Основы комбинаторики и теории чисел

Сергей Григорян

7 ноября 2024 г.

Содержание

1 Лекция 6

1.1 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 1.1. Плотный порядок:

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

Утверждение 1.1. *Плотный порядок - либо тривиальный (т. е. разлные эл-ты не сравнимы), либо опр. на бесконечном мн-ве.*

Определение 1.2. 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 1.1. *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 $b_p \colon b_p < b_i, \forall i$ из использованных ранее.

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

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

$\square$

1.2 Предпорядки

Определение 1.3. Предпорядок (Предпочтения) - отношение, обладающее рефлексивностью и транзитивностью.

Определение 1.4. Полный предпорядок (Рациональные предпочтения) - предпорядок + любые два сравнимы. (или полн. + транз.)

Обозначение.

$$a \gtrsim b \text{ - } \textit{предпор.}$$

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

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

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

Теорема 1.2 (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 $\exists x \in S, y \in T \colon x \precsim y$
   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. $R \le S \le T$:

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

3) Антисимм.:

$$S \le T, T \le S$$

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

- $\Leftarrow$) S, T - классы

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

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

$\Rightarrow$) Даны x, y:

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

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

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

S - класс эквив., T - класс эквив.

□

1.2.1 Агрегирование предпорядков

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

<u>Определение</u> 1.5. Агрегирование по больш-ву:

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

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 1.3. *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.:

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

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

□

2 Лекция 7

2.1 База

Сложение, умножение.
Прицнип Дирихле.
$\{ a_1, \ldots, a_n \}$
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 2.1.

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

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

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

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

Доказательство. Для док-ва последнего, сделаем биекцию:

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

Пример.

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

$$\underset{a}{110}\,\underset{b}{0}\,\underset{c}{0}\dots\underset{m}{0110}\dots\underset{y}{0}\,\underset{z}{0}$$

□

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

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

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

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

Утверждение 2.1. $\forall W \colon |W| \leq 140$

Задача 2.1. $\{ 1, 2, \dots, 30 \}$
$M_1, \dots, M_{15}$ - различные 5-сочет.
Можно ли покрасить числа 1, .., 30 в 2 цвета, чтобы все M_i были неоднοцветными?

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)

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

3 Лекция 8

3.1 Продоложние про тождества

3)

$$C_n^0 + C_n^1 + C_n^2 + \dots C_n^n = 2^n$$

4)

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

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

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

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

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. $\{ a_1, \dots, a_n, a_{n+1} \}$. 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 $k = 0, 1, \dots, m$ 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.

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

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

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

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 3.1. 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

$$\Rightarrow C_{13}^{2} C_{11}^{2} C_{9}^{1} \ldots C_{1}^{1} = \frac{13!}{2!2!1!1! \ldots 1!}$$

Задача 3.2. Даны n_1 объектов a_1, n_2 объектов a_2, $\ldots n_k$ объектов a_k. Сколько способов сформировать n-ти из этих объектов.

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

Теорема 3.1.

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

Тогда:

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

$P(n_1, \ldots, n_k)$ - полиномиальный коэфф.

n_1 - кол-во скобок, из кот. взяли x_1

n_2 - ... x_2

$\vdots$

n_k - ... x_k

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

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 3.2.

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

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

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

$$N(\alpha_1', \dots, \alpha_{n-1}') = N - N(\alpha_1) - \dots - N(\alpha_{n-1}) + \dots + (-1)^{n-1} N(\alpha_1, \dots, \alpha_{n-1}) \tag{1}$$

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

$$M(\alpha_1', \alpha_2', \dots \alpha_{n-1}') = M - M(\alpha_1) - M(\alpha_2) - \dots - M(\alpha_{n-1}) + \dots + (-1)^{n-1}(M(\alpha_1, \dots, \alpha_{n-1}$$

$$= N(\alpha_1', \dots, \alpha_{n-1}', \alpha_n) = N(\alpha_n) - N(\alpha_1, \alpha_n) - \dots - N(\alpha_{n-1}, \alpha_n) + \dots + (-1)^{n-1}(N(\alpha_1, \dots, \tag{2}$$

Тогда, чтобы получить $N(\alpha_1', \dots, \alpha_n')$, вычислим (1) - (2):

$$N(\alpha_1', \dots, \alpha_n') = N - N(\alpha_1) - \dots - N(\alpha_n) + N(\alpha_1, \alpha_2) + \dots + N(\alpha_{n-1}, \alpha_n) + \dots + (-1)^n N(\alpha_1$$

□

4 Лекция 9

7)

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

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

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

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

По формуле вкл.-искл.:

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

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

Задача 4.1. Задача о беспорядках:

<u>Определение</u> 4.1. 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:

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

4.1 Циклические п-ти

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

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

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

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

<u>Пример</u>.

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

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:

4.2 Формула обращения Мёбиуса

Теорема 4.1 (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 4.2. 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 4.2.

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

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

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

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

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

$\square$

Теорема 4.3 (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.

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

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

□

5 Лекция 10

Вспоминаем задачу:

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

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

П-ть r^n:

$$(a_1, \dots, a_n)$$

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

Определение 5.1. Обозначаем как d — **период линейной п-ти**, т. е. min кол-во циклических сдвигов, переводящих её в себя.

Лемма 5.1. $d|n$

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

<u>Лемма</u> 5.2. *$a_1, \dots, a_n$ - периода d, то она представляется, как $\frac{n}{d}$ одинаковых кусков длины d:*

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

Доказательство. Очев. $\square$

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

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

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

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

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

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

$$|W_i| = |V_i|$$

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

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:

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

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

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 5.3.

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

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

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

Локально конечный: $\forall y \in A$

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

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

5.1.1 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 5.4. *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)

□

Теорема 5.5 (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.

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

$$= \sum_{z\preceq y} f(z) \left(\sum_{x\colon z\preceq x\preceq y} \mu(x,y)\right) = 1 + \sum_{z\prec y} f(z) \left(\sum_{x\colon z\preceq x\preceq y} \mu(x,y)\right)$$

Док-во сводится к лемме:

Лемма 5.6.

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

$$\sum_{x\colon z \preceq x \preceq y} \mu(x, y) = 0$$

$\square$