решение. *Всего раскрасок:* 2^{30}
Кол-во раскрасок, в кот-ых M_i *закрашено в один цвет:* 2^{26}
Кол-во раскрасок, в кот-ых хотя бы одно M_i *закрашено в один цвет:*

$$\textit{кол-во} \leq 2^{26} \cdot 15 < 2^{30}$$

Тождества:

1)
$$C_n^k = C_n^{n-k}$$

2)
$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

8 Лекция 8

8.1 Продоложние про тождества

3)
$$C_n^0 + C_n^1 + C_n^2 + \ldots C_n^n = 2^n$$

4)
$$(C_n^0)^2 + \ldots + (C_n^n)^2 = C_{2n}^n$$

Доказательство. 4) Рассм. $\{a_1, \ldots, a_{2n}\}$

Выберем из этого мн-ва все возм. n-сочетания без повторений.
Их C_{2n}^n

$$\{\underbrace{a_1, \ldots, a_n}_{k \text{ объектов}}; \underbrace{a_{n+1}, \ldots a_{2n}}_{n-k \text{ объектов}}\}$$

Из левой половины выбираем k обЪектов, из левой соотв. - $n-k$. Кол-во способов так сделать:

$$C_n^k C_n^{n-k} = (C_n^k)^2$$

Складывая по всем k:

$$\sum_{k=0}^{n} (C_n^k)^2 = C_{2n}^n$$

$\square$

Вопрос: $\sum_{k=0}^{n} (C_n^k)^4$

5) Рассм. $\{a_1, \ldots, a_n, a_{n+1}\}$. Выберем из этого мн-ва все возможные m-сочетания с повторениями. Их:

$$\overline{C_{n+1}^m} = C_{n+m}^m = C_{n+m}^n$$

Для $k = 0, 1, \ldots, m$ рассм. по отдельности все m-сочет. с повторениями, в каждом из которых ровно k объектов a_1. Их:

$$\overline{C_n^{m-k}} = C_{n+m-k-1}^{m-k} = C_{n+m-k-1}^{n-1}$$

Получаем тождество:

$$\sum_{k=0}^{m} C_{n-1+m-k}^{n-1} = C_{n+m}^n$$

Следствие.

$$n = 1\colon 1 + 1 + \underset{m+1}{1} + \ldots + 1 = C_{m+1}^1$$

$$n = 2\colon (m+1) + (m) + \ldots + 1 = C_{m+2}^2 = \frac{(m+2)!}{2!m!} = \frac{m(m+1)}{2}$$

$$n = 3\colon \text{ *Сумма квадратов :)* }$$

6) Полиномиальная ф-ла:

$$(x_1 + \ldots + x_k)^n = \underbrace{(x_1 + \ldots + x_k) \ldots (x_1 + \ldots + x_k)}_{\text{n раз}}$$

Задача 8.1. Комбинаторная задача: посчитать кол-во способов получить из слова КОМБИНАТОРИКА перестановкой букв разные слова.

Решение. *Всего букв: 13.*

к - 2
о - 2
м - 1
б - 1
и - 2
а - 2
н - 1
т - 1
р - 1

$$\Rightarrow C_{13}^2 C_{11}^2 C_9^1 \dots C_1^1 = \frac{13!}{2!2!1!1!\dots 1!}$$

Задача 8.2. Даны n_1 объектов a_1, n_2 объектов a_2, $\dots n_k$ объектов a_k. Сколько способов сформировать n-ти из этих объектов.

Решение. $P(n_1, n_2, \dots, n_k)$ *- кол-во способов сформировать n-ть из наших объектов.*

Теорема 8.1.

$$P(n_1, \dots, n_k) = \frac{n!}{n_1! \dots n_k!}$$

Тогда:

$$(x_1 + \dots + x_k)^n = \underbrace{(x_1 + \dots + x_k) \dots (x_1 + \dots + x_k)}_{\text{n раз}} = \dots + P(n_1, \dots, n_k) x_1^{n_1} \dots x_k^{n_k},$$

$$P(n_1, \dots, n_k) \text{ - полиномиальный коэфф.}$$

$$n_1 \text{ - кол-во скобок, из кот. взяли } x_1$$

$$n_2 \text{ - ... } x_2$$

$$\vdots$$

$$n_k \text{ - ... } x_k$$

$$n_1 + \dots + n_k = n, \forall i, n_i \geq 0 \Rightarrow x_1^{n_1} \dots x_k^{n_k}$$

6)

$$\sum_{n_1+\ldots+n_k=n} P(n_1,\ldots,n_k) = k^n$$

7) Ф-ла включений-исключений: есть N объектов и $\alpha_1,\ldots,\alpha_n$ - св-ва:

Теорема 8.2.

$N(\alpha'_1,\ldots,\alpha'_n) = N - N(\alpha_1) - \ldots - N(\alpha_n) + N(\alpha_1,\alpha_2) + \ldots + N(\alpha_{n-1},\alpha_n) - \ldots + (-1)^n N(\alpha_1,\ldots,$

$$N(\alpha'_1,\ldots,\alpha'_n) =$$

Доказательство. Индукция по числу свойств:

– База:

$$n = 1\colon N(\alpha'_1) = N - N(\alpha_1)$$

– Переход:

$$\forall N, \forall a_1,\ldots,a_N, \forall k \leq n-1, \forall \alpha_1,\ldots\alpha_k \text{ - выполнена теорема.}$$

Берём произв. $N, a_1,\ldots,a_N, \alpha_1,\ldots,\alpha_n$. Рассм. св-ва $\alpha_1,\ldots\alpha_{n-1}$:

$$N(\alpha'_1,\ldots,\alpha'_{n-1}) = N - N(\alpha_1) - \ldots - N(\alpha_{n-1}) + \ldots + (-1)^{n-1} N(\alpha_1,\ldots,\alpha_{n-1}) \quad (1)$$

Выберем из $a_1,\ldots,a_N$ те объекты, кот. обладают св-вом α_n.
Их $N(\alpha_n) = M$, обозначим их, как: $b_1,\ldots,b_M$:

$M(\alpha'_1,\alpha'_2,\ldots\alpha'_{n-1}) = M - M(\alpha_1) - M(\alpha_2) - \ldots - M(\alpha_{n-1}) + \ldots + (-1)^{n-1}(M(\alpha_1,\ldots,\alpha_{n-1}$

$= N(\alpha'_1,\ldots,\alpha'_{n-1},\alpha_n) = N(\alpha_n) - N(\alpha_1,\alpha_n) - \ldots - N(\alpha_{n-1},\alpha_n) + \ldots + (-1)^{n-1}(N(\alpha_1,\ldots,$ (2)

Тогда, чтобы получить $N(\alpha'_1,\ldots,\alpha'_n)$, вычислим (1) - (2):

$N(\alpha'_1,\ldots,\alpha'_n) = N - N(\alpha_1) - \ldots - N(\alpha_n) + N(\alpha_1,\alpha_2) + \ldots + N(\alpha_{n-1},\alpha_n) + \ldots + (-1)^n N(\alpha_1$

□

9 Лекция 9

7)

$$C_n^0 - C_n^1 + \ldots + (-1)^n C_n^n = \begin{cases} 1, n = 0 \\ 0, n > 0 \end{cases}$$

8) Рассм. $A = \{ a_1, \ldots, a_n \}, m < n, m > 0$. Выберем из A все возм. m-разм. с повтор. Их n^m. $N = n^m, \alpha_1, \ldots \alpha_m$. Размещ. обладает св-вом $\alpha_i \iff \alpha_i \notin$ размещению.

$$N(\alpha_i) = (n-1)^m, N(\alpha_i, \alpha_j) = (n-2)^m$$

$$N(\alpha_1', \ldots, \alpha_n') = 0$$

По формуле вкл.-искл.:

$$N(\alpha_1', \ldots, \alpha_n') = n^m - n(n-1)^m + C_n^2(n-2)^n + \ldots$$

$$\Rightarrow 0 = \sum_{k=0}^{n} (-1)^k C_n^k (n-k)^m$$

Задача 9.1. Задача о беспорядках:

Определение 9.1. Беспорядок - перестановка, при кот. $\sigma_i \neq i, \forall i = \overline{1, n}$

Найдём кол-во беспорядков для $n = 100$: . Пусть α_i - св-во, при кот. $\sigma_i = i$, посчитаем:

$$N = 100!$$

$$N(\alpha_1', \alpha_2', \ldots, \alpha_n') = 100! - 99! * 100 + C_{100}^2 \cdot 98! - \ldots = \sum_{k=0}^{n} C_n^k (n-k)! = !n$$

При раскрытии C-шек, получаем:

$$N(\alpha_1', \ldots, \alpha_n') = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{1}{100!} \approx \frac{1}{e}$$

"Физической интуицией"получаем:

$$\left(1 - \frac{1}{100}\right)^{100} \approx \frac{1}{e}$$

9.1 Циклические n-ти

Алфавит: $X = \{ b_1, \dots, b_r \}$. Из b-шек составляем слова длины n.

$$a_1 a_2 \dots a_n, \forall i, a_i \in X$$

$$a_1 \to a_2 \to a_3 \to \dots \to a_{n-1} \to a_n \to a_1$$

Т. е. $a_1 \dots a_n$ отождествляется с $a_2 \dots a_n a_1$, $a_3 \dots a_n a_1 a_2, \dots$.
Однако r^n - кол-во обычных слов, т. е. n не всегда делит r^n.

Пример.

$$r = 3, X = \{ C, O, H \}, n = 4:$$

Следующие слова нужно поделить на 4:

$$COCH$$

$$OCHC$$

$$CHCO$$

$$HCOC$$

Эти на 2:

$$COCO$$

$$OCOC$$

А это на 1:

$$CCCC$$

Для решение этой задачи, для начала, изучим следующий мощный инструмент:

9.2 Формула обращения Мёбиуса

Теорема 9.1 (ОТА)**.**

$$\forall n \geq 2, \exists! \{ p_1, \dots p_s \}, \{ a_1, \dots a_s \}:$$

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$$

*(Это наз-ся **каноническим разложением** n)*

Определение 9.2. Функция Мёбиуса $\mu(n)$:

$$\mu(n) = \begin{cases} 1, n = 1 \\ (-1)^s, n = p_1 \cdot \ldots \cdot p_s \\ 0, \text{ иначе} \end{cases}$$

Лемма 9.2.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, n = 1 \\ 0, \text{ \textit{иначе}} \end{cases}$$

Доказательство. Пусть $n \geq 2 \Rightarrow n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$

$$(d|n) \Rightarrow (d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}, \forall i, 0 \leq \beta_i \leq \alpha_i)$$

$$\sum_{d|n} \mu(d) = \sum_{\beta_1=0}^{\alpha_1} \ldots \sum_{\beta_k=0}^{\alpha_k} \mu(p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}) = \sum_{\beta_1=0}^{1} \ldots \sum_{\beta_k=0}^{1} \mu(p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k})$$

$$= \mu(1) + C_k^1(-1) + C_k^2(-1)^2 + \ldots + C_k^k(-1)^k = \sum_{i=0}^{k} (-1)^k C_k^i = 0$$

□

Теорема 9.3 (Формула обращения Мёбиуса)**.** *Пусть $f = f(n)$ - ф-ция $n \in \mathbb{N}$. Пусть $g(n) = \sum_{d|n} f(d)$. Тогда:*

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Доказательство.

$$\sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{(d,d') \colon d \cdot d'|n} \mu(d) f(d') = \sum_{d|n} f(d) \sum_{d'|\frac{n}{d}} \mu(d') =$$

$$= f(n) \cdot \sum_{d'|1} \mu(d') + \sum_{d|n, d<n} f(d) \sum_{d'|\frac{n}{d}} \mu(d') = f(n) \cdot 1 + \sum_{d|n, d<n} f(d) \cdot 0 = f(n)$$

□

10 Лекция 10

Вспоминаем задачу:

$$X = \{ b_1, \ldots, b_r \} \text{ - алфавит}$$

$$n, a_1, \ldots, a_n \text{ — линейная последовательность}$$

П-ть r^n:

$$(a_1, \ldots, a_n)$$

Циклический сдвиг $a_1, \ldots, a_n \to a_2, a_3, \ldots, a_n, a_1$

Определение 10.1. Обозначаем как d — **период линейной п-ти**, т. е. min кол-во циклических сдвигов, переводящих её в себя.

Лемма 10.1. $d|n$

Доказательство. Предположим, что $n = kd + r, 1 \leq r < d$. Тогда, сдвинув $a_1, \ldots, a_n$ на d, k раз, получим исходную п-ть. Сдвинув на n 1 раз, тоже получаем исх. п-ть. Отсюда, получаем, что сдвигая $a_1, \ldots, a_n$ на $n - k \cdot d = r$, тоже получ. исх. п-ть. Но $r < d$ — противоречие. □

Лемма 10.2. *$a_1, \ldots, a_n$ - периода d, то она представляется, как $\frac{n}{d}$ одинаковых кусков длины d:*

$$a_1, \ldots, a_n = a_1, \ldots a_d, a_{d+1}, \ldots, a_{2d}, a_{2d+1}, \ldots$$

Доказательство. Очев. □

Пусть V - мн-во всех линейных п-тей сост. из нашего алфавита (т. е. $|V| = r^n$)

$$1 = d_1 < d_2 < d_3 \ldots < d_s = n \text{ - все делители числа } n$$

$$V_i = \{ \{ a_n \} \in V \mid \{ a_n \} \text{ - имеет период } d_i \}$$

$$V = V_1 \sqcup V_2 \sqcup V_3 \sqcup \ldots \sqcup V_s$$

$$\Rightarrow r^n = |V_1| + \ldots + |V_s|$$

Пусть W_i - мн-во лин п-тей длины d_i и периода d_i

$$|W_i| = |V_i|$$

$$\Rightarrow r^n = |W_1| + \ldots + |W_s|$$

Обозначим U_i - мн-во различных цикл. п-тей, кот. отвечают лин. п-тям из W_i. Тогда очевидно, что:

$$\frac{|W_i|}{d_i} = |U_i|$$

Введём обозначение:

$$M(d_i) = |U_i|$$

Получаем:

$$r^n = d_1 M(d_1) + d_2 M(d_2) + \ldots d_s M(d_s)$$

$$r^n = \sum_{d|n} d M(d)$$

Напомним ф-лу обращения Мёбиуса:

$$g(n) = \sum_{d|n} f(d) \Rightarrow$$

$$\Rightarrow f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Получаем:

$$nM(n) = \sum_{d|n} \mu(d) \cdot r^{\frac{n}{d}}$$

$$M(n) = \frac{1}{n} \sum_{d|n} \mu(d) \cdot r^{\frac{n}{d}}$$

Тогда ответ, т. е. кол-во циклических п-тей длины n, представим как теорему:

Теорема 10.3.

$$T_r(n) = \sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \left(\sum_{d'|d} \mu(d') r^{\frac{d}{d'}} \right)$$

10.1 Обращение Мёбиуса на чуме (част. уп. мн-во)

$$\mathscr{P} = (A, \preceq)$$

Локально конечный: $\forall y \in A$

$$|\{ x \preceq y \}| < \infty$$

$$(\mathbb{N}, \leq), (\mathbb{N}, |)$$
$$(2^{\{1,2,\ldots,n\}}, \subseteq)$$

10.1.1 Ф-ция Мёбиуса

$$x, y \in \mathbb{A}, x \preceq y$$

$$\mu(x, x) = 1$$

$$x \prec y \colon \mu(x, y) = -\sum_{z \colon x \preceq z \prec y} \mu(x, z)$$

Теорема 10.4. *Если $\mu(x, y)$ - это ф-ция Мёбиуса на $(\mathbb{N}, |)$, а $\mu(n)$ - обратная ф-ция Мёбиуса, тогда:*

$$\mu(x, y) = \mu\left(\frac{y}{x}\right)$$

Доказательство.

$$\mu(x, x) = \mu\left(\frac{x}{x}\right) = 1$$

Индукция по величине $\frac{y}{x}$:

$$\mu(x, y) = -\sum_{z \colon x \preceq z \prec y} \mu(x, z) = -\sum_{z \colon x \preceq z \prec y} \mu\left(\frac{z}{x}\right)$$

Распишем $y = x \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Тогда:

$$\frac{z}{x} = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}, \exists i \colon \beta_i < \alpha_i$$

Рассм. несколько случаев:

1) $\alpha_1 = \ldots = \alpha_s = 1$. Тогда:

$$-\sum_{\ldots} \mu\left(\frac{z}{x}\right) = -\sum_{\beta_1=0}^{1} \ldots \sum_{\beta_s=0}^{1} \mu\left(p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\right) + \mu\left(p_1 \cdot \ldots \cdot p_s\right)$$

В рамках док-ва ф-лы обращ. Мёбиуса, страшная сумма слева $= 0$. Получаем:

$$= \mu(p_1 \cdot \ldots \cdot p_s)$$

2) $\exists i \colon \alpha_i > 1$. Тогда всё то же самое, как и в случае 1 (по опр. ф-ции Мёбиуса)

$\square$

Теорема 10.5 (Ф-ла обращения Мёбиуса)**.** *Пусть* $g(y) = \sum_{x \preceq y} f(x)$. *Тогда:*

$$f(y) = \sum_{x \preceq y} \mu(x, y) g(x)$$

Доказательство.

$$\sum_{x \preceq y} \mu(x,y) \cdot g(x) = \sum_{x \preceq y} \mu(x,y) \cdot \sum_{z \preceq x} f(z) = \sum_{(x,z) \colon z \preceq x \preceq y} \mu(x,y) \cdot f(z) =$$

$$= \sum_{z \preceq y} f(z) \left(\sum_{x \colon z \preceq x \preceq y} \mu(x,y) \right) = f(y) + \sum_{z \prec y} f(z) \left(\sum_{x \colon z \preceq x \preceq y} \mu(x,y) \right)$$

Док-во сводится к лемме:

Лемма 10.6.

$$\forall z, y \colon z \prec y$$

$$\sum_{x \colon z \preceq x \preceq y} \mu(x,y) = I_{z=y}$$

$\square$

11 Лекция 11

<u>Лемма</u> 11.1.

$$\sum_{x\preceq z\preceq y}\mu(z,y)=I_{x=y}$$

Доказательство. $x\prec y$
Докажем индукцие по длине самой <u>длинной</u> цепочки вида:

$$x\prec x_1\prec x_2\prec\ldots\prec x_k\prec y$$

- База индукции: $x\prec y$, а между ними ничего нет.

$$\sum_{x\preceq z\preceq y}\mu(z,y)=\mu(y,y)+\sum_{x\preceq z\prec y}\mu(z,y)=1+\mu(x,y)=1-\sum_{x\preceq z\prec y}\mu(x,z)=$$

$$=1-\mu(x,x)=0$$

- Шаг индукции:

$$\sum_{x\preceq z\preceq y}\mu(z,y)=1+\sum_{x\preceq z\prec y}\mu(z,y)=1-\sum_{x\preceq z\prec y}\sum_{z\preceq u\prec y}\mu(z,u)=$$

$$=1-\sum_{x\preceq u\prec y}\sum_{x\preceq z\prec u}\mu(z,u)=1-\sum_{x\preceq u\prec y}I_{x=u}=1-1=0$$

□

<u>Теорема</u> 11.2. ***Формула обращения Мёбиуса:***

$$g(y)=\sum_{x\preceq y}f(x)\Rightarrow f(y)=\sum_{x\preceq y}\mu(x,y)g(x)$$

<u>Пример</u>. *Рассм. чум:*

$$(2^{\{1,2,\ldots,n\}},\subseteq)$$

Пусть есть ещё некоторые мн-ва $A_1,\ldots,A_n$. Определим также ф-ции:

$$I\in 2^{\{1,2,\ldots,n\}}$$

$f(I)$ — кол-во эл-ов мн-в $A_1, \dots, A_n$, к-рые принадлежат всем таким A_i, что $i \notin I$, т. е.:

$$f(I) = \left|\bigcap_{i \notin I} A_i\right|$$

$$f(\{\,1, 2, \dots, n\,\}) = \left|\bigcup_{i=1}^{n} A_i\right|$$

$g(I)$ — кол-во эл-ов мн-в $A_1, \dots, A_n$, кот-рые принадлежат таким A_i, что $i \notin I$, и не принадлежит всем остальным A_i.

$$f(I) = \sum_{I' \subseteq I} g(I')$$

$$n = 4\colon A_1, \dots, A_4$$

$$I = \{\,1, 2\,\}, f(I) = |A_3 \cap A_4|$$

$$(I' \subseteq I) \iff (I' \in \{\,\{\,1, 2\,\}, \{\,1\,\}, \{\,2\,\}, \emptyset\,\})$$

$$g(\{\,1, 2\,\}) = |A_3 \cap A_4 \backslash A_1 \backslash A_2|$$

$$g(\{\,1\,\}) = |A_2 \cap A_3 \cap A_4 \backslash A_1|$$

$$g(\{\,2\,\}) = |A_1 \cap A_3 \cap A_4 \backslash A_2|$$

$$g(\emptyset) = |A_1 \cap A_2 \cap A_3 \cap A_4|$$

$$g(\{\,1, 2, \dots, n\,\}) = 0$$

Применим ФОМ (ф-лу обращения Мёбиуса):

$$g(I) = \sum_{I' \subseteq I} \mu(I', I) f(I')$$

$$I = \{\,1, 2, \dots, n\,\} \Rightarrow g(I) = 0 = \sum_{I' \subseteq \{\,1,2,\dots,n\,\}} \mu(I', \{\,1, 2, \dots, n\,\}) \cdot f(I') =$$

<u>Лемма</u> 11.3.

$$\mu(I', \{\,1, 2, \dots, n\,\}) = (-1)^{|I| - |I'|}$$

Доказательство. Индукция по $|I| - |I'|$:

- Шаг:

$$I' \subset I \colon \mu(I', I) = -\sum_{I' \subseteq I'' \subset I} \mu(I', I'') = -\sum_{I' \subseteq I'' \subset I} (-1)^{|I''|-|I'|}$$

$$|I''| = |I'|\,, |I'| - 1, \ldots, |I| - 1$$

$\Rightarrow$ Кол-во I'' мощности k: $C_{|I|-|I'|}^{k-|I'|}$

$$\Rightarrow -\sum_{I' \subseteq I'' \subset I} (-1)^{|I''|-|I'|} = -\sum_{k=|I'|}^{|I|-1} C_{|I|-|I'|}^{k-|I'|} (-1)^{k-|I'|} = \big[l = |I'|\big] = -\sum_{l=0}^{|I|-|I'|-1} C_{|I|-|I'|}^{l} (-1)^{l} = (0$$

$$= (-1)^{|I|-|I'|}$$

$\square$

$$= \left| \bigcup_{i=1}^{n} A_i \right| + \sum_{I' \subseteq \{\,1,2,\ldots,n\,\}} (-1)^{n-|I'|} \cdot \left| \bigcap_{i \notin I'} A_i \right|$$

11.1 Линейные рекуррентные соотношения с постоянными коэффициентами

$$F_{n+2} = F_{n+1} + F_n, F_0 = 0, F_1 = 1$$

Последовательность $\{\, y_n \,\}_{n=0}^{\infty}$ удовл. лин. рек. соотношению k-ого порядка с коэф. $a_1, \ldots, a_k \in \mathbb{R}$, если $\forall n$:

$$a_k y_{n+k} + a_{k-1} y_{n+k-1} + \ldots + a_1 y_{n+1} + a_0 y_n = 0$$

$$k = 1 \colon a_1 y_{n+1} + a_0 y_n = 0 \Rightarrow y_n = \left(-\frac{a_0}{a_1}\right) y_0$$

$$k = 2 \colon a_2 y_{n+2} + a_1 y_{n+1} + a_0 y_n = 0$$

Алгоритм:

1) Составим ур-е:

$$a_2 x^2 + a_1 x + a_0 = 0$$

$$a_2 (x - \lambda_1)(x - \lambda_2) = 0$$

I) $\lambda_1 \neq \lambda_2$

Теорема 11.4. *1) $\forall c_1, c_2 \in \mathbb{R}$ п-ть, задающая ф-лой $y_n = c_1\lambda_1^n + c_2\lambda_2^n$ удовл. рекурсии.*

2) Если $\{ y_n \}_{n=0}^{\infty}$ удовл. рек. соотнош., то $\exists c_1, c_2$:

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n$$

Доказательство. 1)

$$a_2(c_1\lambda_1^{n+2} + c_2\lambda_2^{n+2}) + a_1(c_1\lambda_1^{n+1} + c_2\lambda_2^{n+1}) + a_0(c_1\lambda_1^n + c_2\lambda_2^n) =$$

$$= c_1\lambda_1^n(a_2\lambda_1^2 + a_1\lambda_1 + a_0) + c_2\lambda_2^n(a_2\lambda_2^2 + a_1\lambda_2 + a_0) = 0 + 0 = 0$$

2) Сост. систему:

$$\begin{cases} c_1 + c_2 = y_0 \\ c_1\lambda_1 + c_2\lambda_2 = y_1 \end{cases}$$

$$y_n^* = c_1^*\lambda_1^n + c_2^*\lambda_2^n, c_1^*, c_2^* \text{ - решение системы}$$

По п. 1, это соотнош. удовл. рек. соотнош. $\Rightarrow y_n = y_n^* \Rightarrow$ Победа.

□

12 Лекция 12

$$a_k y_{n+k} + a_{k-1}y_{n+k-1} + \ldots + a_0 y_n = 0 \tag{3}$$

Хар-ое ур-ие:

$$a_k x^k + \ldots + a_0 = 0$$

Теорема 12.1 (Основная теорема алгебры). *Мн-н степени k имеет k комплексных корней, т. е.:*

$$P(x) = a_k x^k + \ldots + a_0 = a_k \prod_{i=0}^{k} (x - \lambda_i)$$

где,

$$P(\lambda_i) = 0, \lambda_i \in \mathbb{C}$$

Возьмём эти корни из хар-ого ур-ия. Пусть:

$$\mu_1, \ldots, \mu_r$$

Этот же список корней, без **дубликатов**. Также:

$$m_1, \ldots, m_r$$

Это кратности этих корней.

$$1 \le r \le k$$

$$\sum_{i=1}^{r} m_i = k$$

Обозначим за:

$$P_l(n) = c_l n^l + \ldots + c_0$$

— произвольный мн-н степени l

Теорема 12.2. *1)*

$$\forall P^1_{m_1-1}(n), \ldots, P^r_{m_r-1}(n)$$
$$\hookrightarrow y_n = P^1_{m_1-1}(n)\mu_1^n + \ldots + P^r_{m_r}(n)\mu_r^n$$

— *удовлетворяет* (3)

2) Если $\{ y_n \}_{n=1}^{\infty}$ *удовл.* (3), *то* $\exists P^1_{m_1-1}, \ldots, P^r_{m_r-1}$:

$$y_n = < \text{ запись из п. 1} >$$

12.1 Разбиение чисел на слагаемые

$$n \in \mathbb{N} \colon n = x_1 + \ldots + x_t$$
$$\forall i \colon x_i \in \{ n_1, \ldots, n_k \}$$

(***Офигенные примеры с помидором и попойкой***)

Теорема 12.3 (Решение попойки (упор. разбиений))**.**

$$F(n; n_1, \ldots, n_k) = F(n - n_1; n_1, \ldots, n_k) + \ldots + F(n - n_k; n_1, \ldots, n_k)$$

$$F(0; n_1, \ldots, n_k) = 1; F(-n; n_1, \ldots, n_k) = 0$$

Следствие.

$$F(n; , 1, 2, \ldots, n) = 2^{n-1}$$

Доказательство. ММИ:

1) $n = 1$: $F(1; 1) = 1 = 2^{1-1}$

2)
$$F(n; 1, \ldots, n) = F(n-1; 1, \ldots, n-1) +$$
$$+ F(n-2; 1, 2, \ldots, n-2) + \ldots + F(1; 1) + F(0; 0) =$$
$$= 2^{n-2} + 2^{n-1} + \ldots + 1 + 1 = 2^{n-1}$$

□

Теорема 12.4 (Решение помидора (неупор. разбиения))**.**

$$f(n; n_1, \ldots, n_k) = f(n - n_1; n_1, \ldots, n_k) + f(n; n_2, \ldots, n_k)$$

$$f(0; \ldots) = 1$$

$$f(-n; \ldots) = 0$$

13 Лекция 13

13.1 Диаграммы Юнга

$n \in \mathbb{N}$

$$n = x_1 + \ldots + x_t$$

$$x_1 \le x_2 \le \ldots \le x_t$$

Обозначение. *Канонический вид диаграммы юнга:*

$$x_1 : \underbrace{\circ \circ \circ \ldots \circ}_{x_1 \text{ раз}}$$

$$\vdots$$

$$x_k : \underbrace{\circ \circ \circ \ldots \circ \circ\circ}_{x_k \text{ раз}}$$

Теорема 13.1. *Кол-во разб. (помидорных — неупор.) числа n на не более чем k слагаемых равно кол-ву разб. числа $n + k$ на ровно k слагаемых.*

Доказательство. Добавляем слева от диаграммы юнга столбец размера k. Получаем биекцию. □

Теорема 13.2. *Кол-во разб. (помидорных — неупор.) числа n на не более чем k слагаемых равно кол-ву разб. числа $n+\frac{k(k+1)}{2}$ на ровно k различных слагаемых.*

Доказательство. К i-ой строке слева добавляем i единиц. Если числа были равными, то теперь нет. Нер-ва сохранились. Получили биекцию. □

Теорема 13.3. *Кол-во разб. (помидорных — неупор.) числа n на не более чем k слагаемых равно кол-ву разбиений числа n на слагаемые величины $\leq k$.*

Доказательство. Инвертируем таблицу, превращая строки в столбцы. □

13.2 Эйлер

$$(1-x)(1-x^2)\ldots(1-x^n)\ldots = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \ldots$$

Теорема 13.4. *Пусть $n = \frac{3k^2 \pm k}{2}$, $k \in \mathbb{N} \cup \{0\}$. Тогда коэфф. при x^n равен $(-1)^k$, если же $n \neq \frac{3k^2 \pm k}{2}$, то коэфф. равен 0.*

Посмотрим, причём здесь разбиения? А вот причём:
Коэффициент при x^n:

$$(-x^{n_1})(-x^{n_2})\ldots(-x^{n_t}) = (-1)^t x^n$$

$$n_1 + n_2 + \ldots + n_t = n$$

$n_{\text{чёт}}$ — кол-во разбиений n на различные слагаемые, число кот-ых **чётно**
$n_{\text{нечёт}}$ — кол-во разбиений n на различные слагаемые, число кот-ых **нечётно**
Тогда коэф-т при $x^n \to n_{\text{чёт}} - n_{\text{нечёт.}}$

13.3 Формальные степенные ряды

На мн-ве объектов вида:

$$A = (a_0, a_1, \ldots, a_n, \ldots), a_i \in \mathbb{R}$$

(т. е. бесконечные п-ть чисел)
Введём операции:

1) Сложение:

$$B = (b_0, b_1, \ldots), C = A + B \Rightarrow \forall i\colon c_i = a_i + b_i$$

2) Умножение на число: очев.

3) Умножение ФСР:

$$A, B, C = A \cdot B$$

$$\forall i\colon c_i = \sum_{k=0}^{i} a_k \cdot b_{i-k}$$

4) Взятие обратного:

$$A, C = \frac{1}{A} \iff AC = 1$$

Это такое C, что:

$$\begin{cases} a_0 c_0 = 1 \\ a_0 c_1 + a_1 c_0 = 0 \\ a_0 c_2 + a_1 c_1 + a_2 c_0 = 0 \\ \vdots \end{cases}$$

Система разрешима $\iff a_0 \neq 0$

Пример.

$$\frac{1}{(1-x^2)^2} = \left(\frac{1}{1-x^2}\right)^2 = \left(\frac{1}{1-x}\right)^2 \left(\frac{1}{1+x}\right)^2$$

Деля в столбик 1 на $1-x$, получаем:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + x^6 + \dots + x^{2n} + \dots$$

$$\left(\frac{1}{1-x^2}\right)^2 = 1 + 2x^2 + 3x^4 + \dots + (n+1)x^{2n}$$

$$\left(\frac{1}{1-x}\right)^2 = 1 + 2x + 3x^2 + \dots + (n+1)x^n$$

$$\left(\frac{1}{1+x}\right)^2 = 1 - 2x + 3x^2 + \dots + (-1)^n(n+1)x^n$$

$$\left(\frac{1}{1-x}\right)^2\left(\frac{1}{1+x}\right)^2 = \dots + (1\cdot(-1)^n\cdot(n+1) + 2\cdot(-1)^{n-1}\cdot n + \dots + (n+1)\cdot 1)x^n + \dots$$

Т. е. коэф. при x^n:

$$\sum_{k=0}^{n}(k+1)(-1)^{n-k}(n+1-k) = \begin{cases} 0, n = 2l+1, l \in \mathbb{N} \\ l+1, n = 2l, l \in \mathbb{N} \end{cases}$$

13.4 Производящие ф-ции

$$a_0, \dots, a_n, \dots$$

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

$$S_n(x_0) = \sum_{k=0}^{n} a_k x_0^k$$

Ряд сходится, если:

$$\exists \lim_{n\to\infty} S_n(x_0) \in \mathbb{R}$$

Теорема 13.5 (Коши-Адамар)**.** *Пусть*

$$p = \frac{1}{\overline{\lim}_{n\to\infty}\sqrt[n]{|a_n|}}$$

Если $|x_0| < p$, то ряд с коэф. $\{\, a_n \,\}$ сх-ся. Если $|x_0| > p$, то расх-ся.

Замечание. *Если* $|x_0| < p$, *то* f *можно дифференцировать почленно:*

$$f(x) = \sum_{k=0}^{\infty} a_k x^k \Rightarrow f'(x) = \sum_{k=1}^{\infty} k a_k x^{k-1}$$

Пример. *1)*

$$\sum_{k=0}^{\infty} x^k, |x_0| < 1 \text{ — сх-ся}, |x_0| \geq 1 \text{ — расх-ся}$$

2)

$$\sum_{k=0}^{\infty} 2^k x^k, |x_0| < \frac{1}{2} \text{ — сх-ся, иначе расх-ся}$$

3)

$$a_k = \begin{cases} 2^k, k \text{ — чёт} \\ -3^k, k \text{ — нечет} \end{cases}$$

$$\Rightarrow |x_0| < \frac{1}{3} \text{ — сх-ся, иначе расх-ся}$$

4)

$$\sum_{k=1}^{\infty} \frac{x^k}{k^2}$$

$$|x_0| < 1 \text{ — сх-ся}$$

$$|x_0| > 1 \text{ — расх-ся}$$

$$|x_0| = 1 \text{ — СХ-СЯ и равен } \frac{\pi^2}{6}$$

5)

$$\sum_{k=1}^{\infty} \frac{x^k}{k}, |x_0| = 1 \text{ — расх-ся}$$

14 Лекция 14

14.1 Простой пример

Пример. *1.*

$$\sum_{k=0}^{n} k^2 C_n^k \left(\frac{2}{3}\right)^k$$

$$a_k = C_n^k$$

Производящая ф-ция этой п-ти $f(x) = \sum_{k=0}^{n} C_n^k x^k = (1+x)^n$

$$f'(x) = \sum_{k=0}^{n} k C_n^k x^{k-1}$$

$$xf'(x) = \sum_{k=0}^{n} k C_n^k x^k$$

$$(xf'(x))' = \sum_{k=0}^{n} k^2 C_n^k x^{k-1}$$

$$x(xf'(x))'|_{x=\frac{2}{3}} \text{ — ответ.}$$

2.

$$\sum_{k=0}^{\infty} k^2 F_k \left(\frac{2}{3}\right)^k$$

$$f(x) = \sum_{k=0}^{\infty} F_k x^k = F_0 + F_1 x + F_2 x^2 + \ldots + F_n x^n + \ldots$$

$$xf(x) = \sum_{k=0}^{\infty} x^{k+1} F_k = F_0 x + F_1 x^2 + \ldots + F_n x^{n+1} + \ldots$$

$$x^2 f(x) = \sum_{k=0}^{\infty} x^{k+2} F_k = F_0 x^2 + F_1 x^3 + \ldots F_n x^{n+2} + \ldots$$

Сложим $xf(x)$ *и* $x^2 f(x)$*:*

$$xf(x)+x^2 f(x) = F_0 x+(F_0+F_1)x^2+(F_1+F_2)x^3+\ldots+(F_{n-1}+F_{n-2})x^n+\ldots =$$

$$= f(x) - F_1 x - F_0$$
$$xf(x) + x^2 f(x) = f(x) - x$$
$$f(x) = \frac{x}{1 - x - x^2}$$

Радиус сх-ти:

$$\sum_{k=0}^{\infty} k^2 F_k x^k$$

Это:

$$\frac{1}{\lim_{k\to\infty} \sqrt[k]{k^2 F_k}} = \frac{1}{\phi} \approx= 0.62..$$

14.2 Числа каталана

$$T_n = T_{n-1}T_0 + T_{n-2}T_1 + \ldots + T_0 T_{n-1}$$
$$T_0 = 1$$
$$F(x) = T_0 + T_1 x + T_2 x^2 + \ldots + T_n x_n + \ldots$$
$$F^2(x) = T_0^2 + (T_0T_1 + T_1T_0)x + \ldots + (T_0T_n + T_{n-1}T_1 + \ldots T_nT_0)x^n + \ldots$$
$$F^2(x) = T_1 + T_2 x + T_3 x^2 + \ldots + T_{n+1} x^n$$
$$xF^2(x) = F(x) - T_0;$$
$$xF^2(x) - F(x) + 1 = 0$$
$$F_{1,2}(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$
$$xF_{1,2}(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$
$$xF(x) = \frac{1 - \sqrt{1-4x}}{2}$$
$$\sqrt{1+x} = (1+x)^{\frac{1}{2}} = 1 + C^1_{\frac{1}{2}} x + C^2_{\frac{1}{2}} x^2 + \ldots$$
$$C^n_{\frac{1}{2}} = \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\ldots\left(\frac{1}{2}-n+1\right)}{n!}$$
$$C^n_m = \frac{m!}{n!(m-n)!} = \frac{m(m-1)(m-2)\ldots(m-n+1)}{n!}$$

$$-\frac{1}{2}C_{\frac{1}{2}}^{n}(-4)^n = -\frac{1}{2}(-1)^n\frac{4^n}{2^n n!}\cdot 1\cdot(-1)(-3)(-5)\dots(-(2n-3)) =$$
$$= \frac{2^{n-1}}{n!}\cdot 1\cdot 3\cdot\ldots\cdot(2n-3) = \frac{2^{n-1}}{n!}\cdot\frac{(2n-2)!}{2\cdot 4\cdot 6\cdot\ldots\cdot(2n-2)}$$
$$= \frac{2^{n-1}(2n-2)!}{n!2^{n-1}(n-1)!} = \frac{(2n-2)!}{n(n-1)!(n-1)!} = \frac{1}{n}C_{2n-2}^{n-1}$$
$$\Rightarrow T_{n-1} = \frac{1}{n}C_{2n-2}^{n-1}$$
$$\Rightarrow T_n = \frac{1}{n+1}C_{2n}^{n}$$

14.3 Теорема Эрдеша, Гинзбурга, Зива

Теорема 14.1 (Теорема Эрдеша, Гинзбурга, Зива)**.** *Пусть $a_1,\ldots,a_{2m-1}$ — произвольные целые числа. Тогда из них можно выбрать m чисел, сумма к-рых делится на m.*

Лирическое отступление в теорию сравнений:

Определение 14.1.

$$a \equiv b \pmod m \iff m|(a-b)$$

— a сравнимо с b модулю m

Определение 14.2. Полная система вычетов по модулю m — набор из представителей каждого класса из m классов эквив-ти.

Определение 14.3. Приведённая система вычетов по модулю m — система вычетов, причём каждый представитель взаимнопрост с m.

Обозначение.

$$\textit{НОД}(a,b) = (a,b)$$
$$\textit{НОК}(a,b) = [a,b]$$

Теорема 14.2 (Малая теорема Ферма)**.** *Пусть p — простое, $(a,p)=1$. Тогда:*

$$a^{p-1} \equiv 1 \pmod p$$

Следствие.
$$a^p \equiv a \pmod p$$

Доказательство.

$$a^p = \underbrace{(1 + 1 \overset{p}{+} \ldots + 1)}_{a} = \underbrace{1^p + \ldots + 1^p}_{a} + \underbrace{\ldots\ldots\ldots\ldots}_{P(n_1,\ldots,n_a)=\frac{p!}{n_1!\cdot\ldots\cdot n_a!}\equiv 0 \pmod p}$$

Доказали $a^p \equiv a \pmod p$ ∎

Доказательство. Рассм. $1, 2, \ldots, p-1$. Рассм. $a\cdot 1, \ldots, a\cdot(p-1)$. Докажем, что это то же приведённая система вычетов. Пусть $a \cdot x \equiv a \cdot y \pmod p$:

$$a \cdot x \equiv a \cdot y \pmod p$$

$$a \cdot (x - y) \equiv 0 \pmod p \Rightarrow x \equiv y \pmod p$$

Следовательно в ней нет равных по модулю, а следовательно:

$$(a \cdot 1) \cdot (a \cdot 2) \ldots (a \cdot p) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p$$

$$a^{p-1}(1 \cdot 2 \cdot \ldots \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p$$
$$\Rightarrow a^{p-1} \equiv 1 \pmod p$$

∎

Теорема 14.3 (Эйлера)**.** *Пусть $m \in \mathbb{N}$. Пусть $(a, m) = 1$. Тогда $a^{\phi(m)} \equiv 1 \pmod m$*

Теорема 14.4 (Теорема Эрдеша, Гинзбурга, Зива)**.** *Пусть $a_1, \ldots, a_{2m-1}$ — произвольные целые числа. Тогда из них можно выбрать m чисел, сумма к-рых делится на m.*

Доказательство. Докажем для $m = p$ — простое. Предоположим противное:

$$a_1, \ldots, a_{2p-1}$$

$$\forall I \subset \{1, 2, \ldots, 2p-1\}, |I| = p$$

$$\sum_{i \in I} a_i \not\equiv 0 \pmod p$$

1) По МЛТ, получаем:

$$\sum_{I \subset \{1,2,\dots,n\}, |I|=p} \left(\sum_{i \in I} a_i \right)^{p-1} \equiv C_{2p-1}^{p} \equiv 1 \pmod p$$

2) Раскрывая как полином:

$$\sum_{I \subset \{1,2,\dots,n\}, |I|=p} \left(\sum_{i \in I} a_i \right)^{p-1} \equiv \sum_{I \subset \{1,2,\dots,2p-1\}, |I|=p} \dots$$

□

15 Лекция 15

Задача 15.1.

$$(a_1, b_1), \dots, (a_f, b_f) \in \mathbb{Z}^2$$
$$m \in \mathbb{N}$$

Вопрос: при каком наим. f можно гарантировать, что сумма каких-то m пар по обоим коор-там делится на m.

Замечание. $f \geq 4m - 3$. *Пример:* $m-1$ *раз повторяем* $(1,1)$, *затем* $m-1$ *раз* $(0,1)$, *потом* $(0,0)$ *и* $(1,0)$.

Что думали люди:

- Гипотеза Кемница: $f = 4m - 3$
- 90-е — Алон и Дубинер: $f \leq 6m - 5, m >$
- 2000 год: Роньяи $f \leq 4m - 2$
- 2005 год: Райер: $f = 4m - 3$

Доказательство. Докажем это для $m = p$ — простое.

$$F(x_1, \dots, x_n) \text{ — многочлен от } n \text{ переменных}$$
$$F(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$
$$F(x, y) = \sum c(a, b) x^a y^b$$

Причём члены суммы — одночлены/мономы.

Определение 15.1. **Степень монома** — сумма степеней входящих в него переменных

Определение 15.2. **Степень полинома** — наиб. степень мономов.

Теорема 15.1 (Шевалле-Варнинга)**.** *Пусть* $F_1, \ldots, F_k \in \mathbb{Z}_p[x_1, \ldots, x_n]$ *Пусть* $\deg F_1 + \ldots + \deg F_k < n$. *Рассм. систему сравнений:*

$$\begin{cases} F_1(x_1, \ldots, x_n) \equiv 0 \pmod p \\ \vdots \\ F_k(x_1, \ldots, x_n) \equiv 0 \pmod p \end{cases}$$

Утверждение теоремы: *Если* $(0, \ldots, 0)$ *— решение системы, то* $\exists (x_1, \ldots, x_n)$ *— нетривиальный набор, кот. тоже явл-ся решением системы.*

Лемма 15.2. *Пусть* $(a_1, b_1), \ldots, (a_{3p}, b_{3p}) \in \mathbb{Z}^2$ *и* $\sum_{i=1}^{3p} a_i \equiv \sum_{i=1}^{3p} \equiv 0 \pmod p$. *Тогда*

$$\exists I \subset \{1, 2, \ldots, 3p\}, |I| = p, \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod p$$

Доказательство. Сделаем 3 многочлена:

$$F_1(x_1, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} a_i x_i^{p-1}$$

$$F_2(\ldots) = \sum_{i=1}^{3p-1} b_i x_i^{p-1}$$

$$F_3(\ldots) = \sum_{i=1}^{3p-1} x_i^{p-1}$$

$$\deg F_1 + \deg F_2 + \deg F_3 = 3p - 3 < 3p - 1$$

Заметим, что $(0, \ldots, 0)$ — удовл. трём мн-нам $\Rightarrow$ по т. Шевалле-Варнинга $\exists (x_1, \ldots, x_n)$, удовл. трём мн-нам, в кот. не все равны 0
Обозначим J — мн-во номеров этих x_i, кот. не равны 0.
Мы знаем:

$$\sum_{i=1}^{3p-1} a_i x_i^{p-1} \equiv 0 \pmod p$$

Заметим, что мы можем взять чисто ненулевые x_i, т. е. из J:

$$\sum_{i\in J} a_i x_i^{p-1} \equiv 0 \pmod p \overset{\text{МТФ}}{\equiv} a_i \equiv 0 \pmod p$$

Аналогично:

$$\sum_{i\in J} b_i \equiv 0 \pmod p$$

$$\sum_{i\in J} 1 \equiv 0 \pmod p$$

$$\Rightarrow |J| \in \{\, p, 2p \,\}$$

$$|J| = p \Rightarrow I := J$$

$$|J| = 2p \Rightarrow I := \{\, 1, 2, 3, \ldots 3p \,\} \setminus J$$

Лемма доказана. $\square$

Пусть $n = 4p - 2$. Предположим, что $\forall I \subset \{\, 1, \ldots, n \,\}, |I| = p$, либо $\sum_{i\in I} a_i \not\equiv 0 \pmod p$, либо $\sum_{i\in I} b_i \not\equiv 0 \pmod p$ (Заметим, что отсюда следует то же самое и для $|I| = 3p$ по доказанной лемме)
Введём многочлен-КРОКОДИЛ:

$$F(x_1, \ldots, x_n) = \left(\left(\sum_{i=1}^{n} a_i x_i\right)^{p-1} - 1\right) \cdot \left(\left(\sum_{i=1}^{n} b_i x_i\right)^{p-1} - 1\right) \cdot$$

$$\cdot \left(\left(\sum_{i=1}^{n} x_i\right)^{p-1} - 1\right) \cdot (\sigma_p(x_1, \ldots, x_n) - 2)$$

Где $\sigma_p(x_1, \ldots, x_n)$ — симметрический мн-н:

$$\sigma_1(x_1, \ldots, x_n) = x_1 + \ldots + x_n$$

$$\sigma_2(x_1, \ldots, x_n) = x_1 x_2 + \ldots + x_{n-1} x_n$$

$$\sigma(3)(x_1, \ldots, x_n) = x_1 x_2 x_3 + \ldots + x_{n-2} x_{n-1} x_n$$

$$\vdots$$

Разберём КРОКОДИЛА по косточкам (битикам):

$$(x_1, \ldots, x_n) \in \{\, 0, 1 \,\}^n$$

1) Пусть число ненулевых коор-т равно p или $3p$, I — мн-во ненулвых коор-т:

$$\sum_{i=1}^{n} a_i x_i = \sum_{i \in I} a_i$$

$$\sum_{i=1}^{n} b_i x_i = \sum_{i \in I} b_i$$

Тогда $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$

2) Пусть число ненулевых коор-т равно $2p$, тогда:

$$\sigma_p(x_1, \ldots, x_n) = C_{2p}^{p} \equiv 2 \pmod{p}$$

$$\Rightarrow F \equiv 0 \pmod{p}$$

3) Пусть мн-во ненулевых коор-т имеет мощность, <u>не делящуюся на p</u>.

$$\Rightarrow \left(\left(\sum_{i=1}^{n} x_i \right)^{p-1} - 1 \right) \equiv 0 \pmod{p}$$

$$\Rightarrow F \equiv 0 \pmod{p}$$

4) Остался единственный случай, когда $(x_1, \ldots, x_n) = (0, 0, \ldots, 0)$, тогда:

$$F(0, 0, \ldots, 0) = 2$$

Раскроем скобки, получим что слагаемое имеет соотв. вид, изменим его так:

$$c x_1^{\alpha_1} \ldots x_n^{\alpha_n} \to c x_1^{\beta_1} \ldots x_n^{\beta_n}$$

$$\alpha_i = 0 \Rightarrow \beta_i = 0$$

$$\alpha_i \geq 1 \Rightarrow \beta_i = 1$$

Получаем полином $\widetilde{F}(x_1, \ldots, x_n)$.
УЛЬТРА МЕГА КАТАРСИС:
на $(x_1, \ldots, x_n) \in \{0, 1\}^n \Rightarrow F = \widetilde{F}$. Получаем, что:

$$\widetilde{F} = 2(1 - x_1) \ldots (1 - x_n)$$

$$\deg \widetilde{F} = n = 4p - 2$$

$\square$