对于gcd(a,n)=1的整数，满足a^r%n=1 的最小整数r

称为a模n的阶。

**a模n的阶**，记为ord(a,n)

a\*x%n==1,

则称任意正整数的x是a模n的逆元,一般是取最小的

性质：

* 设（a,n）=1 ，a模n的阶为r. 若正整数N使得a^N≡1(mod n ), 则 r∣N
* 设（a,n）=1, 则a模n的阶r整除ψ（n）.特别的，若n是素数p, 则a模p的阶整除p-1.（[费马小定理](https://baike.baidu.com/item/%E8%B4%B9%E9%A9%AC%E5%AE%9A%E7%90%86)）
* 设gcd（a,n）=1,如果 a 与 n 是互质的整数且n>0，那么ord(a,n)|φ(n)
* 设gcd（a,n）=1,正整数 a^i=a^j(mod n)，当且仅当 i=j mod ord(a,n)

# 原根：

如果 a 与 n 是互质的整数且n>0(gcd（a,n）=1)，那么当ord(a,n)==φ(n)时，

称a为模n的 一个原根，是a为模n的一个原根，是针对n来说的，n是素数就可以理解为ord(a,n)==n-1时，a是n的原根

* 所有的**素数**都有原根,不是所有的整数都有原根。
* 当正整数m有原根时，有φ(φ(m))个原根。
* 如果 a 与 n 是互质的整数且n>0(gcd（a,n）=1)，则如果a是模n的一个原根，那么整数a^1, a^2, … , a^φ(n)构成模n的**既约剩余系**。   
  既约剩余类，即简化剩余类，是指在每个模n的值与n互质的剩余类中，各取一数组成的集合。 这个定理说明了我们在简介中说道的关于原根的一个基本性质，即a^i两两互不相同。

## 原根求法：

**对于素数n的原根：** 设n=p  
求素数p的原根，即 求a 模 p的阶数为 φ(n) 的整数a，所以我们可以通过判断小于 φ(p) 的整数中是否存在整数 x 使得 a^x≡1(mod p) 。

根据阶定义，对于gcd(a,n)=1的整数，满足a^r%n=1 的最小整数r

称为a模n的阶。

检测的数只是 φ(p) 的质因子即可，φ(p)=p-1

对p-1分解质因数,质因数分别是p1 p2 p3 p4..pm

也就是从2枚举g,如果有一个g使得pow(g,(p-1)/pi,p) ==1，那就不是原根，否则就是原根，为什么有一个就不是原根，yi如果存在小于 φ(p)的x，说明φ(p)不是最小的，那a也不是原根。