

«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
20^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

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

Упрощенный вариант описания

Лучший путь, чтобы разобраться с алгоритмом – рассмотреть крайний случай, когда p раскладывается на $2^n + 1$

Учитываем, что, по определению, a имеет степень $p - 1$, следовательно:

$$a^{(p-1)} \equiv 1 \pmod{p} \text{ (1)}$$

Когда $p = 2^n + 1$, то легко определить x через двоичное разложение с коэффициентами $\{q_0, q_1 \dots q_{n-1}\}$, например:

$$x = \sum_{i=0}^{n-1} q_i 2^i = q_0 + q_1 * 2^1 + \dots + q_{n-1} * 2^{n-1}$$

Следствие из (1):

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

Но $a^{(p-1)/2}$ по определению принимает значение, отличное от 1, значит, остаётся одно сравнение:

$$a^{(p-1)/2} \equiv -1 \pmod{p} \text{ (2)}$$

Упрощенный вариант описания

Теперь возведём $a^x \equiv b \pmod{p}$ в степень $\frac{p-1}{2}$:

$$(a^x)^{(p-1)/2} \equiv b^{\frac{p-1}{2}} \pmod{p}$$

Из выкладки (2) следует:

$$(-1)^x \equiv b^{(p-1)/2} \pmod{p}$$

Равенство $(-1)^x = 1$ справедливо, если x – четное, то есть, если в разложении x в виде многочлена свободный член $q_0 = 0$. Соответственно, $(-1)^x = (-1)$, если $q_0 = 1$.

Значит, q_0 всегда можно определить по $b^{(p-1)/2}$ таким образом:

$$b^{(p-1)/2} \pmod{p} \equiv \begin{cases} 1, & q_0 = 0 \\ -1, & q_0 = 1 \end{cases} \quad (3)$$

Упрощенный вариант описания

Теперь преобразуем $b \equiv a^x \pmod{p} \equiv a^{q_0+x_1} \pmod{p}$

Где x_1 – многочлен $(x - q_0)$

Можно ввести новую переменную $z_1 \equiv b * a^{-q_0} \equiv a^{x_1} \pmod{p}$

Рассуждая образом, схожим с тем, что привел нас к выводу (3), приходим к выводу, что

$$z_1^{(p-1)/4} \equiv \begin{cases} 1, & q_1 = 0 \\ -1, & q_1 = 1 \end{cases} \quad (4)$$

Откуда находим q_1 .

Вполне чётко вырисовывается общий алгоритм нахождения всех q_i :

Обозначим степень за $m_i = (p-1)/2^{i+1}$

$$z_i \equiv b * a^{-q_0 - q_1*2 - \dots - q_{n-1}*2^{i-1}} \equiv a^{x_i} \pmod{p}$$

Где

$$x_i = \sum_{k=i}^{n-1} q^k * 2^k$$

$$z_i^{m_i} \equiv (-1)^{q_i} \pmod{p}$$

См. (4), легко находим q_i .

В результате нетрудно вывести $x = q_0 + q_1 * 2^1 + \dots + q_{n-1} * 2^{n-1}$.

Пример применения упрощенного варианта

Пусть $a = 3, b = 11, p = 17 = 2^4 + 1$

Тогда $p - 1 = 2^4$ и x можно представить в виде:

$$x = q_0 + 2 * q_1 + 2^2 * q_2 + 2^3 * q_3$$

1)Находим q_0 :

$$b^{\frac{p-1}{2}} = 11^8 = -1 \pmod{17} \rightarrow q_0 = 1$$

2)Находим $z_1 = b * a^{-q_0} = 11 * 3^{-1} = -2 \pmod{17}$

и
$$m_1 = \frac{p-1}{2^{1+1}} = \frac{17-1}{2^2} = 4$$

Находим q_1 как $z_1^{m_1} = -1 \pmod{17} \rightarrow q_1 = 1$

3)Находим z_2 и m_2 :

$$z_2 = z_1 * a^{-q_1 * 2^1} = (-2) * 3^{-2} = 13 \pmod{17}$$

$$m_2 = \frac{p-1}{2^{3+1}} = \frac{17-1}{2^4} = 1$$

Находим q_2 как $z_2^{m_2} = -1 \pmod{17} \rightarrow q_2 = 1$

Аналогично находим $q_3 = 0$

4) Находим искомый x :

$$x = 1 + 2 * 1 + 4 * 1 + 0 = 7$$

$$3^7 \equiv 11 \pmod{17}$$

Алгоритм (основной)

1 шаг. Для каждого простого делителя числа $(p - 1)$ q_i ($i \in \{1, s\}$) составляем таблицу чисел

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

2 шаг. Для каждого q_i можно представить x через

$$x = x_0 + x_1 * q_i + \dots + x_{a-1} * q_i^{a-1} \pmod{q_i^{a_i}}$$

где $0 \leq x_i \leq q_i - 1$

Тогда верно сравнение (*):

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

С помощью таблицы, составленной на первом шаге, можно **найти x_0** .

3 шаг. Для j от 0 до $q_i - 1$ ЦИКЛ:

Рассматриваем сравнение $a^{x_j * \frac{p-1}{q_i}} = (b * a^{-x_0 - x_1 * q_i - \dots - x_{j-1} * q_i^{j-1}})^{\frac{p-1}{q_i^{j+1}}} \pmod{p}$

Решение каждый раз находится через r -таблицу.

Конец цикла по j

Конец цикла по i

4 шаг. Мы получим s значений x по модулям q_i и значение x по модулю $(p-1)$ можно **найти с помощью китайской теоремы об остатках**

Об эффективности применения

Для применения алгоритма Полига-Хеллмана необходимо знать разложение на множители. В общем случае задача факторизации — достаточно трудоёмкая, однако если делители числа — небольшие (в том смысле, о котором сказано выше), то это число можно быстро разложить на множители даже методом последовательного деления. Таким образом, в том случае, когда эффективен алгоритм Полига-Хеллмана, необходимость факторизации не усложняет задачу.