欧拉函数的定义

> $1 \sim N$ 中与 N 互质的数的个数被称为欧拉函数，记为 $\phi(N)$。
> 若在算数基本定理中，$N = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$，则：
> $\phi(N) = N \times \frac{p_1-1}{p_1} \times \frac{p_2-1}{p_2} \times \ldots \times \frac{p_m-1}{p_m}$

欧拉函数是 积性函数。

即对任意满足 $\gcd(a,b)=1$ 的整数 a,b，有 $\varphi(ab)=\varphi(a)\varphi(b)$。

特别地，当 n 是奇数时 $\varphi(2n)=\varphi(n)$。

欧拉定理

$a^{\varphi(m)} \equiv 1 \pmod{m}$。

```
int main()//求n的欧拉函数个数，如果n为质数，其欧拉函数为n-1
{
    int n;
    cin>>n;
    while(n--)
    {
        int a,res;
        cin>>a;
        res = a;
        for(int i=2;i<=a/i;i++)
        {
            if(a%i==0)
            {
                while(a%i==0)
                    a/=i;
                res = res / i*(i-1);
            }
        }
        if(a>1) res = res /a*(a-1);
        cout<<res<<endl;
```

```
    }
    return 0;
}
```

当n为质数时，可以用快速幂求逆元：

a / b ≡ a * x (mod n)

两边同乘b可得 a ≡ a *b* x (mod n)

即 1 ≡ b * x (mod n)

同 b * x ≡ 1 (mod n)

由费马小定理可知，当n为质数时

b ^ (n - 1) ≡ 1 (mod n) （因为n为质数，n的欧拉函数为n-1）

拆一个b出来可得 b * b ^ (n - 2) ≡ 1 (mod n)

故当n为质数时，b的乘法逆元 x = b ^ (n - 2)

当n不是质数时，可以用扩展欧几里得算法求逆元：

a有逆元的充要条件是a与p互质，所以gcd(a, p) = 1

假设a的逆元为x，那么有a * x ≡ 1 (mod p)

等价：ax + py = 1

exgcd(a, p, x, y)

> 设 a, b 是不全为零的整数，对任意整数 x, y，满足 $\gcd(a,b) \mid ax+by$，且存在整数 x, y, 使得 $ax+by=\gcd(a,b)$.

```
typedef long long LL;
int exgcd(int a, int b, int &x, int &y)//指针引用
{
    if (!b) {
        x = 1, y = 0;
        return a;
    }
    int d = exgcd(b, a % b, y, x);
    y -= a / b * x;
    return d;
}
```

```
int main()
{
    int a, p, x, y;
    cin >>  a >> p;  // if (a < p) swap(a, p);
    int d = exgcd(a, p, x, y);
    if (d == 1) cout << ((LL)x + p) % p << endl;//保证x是正数 d为最大公因数
    return 0;
}
```