1 Решето Эратосфена

Хотим для первых n чисел найти все простые.

1.1 Базовый алгоритм.

Переберем все числа от 1 до n. Для каждого простого числа переберем все кратные ему, и отметим как не простые.

Оценка времени работы

$$\sum_{i=2}^{\frac{n}{\log n}} \frac{n}{P_k} \sim \int_{x=2}^{\frac{n}{\log n}} \frac{n}{k \log k} \sim O(n \log \log n)$$

1.2 Линейный алгоритм.

Будем поддерживать минимальный простой делитель $p[x]$ для каждого числа, а так же список уже найденных простых.

Переберем числа от 2 до n. Если для очередного числа x не найдено делителей, то добавим его в список простых, и скажем, что $p[x] = x$. Переберем все простые $y \leqslant p[x]$, и отметим, что $p[y * x] = y$.

Таким образом, каждое число будет отмечено ровно один раз. При этом, каждая итерация внутреннего цикла отмечает одно число. Таким образом время работы линейно.

Вычисление этой величины позволяет считать числовые функции, выражающиеся через разложение на простые за линейное время.

2 Решение диофантовых уравнений

Пусть есть уравнение $a \cdot x + b \cdot y = 1$, причем $gcd(a, b) = 1$.

Решим рекурсивно уравнение $b \cdot x' + (a \bmod b) \cdot y' = 1$.

Перепишем это равенство. $b \cdot x' + (a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b) \cdot y' = 1$, $a \cdot y' + b \cdot (x' - \left\lfloor \frac{a}{b} \right\rfloor \cdot y')$.

Таким образом, можно пересчитать решение по формулам $x = y'; y = x' - \left\lfloor \frac{a}{b} \right\rfloor \cdot y'$

Заметим, что таким способом можно обращать в кольце остатков по модулю, решая уравнение $a \cdot x + n \cdot y = 1$.

3 Китайская теорема об остатках

Пусть $x \equiv a (\mathrm{mod} n), x \equiv b (\mathrm{mod} m)$, $gcd(n, m) = 1$.

Хотим найти решение по модулю nm.

Будем искать в виде $a + k \cdot n$. Надо решить уравнение $a + k \cdot n = b(\mathrm{mod} m) \Rightarrow k = (b - a) \cdot n^{-1}(\mathrm{mod} m)$.

4 Тест Рабина-Миллера

Пусть p — простое число. В таком случае, нет корней из 1, кроме ± 1. Если же, не простое — то есть.

Выберем случайное число a. Если $gcd(n, a)! = 1, n$, то не простое. Иначе, пусть $m-1 = 2^s \cdot t$, причем t нечетно. Рассмотрим последовательность $a^t, a^{2^1 t}, a^{2^2 t} \ldots$. Если в ней перед 1 идет не -1, то найден нетривиальный корень из 1.

Утверждается, что если n не простое, то чисел, для которых не найдется противоречие не более $\frac{\varphi(n)}{4}$. То есть вероятность ошибки не более $\frac{1}{4}$.

5 ρ-эвристика Полларда

Рассмотрим последовательность $x_k = x_{k-1}^2 + c$. В качестве c можно например взять ± 1. Не следует брать 0 и -2.

Будем поддерживать $y = x_{2^l}$, для максимально возможного l. На каждом шаге будем вычислять $gcd(x - y, n)$. Корень найдется за время порядка первого совпадения остатка по модулю делителя. Статистически числа x_k можно считать случайными. В таком случае, время совпадения имеет порядок $O(\sqrt{p}) = O(\sqrt[4]{n})$.

6 Задача дискретного логарифмирования

Хотим решать уравнение $a^x = b(\mathrm{mod} n)$. Пусть $x = x_1 + \sqrt{n} \cdot x_2$.

Запишем это в виде $a_1^x = b(a^{-\sqrt{n}})_2^x$.

То есть задача имеет вид нахождения двух одинаковых чисел в двух множествах порядка $\sqrt{n}$.

Такая задача решается с помощью сортировки и бинарного поиска или метода двух указателей.

По примарному модулю, дискретное извлечение корня можно свести к дискретному логарифмированию, нахождением первообразного корня.

7 Дискретное извлечение квадратного корня

7.1 По простому модулю

Рассмотрим многочлены по модулю $x^2 - a$. Если, корня из a нет, то это мы получили некоторое поле. В противном случае, мы получили произведение двух колец $\mathbb{Z}/n\mathbb{Z}$.

Рассмотрим многочлен $(a \cdot x + b)^{\frac{p-1}{2}} (\mathrm{mod} x^2 - a)$. При подстановке в него $\sqrt{a}$ мы получим 1. При этом сам многочлен, может иметь 4 значения, которые в квадрате дают 1. Причем, если a и b, выбрать случайными, то все 4 варианта равновероятны (и есть $2p - 1$ вариант, когда получится 0 в одной из компонент). Итого с вероятностью $\frac{2}{4} - \frac{1}{p}$ мы получили нетривиальное условие на $\sqrt{a}$, из которого его можно явно выразить.

7.2 По примарному модулю

Пусть $p \neq 2$. И пусть найден ответ по модулю p^{k-1}.

Будем искать решение в виде $b + x \cdot p^{k-1}$.

$(b + x \cdot p^{k-1})^2 = b^2 + 2 \cdot b \cdot x \cdot p^{k-1} = a (\mathrm{mod} p^k)$ Так как b — решение по модулю p^{k-1}, можно сократить.

$$\frac{b^2 - a}{p^k} + 2 \cdot b \cdot x = 0 (\mathrm{mod} p)$$

.

От сюда можно выразить $x \bmod p$, чего достаточно.

Случай $p = 2$ особенный, так как добавление 2^{k-1} не меняет остаток по модулю 2^k. В этом случае решение надо искать в виде $b + x \cdot 2^{k-2}$, просто перебрав оба варианта. При этом, так можно делать только при $k \geq 3$.

7.3 По не простому модулю

Разложили на примарные + КТО.