

小蒟蒻yyb的博客

AFO

| | | | | | | |
|-----|----|-----|----|----|----|----------------------------|
| 博客园 | 首页 | 新随笔 | 联系 | 订阅 | 管理 | 随笔 - 1280 文章 - 0 评论 - 1717 |
|-----|----|-----|----|----|----|----------------------------|

BSGS算法

BSGS算法

我是看着ppl的博客学的，您可以先[访问ppl的博客](#)

Part1 BSGS算法

求解关于 x 的方程

$$y^x = z(mod\ p)$$

其中 $(y, p) = 1$

做法并不难，我们把 x 写成一个 $am - b$ 的形式

那么，原式变成了

$$y^{am} = zy^b(mod\ p)$$

我们求出所有 b 可能的取值($0 \sim m-1$)，并且计算右边的值

同时用哈希或者 map 之类的东西存起来，方便查询

对于左边，我们可以枚举所有可能的 a ，然后直接查右边的值有没有相等的即可

复杂度是 $O(max(m, p/m))$

不难证明 $m = \sqrt{p}$ 时复杂度最优

所以 $bsgs$ 算法的复杂度是 $O(\sqrt{p})$

模板题：[SDOI2011 计算器](#)

关键代码：

```
int m=sqrt(p)+1;Hash.Clear();
for(RG int i=0,t=z;i<m;++i,t=1ll*t*y%p)Hash.Insert(t,i);
for(RG int i=1,tt=fpow(y,m,p),t=tt;i<=m+1;++i,t=1ll*t*tt%p)
{
    int k=Hash.Query(t);if(k!=-1)continue;
    printf("%d\n",i*m-k);return;
}
```

使用 map 会多个 \log ，在洛谷上我写的 $Hash$ 目前是跑得最快的。。。

Part2 拓展BSGS

假设 $gcd(y, p) \neq 1$ 怎么办？

令 $d = gcd(y, p)$

将方程改写成等式形式


$$y^x + kp = z$$

发现此时的 z 必须要是 d 的倍数，否则无解。

因此，除掉 d

$$\frac{y}{d}y^{x-1} + k\frac{p}{d} = \frac{z}{d}$$

公告

 AmazingCounters.com

 给我写信

-----About Me-----

坐标：HN-CS-CJ
已经退役的大菜鸟。 蒟蒻yyb的
QQ:1357828232
喂喂喂，加我QQ的验证问题填yyb就好啦嘛
QwQ
请备注一下年级和学校还有您的名字（缩写就行啦）
欢迎大家来交换友链

-----有史以来最菜的人-----

垃圾yyb的CSDN博客

-----同一届的巨佬们-----

萝卜
zzzzsy
YCB
the_Despair!
NeosKnight
CyhlInj pp!!!!(AFO)
fdfdf(AFO)
FlashHu(AFO)
lalaxu!lxzy!!(AFO)
mona!(AFO)
zctoylm 小胖(AFO)
Tyher(AFO)
eternal风度 卍(AFO)
ysn(AFO)
dwq(AFO)
Cwen(AFO)
Brïoche lkj(AFO)
特殊部分：单向orz 大聚聚cx233666(怎么大聚聚也AFO了啊喂)

-----学长们-----

wfj_2048(AFO)
贱狗老师(AFO)

-----外校的大佬们-----

Redbag(y!x)
XSC肖查查
Bill Yang
dkw!
xMinh
YYJcaili(有人要求写“麓山第一巨佬”？？)
(被称作麓山第二的？？)jeff小蒟蒻
Refun?Aufun!!!
苏卿念
poorpool破池姐姐！
神仙yyw
litble!!!!
zjp-shadow又吊打我了
Mychael!
zhouzhendong
zyk
fwat
ErkkiErkko
子谦。
slr
Dispwnl
Little_Jian
Paulliant
CDQZ dxy
memset0
wjyyy
Qiuly
CDSS ldx
PhantasmDragon
Tgotp
lk!!!
xht37
heanda
zgjjj
sigongzi
彼柒_littleseven

---将(tian)来(tian)爆踩我们的学弟们---
M-sea
YCH, smy
鸡贼贼、呆鸡、尿鸡
杜杜熊、杜老师
球球

猫贼贼、屎猫
糖姐姐tjj
切题无数的Itst tq
heyujun
xxz
Qihoo360
gj尻
hbx

昵称： 小蒟蒻yyb
园龄： 2年11个月
粉丝： 319
关注： 36
+加关注

| 2019年10月 | | | | | | |
|----------|----|----|----|----|----|----|
| 日 | 一 | 二 | 三 | 四 | 五 | 六 |
| 29 | 30 | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | 31 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |

搜索

积分与排名

积分 - 278082
排名 - 1196

随笔分类

- A -- 模板(27)
- A -- 题解(70)
- A -- 游记&杂项(23)
- A -- 知识点(55)
- OJ -- 51NOD(4)
- OJ -- AtCoder(34)
- OJ -- BZOJ(667)
- OJ -- CJOJ(62)
- OJ -- CodeForces(88)
- OJ -- HDU(26)
- OJ -- Loj(40)
- OJ -- POJ(22)
- OJ -- TopCoder(1)
- OJ -- Uoj(48)
- OJ -- Vjudge(35)
- OJ -- 洛谷(167)
- OJ -- 牛客网(3)
- Source -- NOI(60)
- Source -- NOIIP(30)
- Source -- 各省省选(445)
- Source -- 网络流24题(23)
- 动态规划 -- 决策单调性(4)
- 动态规划 -- 轮廓线&插头(4)
- 动态规划 -- 凸优化(6)
- 动态规划 -- 斜率优化(11)
- 动态规划 -- 状态压缩(22)
- 多项式 -- FFT(38)
- 多项式 -- FWT(10)
- 多项式 -- 常数阶线性递推(3)
- 多项式 -- 多项式运算(12)
- 多项式 -- 拉格朗日插值(7)
- 多项式 -- 生成函数(13)
- 基础算法 -- 动态规划(287)
- 基础算法 -- 模拟(20)
- 基础算法 -- 三分(2)
- 基础算法 -- 搜索(35)
- 基础算法 -- 贪心(78)
- 计算几何 -- 半平面交(2)
- 计算几何 -- 闵可夫斯基和(1)
- 计算几何 -- 其他(4)

这样前面的 y/d 就是一个系数了，
不断检查 $\gcd(\frac{z}{d}, y)$ ，一直除到互质为止
此时的形式就变成了

$$\frac{y^k}{d}y^{x-k} = \frac{z}{d} \pmod{\frac{p}{d}}$$

这样子 $bsgs$ 求解之后在还原回去就行了。

模板:SPOJ Power Modulo Inverted

关键代码

```
void ex_BSGS(int y,int z,int p)
{
    if(z==1){puts("0");return;}
    int k=0,a=1;
    while(233)
    {
        int d=__gcd(y,p);if(d==1)break;
        if(z%d){NoAnswer();return;}
        z/=d;p/=d;++k;a=1ll*a*y/d%p;
        if(z==a){printf("%d\n",k);return;}
    }
    Hash.clear();
    int m=sqrt(p)+1;
    for(int i=0,t=z;i<m;++i,t=1ll*t*y%p)Hash.Insert(t,i);
    for(int i=1,tt=fpow(y,m,p),t=1ll*a*tt%p;i<=m;++i,t=1ll*t*tt%p)
    {
        int B=Hash.Query(t);if(B==-1)continue;
        printf("%d\n",i*m-B+k);return;
    }
    NoAnswer();
}
```

分类: A -- 知识点

好文要顶

关注我

收藏该文

小蒟蒻yyb
关注 - 36
粉丝 - 319
+加关注

« 上一篇: 【BZOJ2329】括号修复 (Splay)
» 下一篇: 【SPOJ】Power Modulo Inverted (拓展BSGS)

posted @ 2018-04-12 19:51 小蒟蒻yyb 阅读(2860) 评论(3) 编辑 收藏

评论列表

#1楼 2018-04-30 22:28 菜狗xzz

orz 博主

引用
对于左边，我们可以枚举所有可能的m，然后直接查右边的值有没有相等的即可

这一段的m应该改成a吧

可能是我太菜了orz

支持(0) 反对(0)

#2楼 2018-10-03 09:40 小蒟蒻ysn