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

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

II СЕМЕСТР

Лектор: *Райгородский*

$h\nu$

Автор: *Киселев Николай*
Репозиторий на Github

весна 2025

Содержание

«««< HEAD

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.

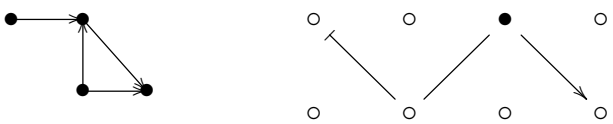
Определение 2.3. $ind_g a$ — такое число, что $g^{ind_g a} = a$

=======

3 Графы

Определение 3.1. Ориентированный граф $G = (V, E)$, где V - конечное множество. $E \subset V \times V$

Определение 3.2. Неориентированный граф $G = (V, E)$, где V - конечное множество. $E \subset C_v^2$



3.1 Алгоритм dfs (поиск в глубину)

Псевдокод:

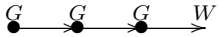
```
vector<vector<int>> g;

vector<int> parent;

vector<int> tin, tout; // время входа и выхода из вершины

vector<string> color; // для покраски вершин
```

Изначально все вершины покрашены в белый цвет - сигнал, что в вершину еще не заходили, цвет серый - вершина в обработке, цвет черный - вершина полностью обработана, больше нас не интересует

```
void dfs(int v) {
  color[v] = "GRAY"; tin[v] = timer; ++timer;
  for (int to: g[v]) {
    if (color[to] == "WHITE"): parent[to] = v; dfs(to);
  }
  tout[v] = timer; ++timer;
  color[v] = "BLACK";
}
```

Лемма 3.1 (О белых путях)**.** *За время с $tin[v]$ до $tout[v]$ dfs посетит все те вершины, которые были достижимы из v по белым путям и перекрасит их в черный цвет.*

Доказательство. Понятно, что перекрасить можем только описанные вершины. Заметим, что GRAY вершины - это в точности стек рекурсии. Значит, в момент $tout[v]$ новых серых не появилось.



Остается доказать, что белые вершины достижимы по белым путям и не могут остаться белыми. Рассотрим вершину u - самую высокую оставшуюся из белых. Тогда ее родитель не мог почернеть без захода в эту вершину. □

Следствие. Пусть изначально все вершины - белые. Тогда после внешнего запуска dfs(s) посетятся все достижимые из s вершины.

Следствие. В графе ∃ цикл, достижимый из $s \leftrightarrow dfs(s)$ в какой-то момент ведет ребро в серую вершину.

Замечание. Мы не пытаемся обойтись 2 цветами - черным и белым, чтобы иметь возможность понять, есть ли цикл в графе

Замечание. Асимптотика алгоритма равно $O(n+m)$, где $n = |V|, m = |E|$.

Определение 3.3. DAG(directed acyclic graph) - ориентированный граф без циклов.

Определение 3.4. Топологическая сортировка графа: перестановка вершин графа, чтобы все ребра вели "слева направо".

Утверждение 3.1. *Топологическая сортировка сущесутвует тогда и только тогда, когда граф - DAG*

Доказательство.

$\rightarrow$ Очев

$\leftarrow$ Алгоритмом: все вершины красим в белый цвет.

```
for (s = 0...n-1)
  if (color[s] == "WHITE") dfs(s)
```

Топологическая сортировка - перестановка вершин в порядке убывания $tout$

Проверим корректность: Достаточно показать, что не может быть ребра из u в v: $tout[u] < tout[v]$. Предположим противное и разберем 2 случая:

(a) $tin[u] < tin[v]$
По лемме о белых путях, к моменту времени выхода из u вершина v уже полностью обработается $\rightarrow tout[v] < tout[u]$. Противоречие.

(b) $tin[v] < tin[u]$ Тогда $\nexists$ пути из v в u. Значит, пол лемме, к моменту $tout[v]$ мы даже не увидим u. А следовательно, $tout[v] < tout[u]$. Противоречие.

□

Определение 3.5. Пусть G - ориентированный граф, $u, v \in V(G)$. Тогда говорим, что u, v сильно связны, если $\exists$ пусть из u в v и из v в u.

Задача. *Сильная связанность - отношение эквивалентности.*

Определение 3.6. Класс эквивалентности по этому отношению - компонента сильной связности (КСС)

3.1.1 Алгоритм Косарайю

Алгоритм выделения КСС за $O(n+m)$

1. dfs от всех вершин, сортируя все вершины в порядке убывания tout
2. В этом порядке запускаем dfs по обратным ребрам (dfs Reversed). Все, что посетим за один такой запуск - очередная КСС.

Корректность?

Доказательство. Ясно, что каждый запуск dfs Reversed обойдет одну или несколько КСС целиком. Но вдруг мы возьмем 2 КСС вместо одной...

Утверждение 3.2.
Пусть C_1, C_2 - две КСС, причем есть ребро из C_1 в C_2. Тогда $max_{x \in C_1}(tout(x)) > max_{y \in C_2}(tout(y))$

Доказательство.

1. $min_{a \in C_1} tin(a) < min_{b \in C_2} tin(b)$

   В этом случае к моменту времени входа в a все вершины в C_1 и C_2 - еще белые. По лемме о белых путях к моменту $tout[a]$ все вершины из C_1 и C_2 покрасятся в черный $\Longrightarrow tout(a) > max_{y \in C_2}(tout(y))$.

2. $min_{a \in C_1} tin(a) > min_{b \in C_2} tin(b)$

   Тогда к моменту входа в b все вершины из C_1 и C_2 еще белые. Отметим, что не существует пути из b в C_1 (иначе C_1 и C_2 - одна КСС). Значит, к моменту выхода из b вся C_1 еще белая $\Longrightarrow max_{x \in C_1}(tout(x)) > max_{y \in C_2}(tout(y))$

□

Теперь воспользуемся утверждением и получим искомое. □

Замечание. Пусть алгоритм Косарайю нумерует все КСС в порядке их обнаружения. $id[v]$ - номер КСС, содержащий v. Значит, если есть ребро из a в b, $id[a] \leqslant id[b]$

a, b *сильно связаны* $\Longrightarrow id[a] = id[b]$