乘法逆元

[**原题地址**](https://www.luogu.com.cn/problem/P3811)
[**参 考**](https://www.luogu.com.cn/problem/solution/P3811)
`![在这里插入图片描述](https://img-blog.csdnimg.cn/4fdf7492256440d7ac71f5dbefece5e2.png?x-oss-process=image/watermark,type_d3F5LXplbmhlaQ,shadow_50,text_Q1NETiBA6L-95409,size_20,color_FFFFFF,t_70,g_se,x_16)`

拓展欧几里得(单个查找，p可以为合数)
```cpp
void Exgcd(ll a, ll b, ll &x, ll &y) {
    if (!b) x = 1, y = 0;
    else Exgcd(b, a % b, y, x), y -= a / b * x;
}
int main() {
    ll x, y;
    Exgcd (a, p, x, y);
    x = (x % p + p) % p;
    printf ("%d\n", x); //x是a在mod p下的逆元
}
```

快速幂(单个查找，p必须为质数)
```cpp
ll quick_pow(ll a,ll b,ll mod){//a^b%mod
    ll ans=1,base=a;
    while(b){
        if(b&1) ans*=base,ans%=mod;
        base*=base,base%=mod;
        b>>=1;
    }
    return ans;
}
int main() {
    ll x = quick_pow(a, p - 2, p); //x为a在mod p意义下的逆元
}
```

线性递推(连续查找，p必须为质数)
```cpp
inv[1] = 1;
for(int i = 1; i < p; ++ i)
    inv[i] = (p - p / i) * inv[p % i] % p;
```

`AC` 代码
```cpp
//#pragma GCC optimize(2)
//std::ios::sync_with_stdio(0)
//clock_t st=clock();
#include<bits/stdc++.h>
#define abss(x) ((x)>(0)?(x):(-1)*(x))
```

```
#define maxs(a,b) ((a)>(b)?(a):(b))
#define mins(a,b) ((a)<(b)?(a):(b))
#define FOR(i,a,b) for(int i=(a);i<=(b);++i)
#define ROF(i,a,b) for(int i=(a);i>=(b);--i)
#define mem(a) memset(a,0,sizeof(a))
const int INF (1<<30);
const int inf (-1<<30);
using namespace std;

const int maxn=3e6+7;
int inv[maxn];

int main(){
    int n,p;
    cin>>n>>p;
    inv[1]=1;
    cout<<"1\n";
    FOR(i,2,n){
        inv[i]=(long long)(p-p/i)*inv[p%i]%p;
        printf("%d\n",inv[i]);
    }
}
```

矩阵快速幂

[P3390 【模板】矩阵快速幂](https://www.luogu.com.cn/problem/P3390)

```cpp
#include<bits/stdc++.h>
#define FOR(i,a,b) for(int i=(a);i<=(b);++i)
#define ll long long
#define mem(a) memset(a,0,sizeof(a))
#define scan(a) scanf("%lld",&(a))
#define print(a) printf("%lld",a)
using namespace std;

const int maxn=105;
const int mod=1e9+7;
ll n,k;

struct matx{
    ll a[maxn][maxn];
    matx(){
        mem(a);
    }
    void unit(){
        FOR(i,1,n)
            a[i][i]=1;
    }
    matx operator *(const matx &b){
        matx c;
        FOR(k,1,n)
            FOR(i,1,n)
```

```
                FOR(j,1,n)
                    c.a[i][j]=(c.a[i][j]+a[i][k]*b.a[k][j]%mod)%mod;
        return c;
    }
    matx operator *=(const matx &b){
        *this=(*this)*b;
        return *this;
    }
};

matx pow(matx Ma,ll k){
    matx Mans;
    Mans.unit();
    do{
        if(k&1) Mans*=Ma;
        Ma*=Ma;
        k>>=1;
    }while(k);
    return Mans;
}

int main(){
    matx Ma;
    cin>>n>>k;
    FOR(i,1,n)
        FOR(j,1,n)
            scan(Ma.a[i][j]);
    matx Mans=pow(Ma,k);
    FOR(i,1,n){
        FOR(j,1,n)
            print(Mans.a[i][j]),putchar(' ');
        putchar('\n');
    }
    return 0;
}
```

快速幂 排列组合

快速幂

不带模数

```cpp
ll qpow(ll a,ll b){//a^b
    ll ans=1,base=a;
    while(b){
        if(b&1) ans*=base;
        base*=base;
        b>>=1;
    }
    return ans;
}
```

带模数，循环式

```cpp
ll qpow(ll a,ll b,ll p){//a^b%p
    ll ans=1,base=a;
    while(b){
        if(b&1) ans*=base,ans%=p;
        base*=base,base%=p;
        b>>=1;
    }
    return ans;
}
```

带模数，递归式

```cpp
ll qpow(ll a,ll b,ll p){
    if(b==1) return a;
    ll t=qpow(a,b/2,p);
    t=t*t%p;
    if(b&1) t=t*a%p;
    return t;
}
```

排列组合

需要用到费马小定理

```cpp
ll C(ll n,ll m,ll p){
    if(n<m) return 0;
    if(m>n-m) m=n-m;
    ll a=1,b=1;
    FOR(i,0,m-1){
        a=(a*(n-i))%p;
        b=(b*(i+1))%p;
    }
    return a*qpow(b,p-2,p)%p;
}
```

卢卡斯定理

[P3807 【模板】卢卡斯定理/Lucas 定理](https://www.luogu.com.cn/problem/P3807)

$Lucas$ 定理：对于质数 p，有
$$ \binom{n}{m}\bmod p = \binom{\left\lfloor n/p \right\rfloor}{\left\lfloor m/p\right\rfloor}\cdot\binom{n\bmod p}{m\bmod p}\bmod p $$
等价于
$$ C(n,m)\%p=C(n/p,m/p)*C(n\%p,m\%p)\%p $$

边界条件：当 $m=0$ 的时候，返回 1 。

`C(n,m)%p = C(n/p,m/p) * C(n%p,m%p)%p`

$Code:$
```cpp
#include<bits/stdc++.h>
#define FOR(i,a,b) for(int i=(a);i<=(b);++i)
typedef long long ll;
using namespace std;

ll qpow(ll a,ll b,ll p){//快速幂
    ll ans=1,base=a;
    while(b){
        if(b&1) ans*=base,ans%=p;
        base*=base,base%=p;
        b>>=1;
    }
    return ans;
}

ll C(ll n,ll m,ll p){//组合数
    if(n<m) return 0;
    if(m>n-m) m=n-m;
    ll a=1,b=1;
    FOR(i,0,m-1){
        a=(a*(n-i))%p;
        b=(b*(i+1))%p;
    }
    return a*qpow(b,p-2,p)%p;//费马小定理
}

ll Lucas(ll n,ll m,ll p){//卢卡斯定理
    if(m==0) return 1;
    return Lucas(n/p,m/p,p)*C(n%p,m%p,p)%p;
}

int main(){
    int T;cin>>T;
    while(T--){
        ll n,m,p;
        cin>>n>>m>>p;
        cout<<Lucas(n+m,m,p)%p<<endl;
    }
    return 0;
}
```

裴蜀定理

[**原题地址-Luogu**](https://www.luogu.com.cn/problem/P4549)
![在这里插入图片描述](https://img-blog.csdnimg.cn/79cfa2cfc3ae4e20b41e4edb09e6b6ea.png?x-oss-

process=image/watermark,type_d3F5LXplbmhlaQ,shadow_50,text_Q1NETiBA6L-95409,size_20,color_FFFFFF,t_70,g_se,x_16)

裴蜀定理

对于整数`a,b`和正整数`x,y`，`ax+by=c`成立的**充要**条件是`gcd(a,b)%c=0`.

推论：`a,b`互质的**充要**条件是存在整数`x,y`，使`ax+by=1`.

拓展：对于`n`个整数`a1,a2,......,an`，`a1*x1+a2*x2+......+an*xn=S`成立的**充要**条件是`gcd(a1,a2,......an)%S=0`.

`AC` 代码

```cpp
//#pragma GCC optimize(2)
//std::ios::sync_with_stdio(0)
//clock_t st=clock();
#include<bits/stdc++.h>
#define abss(x) ((x)>(0)?(x):(-1)*(x))
#define maxs(a,b) ((a)>(b)?(a):(b))
#define mins(a,b) ((a)<(b)?(a):(b))
#define FOR(i,a,b) for(int i=(a);i<=(b);++i)
#define ROF(i,a,b) for(int i=(a);i>=(b);--i)
#define mem(a) memset(a,0,sizeof(a))
const int INF (1<<30);
const int inf (-1<<30);
using namespace std;

int main(){
    int n;
    cin>>n;
    int ans=0,t;
    FOR(i,1,n){
        scanf("%d",&t);
        t=abss(t);
        ans=__gcd(ans,t);
    }
    cout<<ans;
}
```

拓展欧几里得(exgcd)

```cpp
void exgcd(int &x,int &y,int a,int b){
    //使用时exgcd(a,b,a,b)即可，无需全局变量，运行后a、b为一组解
    if(!b){
        x=1,y=0;
        return;
    }
    exgcd(x,y,b,a%b);
    int t;
    t=x,x=y,y=t-a/b*y;
```

}
```

**压行版本**
```cpp
void exgcd(int &x,int &y,int a,int b) {
    if(!b) x=1,y=0;
    else exgcd(y,x,b,a%b),y-=a/b*x;
}
```

线性筛素数

```cpp
//#pragma GCC optimize(2)
//clock_t st=clock();
#include<bits/stdc++.h>
#define abss(x) ((x)>(0)?(x):(-1)*(x))
#define maxs(a,b) ((a)>(b)?(a):(b))
#define mins(a,b) ((a)<(b)?(a):(b))
#define FOR(i,a,b) for(int i=(a);i<=(b);++i)
#define ROF(i,a,b) for(int i=(a);i>=(b);--i)
#define mem(a) memset(a,0,sizeof(a))
const int INF (1<<30);
const int inf (-1<<30);
using namespace std;

const int maxn=1e8+7,maxm=6e6;
bool isPrime[maxn];
int Prime[maxm],cnt=0;

void GetPrime(int n){//数据范围[1,n]
    memset(isPrime,1,sizeof(isPrime));
    isPrime[1]=0;

    FOR(i,2,n){
        if(isPrime[i])//没被筛掉
            Prime[++cnt]=i;//i成为下一个素数

        for(int j=1;j<=cnt and i*Prime[j]<=n;j++){
            isPrime[i*Prime[j]]=0;
            if(i%Prime[j]==0) break;
        }
    }
}//素数被标记为1，合数被标记为0

int main(){
    int n,q,k;
    cin>>n>>q;
    GetPrime(n);
    while(q--){
        scanf("%d",&k);
        printf("%d\n",Prime[k]);
    }

```
    return 0;
}
```