

BSGS 及其拓展

I. BSGS

一. 算法思想:

BSGS 主要应用了分块的思想,或者说“meet in middle”。

细节方面,网络上资源很多,这里不再赘述

二. 局限性: 求逆元时使用了费马小定理,故模数必须是素数

三. 参考代码¹: <http://paste.ubuntu.com/23049155/>²

II. 拓展 BSGS

一. 问题分析:

a) 既然 BSGS 在使用费马小定理时受到限制,那我们就尝试使用拓展欧几里得算法来求逆元。³

b) 直接使用拓展欧几里得算法的话,因为是多解,所以得枚举所有的解,所以复杂度不再是 \sqrt{n} ⁴

c) 为什么针对素数的 BSGS 不需要枚举所有解呢? 是素数的话 p , 设拓展欧几里得求出的基本可行解为 x , 则通解为 $x+k*p$, 在模 p 的意义下,恒为 x 。所以不需要考虑多解的情况

二. 算法思想:

¹ 这里提供的是 Hash 版本,速度会明显比 map/set 版本快。另外 BSGS 是不用带 log 的哦!

² 配套例题: <http://www.lydsy.com/JudgeOnline/problem.php?id=2242>

³ 所以不一定有解

⁴ 实际测试中,这样确实慢了很多,但可以通过部分题目。

参考代码: <http://paste.ubuntu.com/23051295/>

配套题目: <http://www.lydsy.com/JudgeOnline/problem.php?id=2995>

假设我们要求解 $a^x \equiv b \pmod{c}$

我们先将 a^x 与 c 的所有公因数提出来, 将这部分单独算对于答案的贡献。记提取公因数后的 c 为 c'

此时 a^x 与 c' 互质了, 再使用“问题分析 a)”中提到的算法即可⁵

总体时间复杂度仍为 $O(\sqrt{n})$

三. 代码参考: <http://paste.ubuntu.com/23051475/>⁶

III. Reference:

- 一. hht 口述
- 二. 《算法竞赛入门经典·第二版》
- 三. Tony Fang's Blog: tonyfang.is-programmer.com

⁵ a^x 与 c 互质了, 所以与 c 为素数的情况类似, 此时在 $\%c$ 的情况下, 也之多有一个解

⁶ 配套例题: <http://www.lydsy.com/JudgeOnline/problem.php?id=2995>