## **威尔逊定理**

## **描述：**

如果整数p符合(p - 1)! ≡ -1 ( mod p )，则p是素数。但是由于阶乘增长非常快的，其结论对于实际操作意义不大。

通俗点，当且仅当p是素数，则(p-1)! + 1能被p整除。

## **证明：**

### **充分性证明：**

证明其逆反命题即可：如果p是合数，则p不符合(p - 1)! ≡ -1 (mod p)。

当p小于等于4的时候，明显成立。

当p大于4时，

　　如果p不是完全平方数，则p可以分解为ab，a, b ∈ {2, 3, ..., p - 1}，且a != b

　　　　则(p - 1)!必包含a, b，则(p - 1)! ≡ 0 (mod p)

　　如果p是完全平方数，则有p = k^2, 已知当k > 2时，有k, 2k ∈ {2, 3, ..., p -  1}，同上可得(p - 1)! ≡ 0 (mod p)

证毕。

### **必要性证明：**

对于偶质数2显然成立，下面讨论奇质数：

对于质数p，集合B = {1, 2, 3, ..., p - 1}中的每个元素都与p互质（即是其缩系）。

对于B的一个子集A = {2, 3, 4, ..., p - 2}，对每个a ∈ A，使C = {a, 2a, ..., (p - 1)a}，则对于任一个a，C也是p的一个缩系（即每个数对p不同余且不能整除）。

　　关于C是缩系的证明(其实是同余的一个性质）：

　　　　如果存在an, am同余，设n > m，则(an - am) ≡ 0 (mod p)，则a(n - m) ≡ 0 (mod p)，由于a(n - m)也属于C，不存在能整除的。

则对于任意a，在C中，必存在一个对应的ab，使得ab ≡ 1 (mod p)：

　　证明b不属于{1, p - 1, a}：

　　　　如果b = 1，则a ≡ a (mod p)，由于a 属于A，不成立。

　　　　如果b = p - 1，则(p - 1)a ≡ (p - a)(mod p)，当且仅当a = p - 1时成立，但a属于A，不成立。

　　　　如果b = a，若a\*a ≡ 1 (mod p)，则a\*a - 1 ≡ 0 (mod p)，即(a + 1)(a - 1) ≡ 0 (mod p)，当且仅当a = 1或p - 1时成立，不成立。

　　证明如果a不相同，则b也不相同：

　　　　如果对于a，存在b1, b2，使得ab1 ≡ ab2 (mod p)，则a(b1 - b2) ≡ 0 (mod p)，a(b1 - b2)属于C中某项，不存在能整除的。

由上可知，则对于a，存在b ∈ A，a != b，使得ab ≡ 1 (mod p)，则对于2\*3\*4\*...\*(p - 2)，由于：

2b ≡ 1 (mod p)，3b' ≡ 1(mod p)，...，则2\*3\*4\*...\*(p - 2) ≡ 1 (mod p)，

且1 ≡ 1 (mod p)，(p - 1) ≡ -1 (mod p)，则(p - 1)! ≡ -1 (mod p)，证毕。

# 缩系

简化剩余系也称既约剩余系、缩系，是数学术语。缩系的定义，如果一个模m的剩余类里面的数与m互素（显然，只需有一个与m互素，其余的均与M互素）就把他叫做一个与模m互素的剩余类，在与模m互素的全部剩余类中，各取一数所组成的集叫做模M的一组简化剩余系

简化剩余系，**别称**缩系

若整数A1,A2,[...](https://baike.baidu.com/item/..." \t "https://baike.baidu.com/item/%E7%BC%A9%E7%B3%BB/_blank),Am模n分别对应0,1,2,...,n-1中所有m个与n互素的自然数,则称集合{A1,A2,...,Am}为模n的一个缩系,

缩系性质:1、对于任意的与n互质的正整数k，若{A1,A2,...,Am}为模n的一个缩系,(k,n)=1,则{k\*A1,k\*A2,...,k\*Am}也为模n的一个缩系 .

2、(k\*A1)...(k\*Am)≡A1\*A2...Am(modn)

数论四大定理

https://baike.baidu.com/item/%E6%95%B0%E8%AE%BA%E5%9B%9B%E5%A4%A7%E5%AE%9A%E7%90%86/4751986?fr=aladdin