

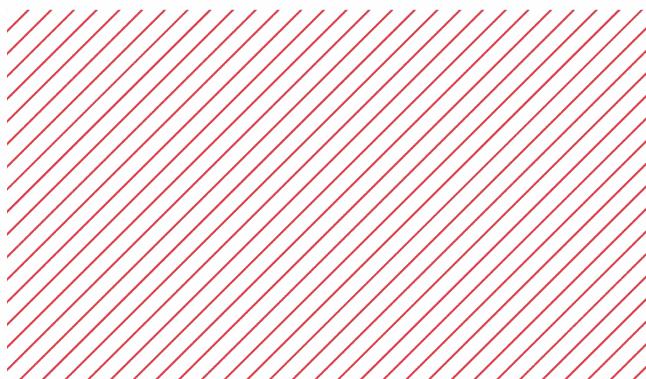
академия
больших
данных



Продвинутая теория чисел

Артем Васильев

Алгоритмы и структуры данных Advanced





Первообразный корень

- Работаем по простому модулю p
- Такой остаток g , что $g^0, g^1, \dots, g^{\phi(p)-1}$ различны
- Всегда существует по простому модулю
- А также по модулям $2, 4, p^k, 2p^k$



Первообразный корень

- Как найти?
- Оказывается, существует много
- $\phi(\phi(\text{mod}))$
- Пробуем случайные значения
- Или даже просто все подряд по возрастанию



Первообразный корень

- Как проверить?
- Медленно: нужно проверить, что среди g^1, g^2, \dots, g^{p-2} не встречается единица
- $O(p)$



Первообразный корень

- Быстрее: если $g^d = 1$, то d - делитель $p - 1$
- Проверяем только d вида $(p - 1) / q$, где q - какой-то простой делитель $p - 1$
- Используем двоичное возведение в степень
- $O(\log^2 p) + \text{факторизация}$



Дискретный логарифм

- Задача: уравнение вида $a^x = b \pmod{m}$, а взаимно просто с m
- Найти x
- Наивное решение за $O(m)$: перебрать все x и проверить



Baby-step-giant-step

- Представим $x = r * k - s$, $k \approx \sqrt{m}$
- $1 \leq r, s \leq k$
- Любое число от 0 до $m-1$ можно представить в таком виде
- $a^{rk-s} = b \pmod{m}$
- $a^{rk} = a^s b \pmod{m}$



Baby-step-giant-step

- Посчитаем множество чисел a^{rk} для всех k от 1 до m
- Аналогично посчитаем $a^s b$ для всех s от 1 до m
- Если в двух множествах есть общий элемент, $a^{rk} = a^s b$, то
нужный $x = rk - b$
- Работает за $O(\sqrt{m})$



Обмен ключами Диффи-Хеллмана

- Алиса, Боб, публичный канал связи
- Нужно обменять какой-то информацией, чтобы и Алиса, и Боб знали некий общий секрет
- Например, ключ для последующего симметричного шифрования
- Реализуем с помощью публичного канала связи!



Обмен ключами Диффи-Хеллмана

- Алиса и Боб придумывают случайные числа A и B
- Алиса посыпает g^A Бобу
- Боб посыпает g^B Алисе
- Алиса, зная g^B и A, вычисляет $(g^B)^A = g^{AB}$
- Боб, зная g^A и B, вычисляет $(g^A)^B = g^{AB}$
- Внешний наблюдатель знает g^A , g^B . Считается, что узнать g^{AB} сложно



Дискретный корень

- Уравнение вида $x^k = b \pmod{p}$
- Сведем к степеням первообразного корня
- $g^{(r^*t)} = g^s \pmod{p}$ для неизвестного t
- $r^*t = s \pmod{p - 1}$
- $O(\sqrt{p})$
- Можно быстрее!
- Сложно для составного модуля (RSA)



Проверка на простоту

- Тест Ферма: проверяет малую теорему ферма
- $a^{p-1} = 1 \pmod{p}$
- Берем случайное число, возводим в степень, проверяем
- Существуют составные числа, что на них тест Ферма не работает
- Числа Кармайкла



Тест Миллера-Рабина

- Уравнение $x^2 = 1 \pmod{m}$ имеет ровно два решения для простого m
- Если нашлось нетривиальное решение, то m - не простое
- Возьмем случайное a
- Как минимум, должен выполняться тест Ферма: $a^{m-1} = 1$



Тест Миллера-Рабина

- Представим $m - 1 = 2^f s$
- Посмотрим на последовательность $a^s, a^{2s}, a^{4s}, a^{8s}, \dots, a^{m-1}$
- Последнее число - единица
- Каждое следующее число - квадрат предыдущего
- Если есть пара соседних чисел, что $a^k \neq \pm 1$, но $a^{2k} = 1$, то m -
точно составное



Тест Миллера-Рабина

- Для составного m , количество таких a , которые проходят тест Миллера-Рабина, $< m/4$
- Без доказательства
- Вероятность false positive $< \frac{1}{4}$
- Если повторить 10 раз, вероятность $< 10^{-6}$



Факторизация

- Медленный метод: проверить все делители до \sqrt{m}
- Обозначим минимальный делитель m за d_{\min}
- Рассмотрим набор из k случайных чисел от 0 до $m - 1$
- Если $k \approx \sqrt{d_{\min}}$, то с неплохой вероятностью есть два числа с одинаковым остатком по модулю d_{\min}
- “Парадокс” дней рождений
- Тогда можно найти $\gcd(m, x - y)$ и разбиться рекурсивно на две подзадачи



ρ-метод Полларда

- Будем генерировать “случайную” последовательность чисел
- Случайное первое число a_0
- Следующее число $a_{i+1} = f(a_i)$
- $f(x) = (x^2 + c) \bmod m$
- Функция, ведущая себя достаточно случайно



ρ-метод Полларда

- Будем искать два числа в последовательности a_0, a_1, a_2, \dots , что $\gcd(a_i - a_j, m) > 1$
- Достаточно проверять только пары вида (a_i, a_{2i})
- Два указателя, один ходит на один шаг, второй ходит по два шага
- $O(\sqrt{d_{\min}})$ шагов в среднем
- $O(m^{1/4})$ в худшем случае