Lucas 定理

结论

$$C_n^m \equiv C_{n/p}^{m/p} \times C_{n \bmod p}^{m \bmod p} (mod\, p)$$

[例题]

Code

```
#include<iostream>
#include<cstring>
#include<algorithm>
#include<cstdio>
#define int long long

using namespace std;

int n,m,p,t,fac[105000];

int inv(int b,int q)//求逆元，费马小定理
{
    int ans = 1;
    for(        ;q;q >>= 1,b = b*b%p)
        {
        if( q%2 != 0 )
                        ans = ans*b%p;
    }
    ans %= p;
    return ans;
}
int C(int n,int m)
{
    if( m > n )
            return 0;
```

```
    return fac[n]*inv((fac[m]*fac[n-m])%p,p-2)%p;
}
int Lucas(int n,int m)
{
    if( m == 0 )
            return 1;
    return (Lucas(n/p,m/p)*C(n%p,m%p))%p;

}
signed main()
{
    cin >> t;
    for(int i = 1;i <= t; i++)
        {
        cin >> n >> m >> p;
        fac[0] = 1;;
        for(int i = 1;i <= p; i++)//预处理阶乘
                {
                        fac[i] = fac[i-1]*i;
                        fac[i] %= p;
                }
        printf("%lld\n",Lucas(n+m,m));
    }
    return 0;
}
```

证明

引理一

$$C_p^x \equiv 0 \ (mod \ p), 0 < x < p$$

证明:

$$C_p^x \equiv \frac{p!}{x! \cdot (p-x)!} \equiv \frac{p \cdot (p-1)!}{x \cdot (x-1)! \cdot (p-x)!} \equiv p \cdot inv(x) \cdot C_{p-1}^{x-1} \equiv 0 \ (mod \ p)$$

引理二

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

证明:

> 二项式定理:
>
> $$(a+b)^n=\sum_{r=0}^{n}C_n^r a^{n-r}b^r$$
>
> 其中，等号右侧叫做等号左侧的二次展开式。

先进行二项式展开

$$(1+x)^p=\sum_{i=0}^{p}C(p,i)x^i$$

根据引理一

$$\sum_{i=0}^{p}C(p,i)x^i \equiv C(p,0)x^0+\cdots+C(p,p)x^p \equiv 1+x^p\ (mod\ p)$$

证明

$$\text{假设} n=q_np+r_n, m=q_mp+r_m$$

$$(1+x)^n \equiv (1+x)^{q_np+r_n} \equiv (1+x)^{q_np}\cdot(1+x)^{r_n} \equiv [(1+x)^p]^{q_n}\cdot(1+x)^{r_n}$$

$$\equiv (1+x^p)^{q_n}\cdot(1+x)^{r_n} \equiv \sum_{i=0}^{q_n}C(q_n,i)x^{p\cdot i}\cdot\sum_{j=0}^{r_n}C(r_n,j)x_j\ (mod\ p)$$

又因为

$$(1+x)^n=\sum_{i=0}^{n}C(n,i)x^i$$

所以

$$\sum_{i=0}^{n}C(n,i)x^i \equiv \sum_{i=0}^{q_n}C(q_n,i)x^{p\cdot i}\cdot\sum_{j=0}^{r_n}C(r_n,j)x_j\ (mod\ p)$$

取两边 x^m 次项的系数，因为 $m = q_m p + r_m$，所以对于等式右边最多只有一种情况满足

$$C_n^m \equiv C_{n/p}^{m/p} \times C_{n\,mod\,p}^{m\,mod\,p} (mod\,p)$$