威尔逊定理

在初等数论中，威尔逊定理给出了判定一个自然数是否为素数的**充分必要条件。**

当且仅当 p 为素数时，

$$(p-1)! \equiv -1(mod\ p)$$

简单点说就是，若 p 为质数，则 p能被 (p-1)!+1 整除。

通过威尔逊定理我们可以构造一下质数分布的函数曲线（结合sin函数的性质）

$$f(n) = sin(\pi * ((n-1)! + 1)/n)$$

当函数值为0时，就可以得出一个质数（是不是很鸡肋）。

由于充分必要条件我们当然也可以用这个来判断质数，不过不好用就对了。

由于阶乘是呈爆炸增长的，其结论对于实际使用不太多。

证明

首先，可以明确

$$(p-1) \equiv -1(mod\ p)$$

根据同余式的性质，我们只需要证明

$$(p-2)! \equiv 1(mod\ p)$$

这个式子突然就有点熟悉了，看下逆元的定义

$$a \cdot a^{-1} \equiv 1(mod\ p)$$

我们考虑其实就是对于 1,2,3,...,p−2 去找模 p 意义下的逆元，**而1的逆元就是1，不需要考虑。**

然后根据

$$x^2 \equiv 1(mod\ p)$$

可以解得

$$x_1 = 1, x_2 = p-1$$

意思就是只有1，p−1 在模 p 意义下的逆元是自己，然而这两个数已经被我们安排了，然后逆元还有**唯一性**与**互反性。**

那么这些数自然是一一对应。

所以

$$(p-2)! \equiv 1(mod\ p)$$

成立。

题目

HDU2973

HDU5391