Свёртка Дирихле и Алгоритмы за $O(n^{\frac{2}{3}})$

pakhomovee

Compiled: 3 августа 2023 г.

Часть I

Обращение Мёбиуса, свертка Дирихле

1 Обращение Мёбиуса

1.1 Полезные функции

Proposition 1.1

Введем несколько функций $\mathbb{Z} \to \mathbb{Z}$ для ясности:

$$1(n) = 1$$

$$id(n) = n$$

$$\mu(n) = \begin{cases} (-1)^k \text{ если n свободно от квадратов и у него k простых делителей} \\ 0 \text{ иначе} \end{cases}$$

$$\tau(n) = \sum_{d|n} 1 = \text{количество делителей n}$$

$$\sigma(n) = \sum_{d|n} d = \text{сумма делителей n}$$

$$\chi_1(n) = \sum_{d|n} \mu(d)$$

Lemma 1.2

$$\chi_1(n) = \begin{cases} 1 \text{ если } n = 1 \\ 0 \text{ иначе} \end{cases}$$

Доказательство. Пусть $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$. Если $\mu(d) \neq 0$, то $\forall i : a_i \leq 1$. $\mu(d) = 1$, если чётное число a_i не равно 0. Таких d ровно $\sum\limits_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2i}$. А d, дающих вклад -1 ровно $\sum\limits_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{2i+1}$. Это суммы чётных и нечётных биномиальных коэффициентов, соответственно. Они равны при $n > 1$, поэтому в этом случае $\chi_1(n) = 0$. 😎

Definition 1.3

Функция Эйлера $\varphi(n)$ — это количество чисел, не больших n, которые взаимно просты с n.

1.2 Обращение Мёбиуса

Theorem 1.4

Пусть f и g — арифметические функции. Тогда:

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

Доказательство.

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \times \left(\sum_{d_1|\frac{n}{d}} f(d_1)\right) = \sum_{d_1|n} f(d_1) \times \left(\sum_{d|\frac{n}{d_1}} \mu(d)\right) = \sum_{d_1|n} f(d_1) \times \chi_1\left(\frac{n}{d_1}\right)$$

Заметим, что сдагаемые с $d_1 \neq n$ равны 0. Получаем $\sum\limits_{d_1|n} f(d_1) \times \chi_1\left(\frac{n}{d_1}\right) = f(n)$.

Аналогично можно доказать равенство и в обратную сторону. 😎

Example. Приведем несколько примеров.

- $1 = \sum\limits_{d|n} \mu(d)\tau\left(\frac{n}{d}\right)$
- $n = \sum\limits_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right)$
- $\mu(n) = \sum\limits_{d|n} \mu(d)\chi_1\left(\frac{n}{d}\right)$
- $n = \sum\limits_{d|n} \varphi(d) \Rightarrow \varphi(n) = \sum\limits_{d|n} \mu(d) \times \frac{n}{d}$

2 Свёртка Дирихле

Definition 2.1

Свертка Дирихле двух арифметических функций определяется следующим образом:

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

Example. Обращение Мёбиуса принимает вид:

$$g = f * 1 \Leftrightarrow f = g * \mu$$

Definition 2.2

Арифметическая функция f называется мультипликативной, если:

$$f(a \cdot b) = f(a) \cdot f(b) \forall a, b \in \mathbb{N}, \text{ таких что } \gcd(a, b) = 1.$$

Рассмотрим свойства свёртки Дирихле:

1. $(f * g) * h = f * (g * h)$
2. $f * g = g * h$
3. $f * (g + h) = f * g + f * h$
4. $f * \chi_1 = \chi_1 * f = f$
5. $f * 0 = 0 * f = 0$
6. Если f и g —мультипликативные функции, то и $f * g$ является мультипликативной функцией.

Доказательство. 1-5. Подстановка.
6. Докажем, что пригcd$(n, m) = 1$: $(f * g)(n \cdot m) = (f * g)(n) \times (f * g)(m)$.

$$(f * g)(n * m) = \sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) = \sum_{d_1|n, d_2|m} f(d_1 d_2) g\left(\frac{nm}{d_1 d_2}\right) = \sum_{d_1|n, d_2|m} f(d_1) f(d_2) g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right)$$

$$= \left(\sum_{d_1|n} f(d_1) g\left(\frac{n}{d_1}\right)\right) \times \left(\sum_{d_2|m} f(d_2) g\left(\frac{m}{d_2}\right)\right) = (f * g)(n) \times (f * g)(m)$$

😎

Example.

- $\tau = 1 * 1$
- $\sigma = id * 1$
- $\chi_1 = \mu * 1$

- $1 = \tau * \mu$
- $id = \sigma * \mu$
- $id = \varphi * 1$
- $\sigma = \phi * \tau$

Часть II

Быстрый подсчет факториалов

2.1 $n < mod$

Задача

Найдите $n!$ по модулю p ($n < p$).

Пусть $y = \sqrt{n}$. Рассмотрим блоки чисел: $[1, \dots, y], [y+1, \dots, 2y], \dots, \left[\left\lfloor \frac{n-y}{y} \right\rfloor \times y + 1, \dots, \left\lfloor \frac{n}{y} \times y \right\rfloor\right]$.

Заметим, что произведени в блоках можно посчитать при помощи fft за $O(y \log^2 n)$, так как это просто multipoint evaluation в многочлене $x(x+1)\dots(x+y-1)$.

Сам многочлен легко получить за $O(y \log^2 n)$ при помощи метода разделяй и властвуй.

Произведение чисел на последнем куске $\left(\left[\left\lfloor \frac{n}{y} \right\rfloor \times y + 1, \dots, n\right]\right)$ можно учесть за $O(y)$. Итого $O(\sqrt{n} \log^2 n)$.

2.2 $n > mod$

Если же $n > p$, мы можем заметить, что произведение чисел $1, 2, \dots, p-1$ имеет остаток -1 по модулю p. Поэтому нам нужно разбить числа от 1 до n на блоки по p чисел. Тогда в последнем блоке (он может быть неполным) нам нужно посчитать факториал при помощи метода из предыдущего пункта. Чтобы учесть остальные блоки, нам нужно просто домножить ответ на $(-1)^{\frac{n}{p}}$ и на факториал числа $\frac{n}{p}$.

Таким образом, мы получили рекурсивную функцию, которую умеем насчитывать за $O(\sqrt{n} \log^2 n \log_p n)$.

3 Несколько факториалов

Теперь мы хотим научиться считать сразу несколько факториалов. Для этого поймем с какой частью подсчета у нас могут возникнуть проблемы. Заметим, что мы можем насчитать префиксные произведение по блокам размера y один раз в оффлайне и отвечать на эту часть за $O(1)$ с предподсчетом за $O(\sqrt{n} \log^2 n)$. Чтобы быстро посчитать произведение на «хвостике» размера не более y мы можем разбить его на степени двойки (их будет $O(\log n)$). Тогда, нам нужно будет посчитать значения многочленов вида $x, x(x+1), x(x+1)(x+2)(x+3), \dots$ в $O(q \log n)$ точках. Это опять же multipoint evaluation. Итоговая асимптотика $O(\sqrt{n} \log^2 n + q \log^3 n)$.

Часть III

Количество простых до n

Пусть $\varphi(n, a)$ — количество чисел не превосходящих n, что их наименьший простой делитель имеет номер больше a. Это легко пересчитать:

$$\varphi(n, a) = \varphi(n, a-1) + \varphi\left(\left\lfloor \frac{n}{p_a} \right\rfloor, a-1\right)$$

Также легко заметить, что для любого m и простых $p_i, p_j > \sqrt{m}$ выполнено $\varphi(m, p_i) + i = \varphi(m, p_j) + j$. Значит,для любого m достаточно хранить $\pi(\sqrt{m})$ значений.

Давайте будем насчитывать φ рекурсивно, но, попав в состояние с $m < n^{2/3}$ просто запомним, что нам нужно посчить значение функции в этой точке и не будем запускаться рекурсивно дальше. На эти запросы несложно ответить оффлайн. Насчитаем для каждого числа до $n^{2/3}$ его минимальный простой делитель, после чего пройдемся с фенвиком и ответим на запросы.

Осталось показать, что запросов будет не сильно много. Заметим, что в любое состояние $\varphi(m, a)$, где $m < n^{2/3}$ мы попали из какого-то состояния с $m' > n^{2/3}$. Так как из каждого состояния есть всего два перехода, количество состояний Q для $m < n^{2/3}$ асимптотически можно оценить как количество состояний для $m > n^{2/3}$. Получаем:

$$Q \le \sum_{j=1}^{n^{1/3}} \pi(\sqrt{n/j}) \; \frac{1}{\log n} \sum_{j=1}^{n^{1/3}} \sqrt{n/j} \; \frac{1}{\log n} \int_1^{n^{1/3}} \sqrt{n/x} dx \; \frac{n^{2/3}}{\log n}$$

Мы работаем за $O(n^{2/3} \log n)$. Выбрав $K = \left(\frac{n}{\log n}\right)^{2/3}$, можно добиться асимптотики $O(n^{2/3} \log^{1/3} n)$.