数学第二讲
离散对数、元根、反演

丁尧尧

上海交通大学

August 12, 2017

目录

对于以下问题:

Definition (离散对数)

给定 a,b,m，其中 a 与 m 互素，求最小的非负（正）整数 x，使得:

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

我们称 x 为在模 m 意义下，以 a 为底的 b 的离散对数，记作 $ind_a b$。

给出 a, b, m，（我们假设 a 与 m 互素）我们如何求 x 呢？

有一个叫做大步小步的算法（Baby Step Giant Step）。我们假设 $x = ic + j$ 是一个答案（其中 c 是我们自己选定的一个在 $2, m-1$ 之间的数）。我们先计算出：

$$a^1, a^2, a^3, \cdots, a^{b-1}$$

如果发现其中某个值是 b，那么我们就找到答案了。否则，我们将这些数放在一个数据结构中（平衡二叉树，哈希表都可以），要求可以通过 a^i 的值快速得到 i。那么我们再依次算出：

$$ba^{-c}, ba^{-2c}, \cdots, ba^{-kc}$$

每算完一个 ba^{-ic}，我们就看上面的数据结构中是否有一个值 a^j 等于它，如果有，那么它们满足：

$$a^j \equiv ba^{-ic} \pmod{m}$$

即：

$$a^{ic+j} \equiv b \pmod{m}$$

分析复杂度，如果我们上面用哈希表存，那么可以 $O(1)$ 判断某个值是否存在。
那么我们总共需要计算的数的个数是 $O(b+\frac{m}{b})$，我们取 $b=\sqrt{m}$，
可以得到 $O(\sqrt{m})$ 的复杂度.
上面的方法,a 不限于整数，还可以是矩阵，但都有同一个要求，即 a 存在乘法逆元.

我们先介绍一些概念.

Definition (剩余系)

对于给定模数 $m(m > 0)$, 如果有一组数 $\{a_i\}$:

$$a_1, a_2, a_3, \ldots, a_m$$

满足:

$$a_i \neq a_j \quad (i \neq j)$$

那么我们将 $\{a_i\}$ 称作模 m 的一组完全剩余系.

类似的有:

Definition (既约剩余系)

对于给定模数 $m(m > 0)$，如果有一组数 $\{a_i\}$:

$$a_1, a_2, a_3, \ldots, a_k$$

满足:

$$a_i \neq a_j \quad (i \neq j)$$

以及:

$$gcd(a_i, m) = 1$$

那么我们将 $\{a_i\}$ 称作模 m 的一组既约剩余系.

模 m 的既约剩余系的数的个数记作 $\varphi(m)$.

Definition (阶)

给定一个与 m 互素的 a，则最小的一个满足:

$$a^r \equiv 1 \pmod{m}$$

的正整数 r 叫做 a 模 m 的阶，一般记作 $r = \delta_m(a)$

Definition (元根)

对于模数 m，如果存在一个数 g，满足:

$$\delta_m(g) = \varphi(m)$$

我们则称 g 为模 m 的一个元根

我们知道，如果 a 与 m 互素，那么：

$$a^1, a^2, a^3, \ldots, a^i, \ldots$$

都与 m 互素，即它们都是缩系的元素.
元根的意义在于，将缩系中的每一个元素，都与一个 g^i 这种形式对应起来.
假如我们找到了一个模 m 的元根 g，想求其缩系中的一个元素 a 对应的指数是什么，我们就可以用离散对数找到满足：

$$g^i \equiv a \pmod{m}$$

的 i.

并不是所有数都有元根.

Theorem

只有形如:

$$1, 2, 4, p^i, 2p^i$$

的数存在元根.

那么我们怎样找元根呢?

Theorem

如果存在正数 a, b, m, 且 $gcd(a, m) = 1$, 满足

$$a^b \equiv 1 \pmod{m}$$

那么有:

$$\delta_m(a) \mid b$$

通过上面这个定理可以证明:

Theorem

对于给定的与 $m > 2$ 互素的一个数 g, g 是 m 的一个元根当且仅当对于 $\varphi(m)$ 的所有素因子 p_i, 有:

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod m$$

因为在 10^9 范围内的所有素数的最小的元根都很小 (最大的不过一百多), 所以我们可以暴力从小到大 check.

我们来道例题看看:

例题 1

给你 a, b, m，都是正整数，其中 m 是素数，求:

$$a^x \equiv b \quad (mod\ m)$$

其中:$2 \leq m \leq 2 \times 10^9$,$1 \leq a, b \ < m$

很容易离散对数就可以秒了对不对.

例题 2

给你 a_1, b_1, a_2, b_2, m, 都是正整数, 其中 m 是素数, 求满足下面条件的 x:

$$a_i^x \equiv b_i \quad (mod m) \quad (i = 1, 2)$$

其中:$2 \leq m \leq 2 \times 10^9$

先找到 m 的一个元根, 然后找到 a_i 和 b_i 的离散对数:

$$g^{c_i} \equiv a_i \quad (mod m)$$

$$g^{d_i} \equiv b_i \quad (mod m)$$

然后就把问题化简成了:

$$g^{xc_i} \equiv g^{d_i} \quad (mod m)$$

因为 g 是模 m 的元根, 所以上面的方程等价于:

$$xc_i \equiv d_i \quad (mod \quad m-1)$$

从而把问题转化为解一元一次同余方程组的问题.

例题 3

给你 a, b, m，其中 m 是质数，求 x 满足:

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

同样先求离散对数，然后解一次方程，得到 $ind_g(x)$，最后快速幂一下就行了.

元根，离散对数，主要的作用是把一些和指数有关的问题转化成一般的一次同余方程，类似于正实数上的开 log 运算.
只是在模意义下，我们的底需要精细地选取.