МФТИ

Алгоритмы и структуры данных, осень 2022

Семинар №07. Теория чисел

1. По данным числам a, b найдите целые x, y, такие что $ax + by = (a, b)$. Для каждого c опишите все решения уравнения $ax + by = c$.
2. За $O(n)$ для каждого $i \in [2, n]$ найдите $mind(i)$ — минимальный простой делитель i.
3. Дано простое число p, а также число a, причём $(a, p) = 1$. Как найти $a^{-1} \pmod p$?
4. Дано произвольное число m, а также число a, причём $(a, m) = 1$. Как найти $a^{-1} \pmod m$?
5. Приведите эффективный алгоритм для вычисления $a^{b^c} \pmod p$ для целых положительных a, b, c и простого p.
6. Найдите наибольший общий делитель двух **длинных** чисел a и b за полиномиальное время от их длины.
7. Найдите обратные к $1, 2, \ldots, n$ по простому модулю p за $O(n)$.
8. Найдите

а) $\sum\limits_{k=0}^{n} C_n^k$;

б) $\sum\limits_{k=0}^{n} k \cdot C_n^k$;

в) $\sum\limits_{k=0}^{n} k^2 \cdot C_n^k$.

9. Пусть дано n чисел от 2 до L. Проверьте каждое из них на простоту на общее время $O(\sqrt{L} + n\sqrt{L}/\log L)$.
10. Найдите количество пар целых положительных чисел (x, y), таких что $xy \leqslant n$, за $O(\sqrt{n})$.
11. За $O(\sqrt{n})$ найдите количество целых чисел в отрезке $[1, n]$, свободных от квадратов.
12. Найдите $\Phi(n) = \sum\limits_{k=1}^{n} \varphi(k)$, где $\varphi(\cdot)$ — функция Эйлера. Это число равно количеству пар взаимно простых чисел (a, b) с условиями $1 \leqslant a \leqslant b \leqslant n$. Асимптотика: а) $O(n)$; б) $O(n^{3/4})$.
13. Пусть g — первообразный корень по простому модулю p, то есть $\{g^0, g^1, \ldots, g^{p-2}\} = \{1, 2, \ldots, p-1\} \pmod p$. Предложите способ решать уравнения вида $g^x = a \pmod p$ за $O(\sqrt{p})$ в среднем.

1. Воспользуйтесь расширенным алгоритмом Евклида нахождения наибольшего общего делителя. Зная x' и y', такие что $ax' + (b\%a)y' = (a, b)$, найдите искомые x, y.
2. Если p — минимальный простой делитель числа k, то обновите $mind(k)$ при просмотре k/p.

```
vector<int> primes;
vector<int> mind(n + 1);
for (int i = 2; i <= n; ++i) {
    mind[i] = i;
}

for (int i = 2; i <= n; ++i) {
    if (mind[i] == i) {
        primes.push_back(i);
    }
    for (int p : primes) {
        if (p * i > n || p > mind[i]) {
            break;
        }
        mind[i * p] = p;
    }
}
```

---

3. Малая теорема Ферма утверждает (в данном случае), что $a^{p-1} \equiv 1 \pmod p$.
4. Теорема Эйлера утверждает (в данном случае), что $a^{\varphi(m)} \equiv 1 \pmod p$. Значение $\varphi(m)$ можно найти разложением m на простые сомножители. Альтернативно, можно решить уравнение $ax + my = 1$, тогда x будет обратным к a.
5. Нужно вычислить $b^c \pmod{p-1}$. Это можно сделать с помощью бинарного возведения в степень.
6. Воспользуйтесь соотношением

$$(a,b) = \begin{cases} 2\left(\frac{a}{2}, \frac{b}{2}\right), & \text{если } a \text{и } b \text{ чётны,} \\ \left(\frac{a}{2}, b\right), & \text{если } a \text{ чётно, а } b \text{ нечётно,} \\ (a, b-a), & \text{если } a \text{ и } b \text{ нечётны, и при этом } b \geqslant a. \end{cases}$$

7. Ищем $r_1, \ldots, r_n$. Очевидно, $r_1 = 1$. Далее, если все меньшие r_j найдены, то

$$r_i \equiv -\left\lfloor \frac{p}{i} \right\rfloor \cdot r_{p\%i} \pmod p.$$

8. Воспользуйтесь тем, что $k^2 = k(k-1) + k$.
9. За $O(\sqrt{L})$ найдите все простые на отрезке $[1, \sqrt{L}]$. Их по порядку будет $\sqrt{L}/\log L$.
10. Ответ равен

$$\sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor.$$

Слагаемое под знаком суммы принимает $O(\sqrt{n})$ различных значений.
11. Воспользуйтесь формулой включений-исключений: сначала возьмите все числа, затем исключите делящиеся на 4 или на 9, потом верните делящиеся на 36 и т.д. Ответ будет равен

$$\sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \mu(k) \left\lfloor \frac{n}{k^2} \right\rfloor.$$

Здесь $\mu(\cdot)$ — функция Мёбиуса.
12. Докажите, что

$$\sum_{d|k} \varphi(d) = k, \text{ и } \sum_{d=1}^{n} \Phi\left(\left\lfloor \frac{n}{d} \right\rfloor\right) = \frac{n(n+1)}{2}.$$

Отсюда

$$\Phi(n) = \frac{n(n+1)}{2} - \sum_{d=2}^{n} \Phi\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

13. Пусть $K = \lfloor \sqrt{p} \rfloor$. Сохраните $g^0, g^1, \ldots, g^K$ в одну хеш-таблицу, а $g^0, g^K, g^{2K}, \ldots, g^{K \cdot K}$ — в другую (нам хватит только второй). Тогда $x = \alpha K + \beta$, где $\alpha, \beta \in [0, K]$. Перебирайте β и проверяйте наличие подходящего α во второй хеш-таблице.