扩展BSGS

原理

求解 $$ a^x\equiv b\pmod p $$ 其中 a,p 不一定互质。

当 $a\perp p$ 时，在模 p 意义下 a 存在逆元，因此可以用 BSGS 算法求解。于是我们想办法让他们变得互质。

具体地，设 $d_1=\gcd(a,p)$，如果 $d_1\nmid b$，则原方程无解。否则我们把方程同时除以 d_1，得到 $$ \frac{a}{d_1}\cdot a^{x-1}\equiv\frac{b}{d_1}\pmod{\frac{p}{d_1}} $$ 如果 a 和 $\frac{p}{d_1}$ 仍不互质就再除，设 $d_2=\gcd(a,\frac{p}{d_1})$，如果 $d_2\nmid\frac{b}{d_1}$，则方程无解；否则同时除以 d_2 得到 $$ \frac{a^2}{d_1d_2}\cdot a^{x-2}\equiv\frac{b}{d_1d_2}\pmod{\frac{p}{d_1d_2}} $$ 同理，这样不停地判断下去。直到 $a\perp \frac{p}{d_1d_2\cdots d_k}$。

记 $D=\prod_{i=1}^k d_i$，于是方程就变成了这样 $$ \frac{a^k}{D}\cdot a^{x-k}\equiv\frac{b}{D}\pmod{\frac p D} $$ 由于 $a\perp \frac p D$，于是推出 $\frac{a^k}{D}\perp\frac p D$，这样 $\frac{a^k}{D}$ 就有逆元了，于是把它丢到方程右边，这就是一个普通的 BSGS 问题了，于是求解 $x-k$ 后再加上 k 就是原方程的解了。

注意，不排除解小于等于 k 的情况，所以在消因子之前做一下 $\Theta(k)$ 枚举，直接验证 $a^i\equiv b\pmod p$，这样就能避免这种情况。

例题

Luogu4195 模板 exBSGS

题意：给定 a,p,b，求满足 $a^x\equiv b\pmod p$ 的最小自然数 x。

题解：模板题。

代码：``qwq`` 对应原理中的 d_i，``qaq`` 对应原理中的 $\frac{a^k}{D}$。

```
#include<bits/stdc++.h>
using namespace std;
typedef long long ll;
unordered_map<ll,int>H;
int N,M,P,ans;// N^x = M (mod P)
ll gcd(ll a,ll b){
    return !b?a:gcd(b,a%b);
}
ll expow(ll a,ll b,ll mod){
    ll ret=1;
    for(;b;a=a*a%mod,b>>=1)
        if(b&1) ret=ret*a%mod;
    return ret%mod;
```

```
}
ll exgcd(ll &x,ll &y,ll a,ll b){
    if(!b){x=1,y=0;return a;}
    ll g=exgcd(y,x,b,a%b);y-=x*(a/b);return g;
}
ll BSGS(ll a,ll b,ll mod,ll qaq){
    H.clear();
    ll Q,p=ceil(sqrt(mod)),x,y;
    exgcd(x,y,qaq,mod);
    b=(b*x%mod+mod)%mod;
    Q=expow(a,p,mod);
    exgcd(x,y,Q,mod);
    Q=(x%mod+mod)%mod;
    for(ll i=1,j=0;j<=p;j++,i=i*a%mod)
        if(!H.count(i)) H[i]=j;
    for(ll i=b,j=0;j<=p;j++,i=i*Q%mod)
        if(H[i]) return j*p+H[i];
    return -1;
}
ll exBSGS(){
    ll qaq=1;
    ll k=0,qwq=1;
    if(M==1) return 0;
    while((qwq=gcd(N,P))>1){
        if(M%qwq) return -1;
        k++,M/=qwq,P/=qwq,qaq=qaq*(N/qwq)%P;
        if(qaq==M) return k;
    }
    return (qwq=BSGS(N,M,P,qaq))==-1?-1:qwq+k;
}
int main(){
    while(scanf("%d",&N)){// N^x = M (mod P)
        scanf("%d %d",&P,&M);
        if(!N&&!M&&!P) return 0;
        N%=P,M%=P,ans=exBSGS();
        if(ans<0) puts("No Solution");
        else printf("%d\n",ans);
    }
    return 0;
}
```