二次剩余模板

给定 n 和 p 求解关于 x 的方程 $x^2\equiv n\pmod{p}$

例题

P5491 【模板】二次剩余

```
#include<bits/stdc++.h>
using namespace std;
typedef long long ll;
int t;
ll n,p;
ll w;
struct num{
    ll x,y;
};
num mul(num a,num b,ll p){
    num ans={0,0};
    ans.x=((a.x*b.x%p+a.y*b.y%p*w%p)%p+p)%p;
    ans.y=((a.x*b.y%p+a.y*b.x%p)%p+p)%p;
    return ans;
}
ll binpow_real(ll a,ll b,ll p){//实部快速幂
    ll ans=1;
    while(b){
        if(b&1) ans=ans*a%p;
        a=a*a%p;
        b>>=1;
    }
    return ans;
}
ll binpow_imag(num a,ll b,ll p){//虚部快速幂
    num ans={1,0};
    while(b){
        if(b&1) ans=mul(ans,a,p);
        a=mul(a,a,p);
        b>>=1;
    }
    return ans.x%p;
}
ll cipolla(ll n,ll p){
    n%=p;
    if(p==2) return n;
    if(binpow_real(n,(p-1)/2,p)==p-1) return -1;
    ll a;
    while(1){
        a=rand()%p;
```

```
        w=((a*a%p-n)%p+p)%p;
        if(binpow_real(w,(p-1)/2,p)==p-1) break;
    }
    num x={a,1};
    return binpow_imag(x,(p+1)/2,p);
}

int main(){
    srand(time(0));
    scanf("%d",&t);
    while(t--){
        scanf("%lld %lld",&n,&p);
        if(!n){
            printf("0\n");continue;
        }
        ll ans1=cipolla(n,p),ans2;
        if(ans1==-1) printf("Hola!\n");
        else{
            ans2=p-ans1;
            if(ans1>ans2) swap(ans1,ans2);
            if(ans1==ans2) printf("%lld\n",ans1);
            else printf("%lld %lld\n",ans1,ans2);
        }
    }
    return 0;
}
```