«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 а фиксировано и если существует $\log_a b \epsilon Z/|G|Z$, если $|\mathrm{G}| < \infty$.

Задача дискретного логарифмирования

Рассмотрим уравнение

$$a^x \equiv b(mod\, p) \quad (1)$$

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

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.

$$a^x \equiv b(mod\ p)$$

Алгоритм поиска x основан на представлении x в виде $Hu - v\ mod\ (p-1)$, где $H = \left|\sqrt{p}\right| + 1$ 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 $c \equiv a^H (mod\ p)$

Шаг 3. Составить таблицу значений $c^u (mod\ p)$, $1 \ll u \ll H$, упорядочить её

Шаг 4. Составить аналогичную таблицу $b * a^v (mod\ p)$,

$0 \ll v \ll H$, упорядочить

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

$$c^u \equiv b * a^v (mod\ p)$$

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

Значит, **мы нашли** $\boldsymbol{x \equiv Hu - v\ mod(p-1)}$

Доказательство корректности алгоритма

Любое число x, $0 \ll x \ll p - 2$ можно представить в виде $\mathrm{x} \equiv \mathrm{Hu} - \mathrm{v} \bmod (\mathrm{p} - 1)$, где $1 \ll \mathrm{u} \ll \mathrm{H}$, $0 \ll v \ll H$. 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 $H\hat{}2 > p$. Из этого следует корректность алгоритма.

Алгоритм Полига - Хеллмана

Пусть задано уравнение

$$a^x \equiv b(mod\ p)$$

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

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

Алгоритм

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

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

2 шаг. Для каждого просто числа q, $q, q^{\propto} \mid p - 1$ находим $\log_a b\ (mod\ q^{\propto})$
Пусть $x \equiv \log_a b\ (mod\ q^{\propto}) \equiv x_0 + x_1 q + \dots + x_{\propto-1} q^{\propto-1} (mod\ q^{\propto})$, где
$0 \ll x_i \ll q - 1$. Тогда из (1) следует, что

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

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

$$(ba^{-x_0})^{(p-1)/q} \equiv a^{\frac{x1(p-1)}{q}} (mod\ p)$$

Аналогично находим остальные x. Находим
$\log_a b\ (mod\ p - 1)$с помощью китайской теоремы об остатках