BSGS算法

用于求解 $A^x=B(mod C)$ 这样的方程

当A与C互质时，令 $x=im+j$, 原式可化为 $A^j=B\cdot A^{-mi}(mod C)$ 然后循环遍历j并把 $(A^{j}\%C,j)$ 加入哈希表中，然后枚举左边 $B\cdot A^{-mi}\%C$从哈希表中查找，若存在，则得到一组解

代码

```
#define MOD 76543
int hs[MOD],head[MOD],next[MOD],id[MOD],top;
void insert(int x, int y)
{
    int k = x%MOD;
    hs[top] = x, id[top] = y, next[top] = head[k], head[k] = top++;
}
int find(int x)
{
    int k = x%MOD;
    for(int i = head[k]; i != -1; i = next[i])
        if(hs[i] == x)
            return id[i];
    return -1;
}
int BSGS(int a,int b,int c)
{
    memset(head, -1, sizeof(head));
    top = 1;
    if(b == 1)
        return 0;
    int m = sqrt(c*1.0), j;
    long long x = 1, p = 1;
    for(int i = 0; i < m; ++i, p = p*a%c)
        insert(p*b%c, i);
    for(long long i = m; ;i += m)
    {
        if( (j = find(x = x*p%c)) != -1 )
            return i-j;  //a^(ms-j)=b(mod c)
        if(i > c)
            break;
    }
    return -1;
}
```

题目

洛谷p3846

BSGS模板题

```
#include <iostream>
#include <cstdio>
#include <algorithm>
#include <cstring>
#include <cmath>
#include <map>

using namespace std;

typedef long long ll;

const int mod = 1e6 + 7;

struct hashtable { //哈希表
    int mp[1000700], hsh[1000700];

    inline int find(int x) {
        int t = x % mod;
        while (mp[t] != x && mp[t] != -1) { t = t + 107; if (t >= mod) t -= mod; }
        return t;
    }

    inline void insert(int x, int i) { int f = find(x); mp[f] = x; hsh[f] = i; }

    inline bool isin(int x) { int f = find(x); return mp[f] == x; }

    inline int IAKIOI(int x) { int f = find(x); return hsh[f]; }

    inline void clear() {
        memset(hsh, -1, sizeof hsh); memset(mp, -1, sizeof mp);
    }
}ht;

int main() {
    int b, p, n, m; scanf("%d%d%d", &p, &b, &n);
    ht.clear(); if (n == 1) return puts("0") & 0;
    m = ceil(sqrt((double)p)) + 1; int s = 1;
    for (int i = 1; i <= m; ++i, s = (1LL * s * b) % p, n = (1LL * n * b) % p) ht.insert(n, i); //插入哈希表
    b = s;
    for (int i = 1; i <= m; ++i, b = (1LL * b * s) % p)
        if (ht.isin(b)) return printf("%d\n", i * m - ht.IAKIOI(b) + 1) & 0;
    return puts("no solution") & 0;
}
```