数学第二讲

离散对数、元根、反演

丁尧尧

上海交通大学

August 4, 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：

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