

«Алгоритмы дискретного логарифмирования. Алгоритм согласования, алгоритм Полига- Хеллмана»

Подготовила: Гусева Екатерина (6373)

Задача дискретного логарифмирования

Пусть G – мультипликативная абелева группа, $a, b \in G$. Тогда задача нахождения решения уравнения

$$a^x = b$$

Называется задачей дискретного логарифмирования в группе G . Её решение x называется дискретным логарифмом элемента b по основанию a , если основание a фиксировано и если существует $\log_a b \in \mathbb{Z}/|G|\mathbb{Z}$, если $|G| < \infty$.

Задача дискретного логарифмирования

Рассмотрим уравнение

$$a^x \equiv b \pmod{p} \quad (1)$$

В группе $(\mathbb{Z}/p\mathbb{Z})^*$ где p – простое число. Будем предполагать, что порядок $a \pmod{p}$ равен $p - 1$. Тогда уравнение разрешимо, и решение x является элементом $\mathbb{Z}/(p - 1)\mathbb{Z}$.

С помощью перебора уравнение (1) можно решить за $O(p)$ Арифметических операций. Но можно ли придумать более эффективный алгоритм?

Алгоритм согласования

(Алгоритм Гельфонда — Шенкса)

Теория

Идея алгоритма состоит в выборе оптимального соотношения времени и памяти, а именно в усовершенствованном поиске показателя степени.

$$a^x \equiv b \pmod{p}$$

Алгоритм поиска x основан на представлении x в виде $Hu - v \pmod{p-1}$, где $H = \lfloor \sqrt{p} \rfloor + 1$ и переборе $1 \ll u \ll H, 0 \ll v \ll H$.

Данный алгоритм имеет сложность $O(p^{1/2} \log p)$

Алгоритм

Шаг 1. $H = \lfloor \sqrt{p} \rfloor + 1$

Шаг 2. Найти $c \equiv a^H \pmod{p}$

Шаг 3. Составить таблицу значений $c^u \pmod{p}$, $1 \ll u \ll H$, упорядочить её

Шаг 4. Составить аналогичную таблицу $b * a^v \pmod{p}$,

$0 \ll v \ll H$, упорядочить

Шаг 5. Найти совпадающие элементы для 1 и 2 таблиц. Для них

$$c^u \equiv b * a^v \pmod{p}$$

Из шага 2 и нехитрых математических преобразований прямо следует, что $a^{Hu - v} \equiv b \pmod{p}$

Значит, мы нашли $x \equiv Hu - v \pmod{p - 1}$

Доказательство корректности алгоритма

Любое число x , $0 \ll x \ll p - 2$ можно представить в виде $x \equiv Hu - v \pmod{p - 1}$, где $1 \ll u \ll H$, $0 \ll v \ll H$. Действительно, набор чисел $H, H - 1, H - 2, \dots, H - H, 2H, 2H - 1, \dots, 2H - H, \dots, H^2, H^2 - 1, \dots, H^2 - H$ содержит в себе набор чисел $0, 1, \dots, p - 2$, поскольку $H^2 > p$. Из этого следует корректность алгоритма.

Примеры

Пусть $5^x \equiv 3 \pmod{23}$

Тогда $H = \lceil \sqrt{23} \rceil + 1 = 5$, $c \equiv a^H \pmod{p} \equiv 5^5 \pmod{23} = 20$

Составляем таблицу для $c^u \pmod{p}$, $1 \ll u \ll H$:

u	1	2	3	4	5
5^u	20	9	19	12	10

Составляем таблицу для $b * a^v \pmod{p}$, $0 \ll v \ll H$:

v	0	1	2	3	4	5
$3 * 5^v$	3	15	6	7	12	75

$$x = Hu - v = 5 * 4 - 4 = 16 \pmod{23}$$

$$5^{16} \equiv 3 \pmod{23}$$

Усовершенствование производительности алгоритма

Реализация

Существует способ улучшить производительность алгоритма Гельфонда — Шенкса. Он заключается в использовании эффективной схемы доступа к таблице. Лучший способ — использование хеш-таблицы. Следует производить хеширование по второй компоненте, а затем выполнять поиск по хешу в таблице. Так как доступ и добавление элементов в хеш-таблицу работает за время $O(1)$ (константа), то асимптотически это не замедляет алгоритм.

Время работы алгоритма оценивается как $O(\sqrt{n})$, что намного лучше, чем время работы полного перебора показателей степени

Алгоритм Полига - Хеллмана

Пусть задано уравнение

$$a^x \equiv b \pmod{p}$$

И известно разложение числа $p-1$ на простые множители:

$$p - 1 = \prod_{i=1}^{i=k} q_i^{\alpha_i}$$

Идея алгоритма

Суть алгоритма в том, что достаточно найти x по модулям $q_i^{\alpha_i}$ для всех i , а затем решение исходного сравнения можно найти с помощью китайской теоремы об остатках.

Чтобы найти x по каждому из таких модулей, нужно решить сравнение

$$(a^x)^{\frac{(p-1)}{q_i^{\alpha_i}}} \equiv b^{\frac{(p-1)}{q_i^{\alpha_i}}} \pmod{p}$$

Алгоритм

1 шаг. Для каждого простого числа $q, q \mid p - 1$ составляем таблицу чисел

$$r_{q,j} \equiv a^{\frac{j(p-1)}{q}} \pmod{p} \quad j = 0, \dots, q - 1$$

2 шаг. Для каждого простого числа $q, q, q^\alpha \mid p - 1$ находим $\log_a b \pmod{q^\alpha}$

Пусть $x \equiv \log_a b \pmod{q^\alpha} \equiv x_0 + x_1 q + \dots + x_{\alpha-1} q^{\alpha-1} \pmod{q^\alpha}$, где $0 \ll x_i \ll q - 1$. Тогда из (1) следует, что

$$b^{\frac{(p-1)}{q}} \equiv a^{\frac{x_0(p-1)}{q}} \pmod{p}$$

С помощью таблицы шага 1 находим x_0 . Тогда выполнено сравнение:

$$(ba^{-x_0})^{(p-1)/q} \equiv a^{\frac{x_1(p-1)}{q}} \pmod{p}$$

Аналогично находим остальные x . Находим

$\log_a b \pmod{p - 1}$ с помощью китайской теоремы об остатках