Основы комбинаторики и теории чисел

Сергей Григорян

5 декабря 2024 г.

Содержание

1 Лекция 12

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

Хар-ое ур-ие:

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

Теорема 1.1 (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.

$$1 \leq r \leq k$$

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

Обозначим за:

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

— произвольный мн-н степени l

Теорема 1.2. *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* (1)

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

$$y_n = < \text{ запись из п. 1 } >$$

1.1 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 1.3 (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) $n = 1\colon F(1; 1) = 1 = 2^{1-1}$

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 1.4 (Решение помидора (неупор. разбиения))**.**

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

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

2 Лекция 13

2.1 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 2.1. *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 2.2. *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 2.3. *Кол-во разб. (помидорных — неупор.) числа n на не более чем k слагаемых равно кол-ву разбиений числа n на слагаемые величины $\le k$.*

Доказательство. Инвертируем таблицу, превращая строки в столбцы. □

2.2 Эйлер

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

Теорема 2.4. *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:

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

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

$n_{\text{чёт}}$ — 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 $x^n \to n_{\text{чёт}} - n_{\text{нечёт.}}$

2.3 Формальные степенные ряды

На мн-ве объектов вида:

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

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

1) Сложение:

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

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) <u>Взятие обратного</u>:

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

Это такое C, что:

$$\begin{cases} a_0c_0 = 1 \\ a_0c_1 + a_1c_0 = 0 \\ a_0c_2 + a_1c_1 + a_2c_0 = 0 \\ \vdots \end{cases}$$

Система разрешима $\iff a_0 \neq 0$

<u>**Пример.**</u>

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

Деля в столбик 1 *на* $1-x$*, получаем:*

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

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

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

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

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

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

Т. е. коэф. при x^n*:*

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

2.4 Производящие ф-ции

$$a_0, \ldots, a_n, \ldots$$

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

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

Ряд сходится, если:

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

Теорема 2.5 (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)

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

$$|x_0| < 1 \text{ — } \textit{сх-ся}$$

$$|x_0| > 1 \text{ — } \textit{расх-ся}$$

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

5)

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

3 Лекция 14

3.1 Простой пример

Пример. *1.*

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

$$a_k = C_n^k$$

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

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

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

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

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

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:

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

3.2 Числа каталана

$$T_n = T_{n-1} T_0 + T_{n-2} T_1 + \ldots + T_0 T_{n-1}$$

$$T_0 = 1$$

$$F(x) = T_0 + T_1 x + T_2 x^2 + \ldots + T_n x_n + \ldots$$

$$F^2(x) = T_0^2 + (T_0 T_1 + T_1 T_0)x + \ldots + (T_0 T_n + T_{n-1} T_1 + \ldots T_n T_0)x^n + \ldots$$

$$F^2(x) = T_1 + T_2 x + T_3 x^2 + \ldots + T_{n+1} x^n$$

$$xF^2(x) = F(x) - T_0;$$

$$xF^2(x) - F(x) + 1 = 0$$

$$F_{1,2}(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

$$xF_{1,2}(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

$$xF(x) = \frac{1 - \sqrt{1-4x}}{2}$$

$$\sqrt{1+x} = (1+x)^{\frac{1}{2}} = 1 + C^1_{\frac{1}{2}}x + C^2_{\frac{1}{2}}x^2 + \dots$$

$$C^n_{\frac{1}{2}} = \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\dots\left(\frac{1}{2}-n+1\right)}{n!}$$

$$C^n_m = \frac{m!}{n!(m-n)!} = \frac{m(m-1)(m-2)\dots(m-n+1)}{n!}$$

$$-\frac{1}{2}C^n_{\frac{1}{2}}(-4)^n = -\frac{1}{2}(-1)^n\frac{4^n}{2^n n!} \cdot 1 \cdot (-1)(-3)(-5)\dots(-(2n-3)) =$$

$$= \frac{2^{n-1}}{n!} \cdot 1 \cdot 3 \cdot \ldots \cdot (2n-3) = \frac{2^{n-1}}{n!} \cdot \frac{(2n-2)!}{2 \cdot 4 \cdot 6 \cdot \ldots \cdot (2n-2)}$$

$$= \frac{2^{n-1}(2n-2)!}{n!2^{n-1}(n-1)!} = \frac{(2n-2)!}{n(n-1)!(n-1)!} = \frac{1}{n}C^{n-1}_{2n-2}$$

$$\Rightarrow T_{n-1} = \frac{1}{n}C^{n-1}_{2n-2}$$

$$\Rightarrow T_n = \frac{1}{n+1}C^n_{2n}$$

3.3 Теорема Эрдеша, Гинзбурга, Зива

Теорема 3.1 (Теорема Эрдеша, Гинзбурга, Зива)**.** *Пусть $a_1, \dots, a_{2m-1}$ — произвольные целые числа. Тогда из них можно выбрать m чисел, сумма к-рых делится на m.*

Лирическое отступление в теорию сравнений:

Определение 3.1.

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

— a сравнимо с b модулю m

Определение 3.2. Полная система вычетов по модулю m — набор из представителей каждого класса из m классов эквив-ти.

Определение 3.3. Приведённая система вычетов по модулю m — система вычетов, причём каждый представитель взаимнопрост с m.

Обозначение.

$$\text{НОД}(a,b) = (a,b)$$

$$\text{НОК}(a,b) = [a,b]$$

Теорема 3.2 (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 3.3 (Эйлера)**.** *Пусть $m \in \mathbb{N}$. Пусть $(a,m)=1$. Тогда $a^{\phi(m)} \equiv 1 \pmod m$*

Теорема 3.4 (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:

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

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

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

□