```
1. 设p是素数，计算(p-1)! (mod p），找出规律，写成定理，并给出证明。
2. 设n是合数，计算(n-1)! (mod n），找出规律，写成定理，并给出证明。提示：可以编程找规律。
```

1.设p为素数，定理为：当p既为素数又为整数时，必有

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

证明:

(p-1)!  = (p-1)✕(p-2)✕...1

因为p是素数，p与小于它的正整数都是互素

当p=2时， (2-1)!  (mod 2)=1 (mod 2) 显然成立

对于2以上的奇素数，有 a∈（1，p-1)，必定存在乘法逆元a' ∈(1,p-1)，使得

$$aa'\equiv1(mod\quad p)$$

且a != a' ,两两配对，有

$$2\cdot3\cdots(p-2)\equiv1(mod\quad p)$$

又有p-1与p互素，而且1和p-1的逆是它本身

故

$$(p-1)!=1\cdot2\cdot3\cdots(p-2)\cdot(p-1)\equiv1\cdot(p-1)(mod\quad p)$$

2.设n为合数，定理为：当n为整数时，除4外，必有

$$(n-1)!(mod\quad n)=0$$

特例：n=4时，等于2

```
代码：
int mos(int n)
{
    int sum = 1;
    for (int i = 1; i <n; i++)
        sum *= i;
    printf("%d\n", sum);
    sum = (sum % n);
    return sum;
}
```

证明:

例外：n=4时， (4-1)! (mod 4) = 2

n≥4时，(n-1)! = 1·2·3⋯(n-2)·(n-1)，(n-1)!必定包括了合数n的所有积因子，这些因子相乘必定有一组p,q,使得

$$n=p\cdot q$$

成立

必有p≠q，且p , q均大于1 ， 使得n能被这两个数的乘积整除，使得整个(n-1)的阶乘mod n 的余数为0