SPb HSE, ПАДИИ, 1 курс, весна 2024/25
Практика по алгоритмам #28

Теория чисел 1
29 апреля

Собрано 29 апреля 2025 г. в 13:51

Содержание

Теория чисел 1

1. **Решето Эратосфена**
   a) $n \leqslant 10^6$. Найти все простые числа на $[n^2, n^2 + n]$ за $\mathcal{O}(n \log\log n)$.
   b) Найти все простые на $[1, n]$ за $\mathcal{O}(n \log\log n)$ с $\mathcal{O}(\sqrt{n})$ памяти.

2. **B-гладкие**

   Число называется B-гладким, если все его простые делители не более B.
   Найдите все B-гладкие числа от 1 до $n \leqslant 10^6$.

3. **Применяем решето**

   Для каждого числа от 1 до $n \leqslant 10^6$ найти (a) количество делителей, (b) функцию Эйлера.

4. **Евклид и ручной труд**
   a) Найдите обратное к 999 по модулю 10^9.
   b) Найдите обратное к 5 по модулю 207.

5. **Расширенный Евклид**
   a) Придумаем/вспомним рекурсивного расширенного Евклида: найти x, y: $ax+by=\gcd(a,b)$.
   b) Докажите, что на каждом шаге рекурсивного Евклида $|x_i| \leqslant |b|$ и $|y_i| \leqslant |a|$.
   c) Описать все решения диофантова уравнения $ax \equiv b \pmod m$.
   d) `(*)` Найти x, y: $ax + by = c, |x| + |y| \to \min$.

6. **RSA**
   a) Пусть $n = pq$, известно $\varphi(n)$, разложите n на множители.
   b) Пусть у нас есть «волшебный» оракул. Для любого открытого ключа (n, e) оракул может взломать 1% из всех возможных зашифрованных сообщений. Придумайте алгоритм, который взламывает любое сообщение. Матожидание времени работы $\mathcal{O}(\text{poly}(\log n))$.

7. **RSA и реальный мир**

   Предложите быстрый способ передачи большого объёма закодированных данных.
   Наш арсенал: Диффи-Хеллман, RSA, XOR-кодирование, псевдорандом.

8. **Биномиальные коэффициенты по модулю**

   При данных $n \leqslant 10^6$ и простом $p \leqslant 10^6$ можно представить $n! = p^k r$. Поймите, как быстро найти k и $r \bmod p$. Пользуясь этим, найдите $\binom{n}{k} \bmod m$. Какой предподсчёт нужно сделать, чтобы, зная заранее m, отвечать на запрос $n, k \leqslant 10^6$, $\binom{n}{k} \bmod m$ за $\mathcal{O}(\log m)$.

9. `(*)` **Квадратичное решето**

   Число называется B-гладким, если все его простые делители не более $B \leqslant 1000$.
   Найдите все B-гладкие числа вида $(\lfloor\sqrt{M}\rfloor + i)^2 \bmod M$, где $i = 1..N \leqslant 10^6$, M очень большое.

10. `(*)` **Магия**

    Поймите, что делает код:

```
f[1] = 1;
for (int i = 2; i < p; i++)
    f[i] = (p - f[p % i]) * (p / i) % p;
```

Разбор задач практики

1. **Решето Эратосфена**
   a) За $\mathcal{O}(n \log\log n)$ нашли все простые от 1 до n. Теперь для каждого простого p_k вычеркнем все числа на отрезке $[n^2..n^2+n]$, кратные ему. Сделаем это за $\mathcal{O}(\frac{n}{p_k})$.
   b) Предподсчитаем все простые от 1 до $\sqrt{n}$. Для каждого отрезка $[i\sqrt{n}..(i+1)\sqrt{n})$ вычеркнем все непростые за $\mathcal{O}(\sqrt{n}+\sqrt{n})$ (количество простые + длина отрезка).

2. **B-Гладкие**

   `is[x] = (p[x] <= B and is[x / p[x]])`

3. **Применяем решето**

```
int d[N]; // d[x] - минимальный простой делитель x
int cnt[N]; // cnt[x] - степень вхождения d[x]
int y[N]; // y[x] = x / d[x]^cnt[x]
// Запустили решето, нашли d[], d[1] = 0
cnt_div[1] = sum_div[1] = mu[1] = 1;
for (int x = 2; x < N; x++):
    int z = x / d[x];
    if (d[x] == d[z])
        cnt[x] = cnt[z] + 1, y[x] = y[z];
    else
        cnt[x] = 1, y[x] = z;
    cnt_div[x] = cnt_div[y[x]] * (cnt[x] + 1);
    sum_div[x] = sum_div[y[x]] * ((x / y[x] * d[x] - 1) / (d[x] - 1));
    mu[x] = cnt[x] > 1 ? 0 : -mu[y[x]];
```

4. **Евклид и ручной труд**

   $999 \cdot x + 10^9 \cdot y = 1$

   $10^9 \bmod 999 = 1 \Rightarrow$ решаем $999 \cdot x' + 1 \cdot y' = 1 \Rightarrow x' = 0,\ y' = 1.$

   $999 \cdot 0 + (10^9 - \lfloor \frac{10^9}{999} \rfloor \cdot 999) = 1 \Rightarrow -1\,001\,001 \cdot 999 + 10^9 \cdot 1 = 1 \Rightarrow x = -1\,001\,001$

5. **Расширенный Евклид**
   a) См. конспект.
   b) Индукция. База: $b = 0 \Rightarrow x = 1, y = 0$. Переход:
   $r = a - kb = a \bmod b \wedge (a-kb)x' + by' = (a,b)$
   $x = x' \wedge y = y' - kx'$, по индукции имеем $|x'| \leqslant b \wedge |y'| \leqslant r \Rightarrow |y' - kx'| \leqslant r + kb = a$ ■
   c) $ax_0 + my = (a,m) \Rightarrow ax_0\frac{b}{(a,m)} \equiv b \bmod m \Rightarrow x \in \{x_0\frac{b}{(a,m)} + k\frac{m}{(a,m)} \quad | \quad \forall k \in \mathbb{Z}\}$.
   d) $\forall k \in \mathbb{Z}\ \ (x_0, y_0) + k(\frac{b}{gcd(a,b)}, \frac{-a}{gcd(a,b)})$ — решение. $|x_0 + k\frac{b}{gcd(a,b)}| + |y_0 + k\frac{-a}{gcd(a,b)}|$ — почти линейная функция от k. Если бы мы знали, как раскрывается модуль, функция была бы линейной и минимум достигался бы на одном из краёв ⇒

   Решение: нарисуем прямую $ax + by = c$, она пересекает оси координат, проверим два решения ближние к абциссе, два решения ближние к ординате.

6. **RSA**
   a) Пусть $n = pq$, известно $\varphi(n) \Rightarrow \varphi(n) = n - p - q + 1 \Rightarrow p + q = -(\varphi(n) - n - 1) \Rightarrow x^2 + (\varphi(n) - n - 1)x + n = 0$ имеет корни p, q.

b) Нам дали $c = m^e \bmod n$. Загадаем случайное число r.
Дадим оракулу $r^e c \bmod n = (rm)^e \bmod n$, с вероятностью 0.01 он расшифрует.

7. **RSA и реальный мир**

Пример решения – каждый блок длины ≈16m (?) XOR-шифровать псевдослучайным ключом. Самый первый ключ получен или DH, или RSA.

8. **Биномиальные коэффициенты по модулю**

[e-maxx]
Если умеем по модулю p^k, то по КТО умеем и по модулю m.
Предподсчёт: для каждого p из разложения m храним все факториалы в форме $p^{k_i} \cdot r_i$.

9. (*) **Квадратичное решето**

По каждому простому модулю $p_k \leqslant B$ у нас есть квадратное уравнение: $i^2 + i \cdot \sqrt{M} + c_0 \equiv 0 \bmod p_k$. У квадратного уравнения по модулю p_k до 2 корней, найдём i_0 и i_1 за $\mathcal{O}(p_k)$, и возьмём серию $i_0 + p_k \cdot j$ и $i_1 + p_k \cdot j$. Таким образом за $\mathcal{O}(N \log \log B)$ мы поделим все числа, которые делятся на p_k, если какое-то доделится до 1, оно B-гладкое.

10. (*) **Магия**

См. конспект. Мы за $\mathcal{O}(p)$ посчитали обратные к $1..p-1$.

Домашнее задание

3.1. Обязательная часть

1. **(2) Евклид и полезность**

   Лягушонок Вася живёт на прямой. Он умеет целеустремлённо прыгать только вперёд.
   Устройство лапок позволяет прыгать ему только на a или b вперёд.
   Может ли он попасть в точку c?

2. **(2) Взлом RSA при малом** e

   Аня решила послать приглашение на секретную вечеринку Боре, Ване и Гоше. Аня разослала им одинаковый текст приглашения M закодированный с помощью RSA. У Вани, Бори и Гоши выбраны различные n, но ключ e у всех одинаковый: $e = 3$. Придумайте, как Дима сможет узнать (за полиномиальное от суммы длин всех чисел время), где будет происходить секретная вечеринка, если ему доступны все три шифрованных приглашения и открытые ключи.

3.2. Дополнительная часть

1. **(2) Подсчёт** d^p **в лоб**

   Мы умеем за $\mathcal{O}(n)$ для всех $x \in [2, n]$ искать $d[x]$ – минимальный простой делитель x. Умеем искать и $p[x]$, степень вхождения $d[x]$ в x, за $\mathcal{O}(n)$ динамикой.
   Докажите, что наивный поиск $p[x]$ работает тоже за $\mathcal{O}(n)$:
   `for (x = 2..N) for (y = x; d[y] == d[x]; y /= d[x]) p[x]++`

   Есть короткое док-во совсем без алгебры.

2. **(2) Попасть в взаимнопростое**

   Чтобы найти первообразный корень g, достаточно попасть в любое $g^j : (j, p-1) = 1$.
   Отсюда вопрос, какая вероятность случайным тыком попасть во взаимнопростое с $p-1$?