a^x=b mod p model bsgs

$a^x = b(modp)$. 这样的x称为离散对数, 可以写为$log_a(b)(modp)$

设$x = k * n + i(n$为某常正整数$)$, 则原方程$-> (a^n)^k = b * (a^(- 1))^i$

将$(b * a^{-1})^i, i), i = 0, 1, \ldots, n - 1$存入表$(table, c + +$中可以用$unordered_map)$中,

然后枚举k, 在表中查找$(a^n)^k$即可, 复杂度$O(n + p/n)$, 取$n = \sqrt{p}$, 则$O(\sqrt{p})$.

```
#define ll long long
ll bsgs(ll a,ll b,ll p){
    static unordered_map<ll,ll> tab;
    tab.clear();
    ll u=(ll)sqrt(p)+1;
    ll now=1,step;
    for(int i=0;i<u-1;i++){
        ll tmp=b*inv(now,p)%p;
        if(!tab.count(tmp))
            tab[tmp]=i;
        (now*=a)%=p;
    }
    step=now;
    now=1;
    for(ll i=0;i<p;i+=u){
        if(tab.count(now))
            return i+tab[now];
        (now*=step)%=p;
    }
    return -1;
}

```