求解$x^a \equiv b(mod\ m)$

CDQZ OI Team*

July 14, 2011

Contents

1 题目描述

求方程$x^a \equiv b(mod\ m)$的所有解，其中m是素数。

2 理论支持

2.1 定义

r对模m的指数$Ord_m(r)$为使$r^d \equiv 1\ (mod\ m)$成立的最小正整数，若$Ord_m(r) = \varphi(m)$，则称r是m的原根。

*发现者：before_rain，探索者：ymfoi，执笔者：csimstu

2.2 性质

令$\delta = Ord_m(r)$，则$r^0, r^1, r^2 \ldots, r^{\delta-1}$模$m$两两不同余。假设同余，就可以得到一个更小的$\delta$，于假设不符。

2.3 用途

由于m是素数，由费马小定理知，$r^{m-1} \equiv 1 \ (mod\ m)$，故$\delta = \varphi(m) = m - 1$。于是，$r^0, r^1, r^2 \ldots, r^{m-2}$恰好组成了一个1到$m-1$的排列[1]。反过来，每一个1到$m-1$的的数（即这个同余系中的每一个数）都可以表成$r^k$。不妨设$x = r^i$，$b = r^j$，于是有

$$r^{ia} \equiv r^j \ (mod\ m)$$

因为$r^0, r^1, r^2 \ldots, r^{m-2}$恰好组成了一个1到$m-1$的排列，所以上式可写成$ia \equiv j \ (mod\ m-1)$。如果求得了$j$，就能解出$i$，从而得到$x = r^i$的值。

3 Stage I: 求m的原根

目前还没有快速求原根的方法。幸运的是，解决本问题只需求出一个原根，且经过科学验证，在小于10^9的数中，每个数最小的原根最多只有几十。枚举原根r即可。验证也可以做得很快：可以证明，只需验证$\frac{m-1}{p}$，其中p是能整除$m-1$的素数。可以暴力分解质因数。

4 Stage II: 求离散对数j

因为$j \leq m-1$，可以设$p = \lfloor \sqrt{m-1} \rfloor$，这样一来，$j$可以写成$j = pk + s$，只需要枚举$k$于$s$中的一个，利用乘法逆元，看另一个是否能满足。如果套上map，复杂度为$O(\sqrt{m} \log m)$;

5 Stage III: 解线性同余方程

直接上扩展欧几里得算法。在算每一个解的时候，可以暴力枚举，直到出现重复，因为答案肯定不会太多。

6 注意事项

1. 不管是乘法还是加法都要记得转long long并取模。特别注意加法以及负数。
2. 用扩展欧几里得算法时要注意答案是否完整。

[1] 只考虑$r > 0$的情况，$r = 0$可以特判。

7 代码

1. ymfoi的代码，特点：形状优美，结构匀称。
2. csimstu的代码，特点：耦合度低，易于阅读，STL使用较多，pascaler慎入。