Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

II СЕМЕСТР

Лектор: *Райгородский*

Автор: *Киселев Николай*
Репозиторий на Github

весна 2025

Содержание

1 Распределение простых чисел

Определение 1.1. $\pi(x) = |\{p \leqslant x | p - \text{простое}\}|$

Определение 1.2. $\theta(x) = \sum_{p \leqslant x} \ln p$

Определение 1.3. $\psi(x) = \sum_{(p,\alpha), p^\alpha \leqslant x} \ln p = \sum_{p \leqslant x} \ln p [\log_p x] = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \leqslant \sum_{p \leqslant x} \ln p$

Также введем:

$$\lambda_1 = \overline{\lim}_{x\to\infty} \frac{\theta(x)}{x}, \lambda_2 = \overline{\lim}_{x\to\infty} \frac{\psi(x)}{x}, \lambda_3 = \overline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\ln x}$$

$$\mu_1 = \underline{\lim}_{x\to\infty} \frac{\theta(x)}{x}, \mu_2 = \underline{\lim}_{x\to\infty} \frac{\psi(x)}{x}, \mu_3 = \underline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\ln x}$$

Лемма 1.1. $\lambda_1 = \lambda_2 = \lambda_3, \mu_1 = \mu_2 = \mu_3$

Доказательство.

$$\frac{\theta(x)}{x} = \frac{\sum_{p \leqslant x} \ln p}{x} \leqslant \frac{\psi(x)}{x} \leqslant \frac{\sum_{p \leqslant x} \ln x}{x} = \frac{\ln x}{x} \sum_{p \leqslant x} 1 = \frac{\ln x}{x} \pi(x) = \frac{\pi(x)}{x/\ln x}$$

$$\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$$

При $\beta \in [0, 1)$:

$$\theta(x) = \sum_{p \leqslant x} \ln p \geqslant \sum_{x^\beta < p \leqslant x} \ln p \geqslant \sum_{x^\beta < p \leqslant x} \ln x^\beta = \beta \ln x \sum_{x^\beta < p \leqslant x} 1 = \beta \ln x \left(\pi(x) - \pi\left(x^\beta\right)\right)$$

Заметим, что $x > \pi(x)$:

$$\beta \ln x \left(\pi(x) - \pi\left(x^\beta\right)\right) \geqslant \beta \ln x \left(\pi(x) - x^\beta\right)$$

$$\frac{\theta(x)}{x} \geqslant \frac{\beta \pi(x)}{x/\ln x} - \frac{\beta x^\beta \ln x}{x}$$

$$\overline{\lim}_{x\to\infty} \frac{\theta(x)}{x} \geqslant \overline{\lim}_{x\to\infty} \left(\frac{\beta\pi(x)}{x/\ln x} - \frac{\beta x^\beta \ln x}{x}\right) = \overline{\lim}_{x\to\infty} \frac{\beta\pi(x)}{x/\ln x} \quad \forall \beta \in [0, 1)$$

Теперь, если взять супремум по β, получится

$$\overline{\lim}_{x\to\infty} \frac{\theta(x)}{x} \geqslant \overline{\lim}_{x\to\infty} \frac{\pi(x)}{x/\ln x} \Rightarrow \lambda_1 \geqslant \lambda_3$$

Итого, $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3 \leqslant \lambda_1 \Rightarrow$ они все равны □

Теорема 1.1.

$$\pi(x) \sim \frac{x}{\ln x}$$

Теорема 1.2 (Чебышев)**.** $\forall \varepsilon > 0 \exists x_0 \forall x > x_0:$

$$(1-\varepsilon)\frac{x}{\ln x} \cdot \ln 2 \leqslant \pi(x) \leqslant (1+\varepsilon)\frac{x}{\ln x} \cdot 4\ln 2$$

Доказательство. Рассмотрим C_{2n}^n. Заметим, что $C_{2n}^n < 2^{2n}$. $\ln C_{2n}^n < 2n \ln 2$

$$C_{2n}^n = \frac{(2n)!}{n!n!} \geqslant \prod_{n<p\leqslant 2n} p \Rightarrow \ln C_{2n}^n \geqslant \sum_{n<p\leqslant 2n} \ln p = \theta(2n) - \theta(n)$$

Рассмотрим $n = 1, 2, \dots 2^k$.

$$2n \ln 2 > \ln C_{2n}^n \geqslant \theta(2n) - \theta(n)$$

$$2n \ln 2 > \theta(2n) - \theta(n)$$
$$2(1 + 2 + \dots + 2^k) \ln 2 > \theta\left(2^{k+1}\right)$$
$$2^{k+1} \ln 2 > \theta\left(2^{k+1}\right)$$

Расмотрим $2^k \leqslant x \leqslant 2^{k+1}$

$$\theta(x) \leqslant \theta(2^{k+1}) < 2^{k+2} \ln 2 < 4x \ln 2 \Rightarrow \frac{\theta(x)}{x} < 4 \ln 2$$

Получили правое неравенство. Теперь получим левое:

$$C_{2n}^0 + C_{2n}^1 + \dots + C_{2n}^{2n} = 2^{2n} \Rightarrow C_{2n}^n > \frac{2^{2n}}{2n+1}$$

$$\ln C_{2n}^n > 2n \ln 2 - \ln(2n+1)$$

$$C_{2n}^n = \frac{(2n)!}{n!n!} = \frac{\prod_{p\leqslant 2n} p^{\left[\frac{2n}{p}\right]+\left[\frac{2n}{p^2}\right]+\dots}}{\left(\prod_{p\leqslant 2n} p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\dots}\right)^2} =$$

$$= \prod_{p\leqslant 2n} p^{\left(\left[\frac{2n}{p}\right]-\left[\frac{n}{p}\right]\right)+\left(\left[\frac{2n}{p^2}\right]-\left[\frac{n}{p^2}\right]\right)+\dots} \leqslant \prod_{p\leqslant 2n} P^{[\log_p(2n)]} = e^{\psi(2n)} \Rightarrow \ln C_{2n} \leqslant \psi(2n)$$

$$\psi(2n) \geqslant 2n \ln 2 - \ln(2n+1) > (x-2) - \ln(x+1)$$

Если $x \in [2n, 2n+2)$, то $\psi(x) \geqslant \psi(2n) \geqslant (x-2)\ln 2 - \ln(x+1)$. Итого:

$$\frac{\psi(x)}{x} \geqslant \frac{x-2}{x} \ln 2 - \frac{\ln(x+1)}{x} \Rightarrow \mu_2 \geqslant \ln 2, \mu_3 \geqslant \ln 2$$

И тогда:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} \geqslant \ln 2$$

Но тогда, с какого-то момента:

$$(1 - \varepsilon x)\frac{x}{\ln x} \ln 2 \leqslant \pi(x)$$

□

Анекдот: Райгор учился на кафедре мехмата в девяностые годы и интересовался теорией чисел. Один раз он сидел со своим руководителем на кафедре, и вдруг туда заходит калоритный иностранец с сильным акцентом. Зашел и говорит: "А не расскажите лы вы мнэ, сколко нулэй на концэ числа 100!". Они с научруком ему объяснини, что надо посчитать степень вхождения 5 и 2, в общем он понял и ушел. Приходит через неделю и говорит: "Я понял, как пощитать колычество нулэй на концэ числа 100!, а тэпэрь скажытэ мнэ, как пащитать калычество нулэй на концэ числа 1000!"

Утверждение 1.1 (Постулат Бертрана)**.** $\forall x \geqslant 2 \exists p \in [x, 2x] = [x, x + x]$

Но это сложно, мы займемся другим вопросом: При каких $f(x)$ можно рассчитывать на существование $p \in [x, x + f(x)]$ хотя бы при $x \geqslant x_0$.

Утверждение 1.2 (Асимптотический Закон Распределения Простых Чисел)**.** $f(x) = o(x)$

Утверждение 1.3 (Гипотеза)**.** $f(x) = O(\ln^2 x)$

2 Первообразный Корень

Определение 2.1. Пусть $(a, m) = 1$. Показатель числа $a \mod m$ — это минимальное δ, такое, что $a^\delta \equiv_m 1$.

Утверждение 2.1. $\delta | \varphi(m)$

Определение 2.2. Пусть $(a, m) = 1$. Если показатель $a \mod m = \varphi(m)$, то a называется первообразным корнем и обозначается g.

Замечание. Если по $\mod m \exists$ первообразный корень, то $1, g, g^2 \dots g^{\varphi(m)-1}$ — все взаимно простые с m остатки.

Определение 2.3. $ind_g a$ — такое число, что $g^{ind_g a} = a$