$$\boxed{a \equiv b \pmod{p}}$$

$$a \bmod p = b \bmod p$$

$$1 \equiv 6 \pmod{5}$$ %

$$-4 \equiv 1$$

$$-4 \% 5 = -4$$

$$(-4 + p) \% p$$

0, 1, 2, 3, 4

$$\underbrace{3 \times 4 \times 6 \times 7 \times 2 \times 3}_{} \bmod 5$$

边乘边模 ✓

$3^{10000} \bmod 5$

$a=3$

$a*=4$

$a\%=5$

$a*=6$

$a\%=5$

---

int 不会溢出

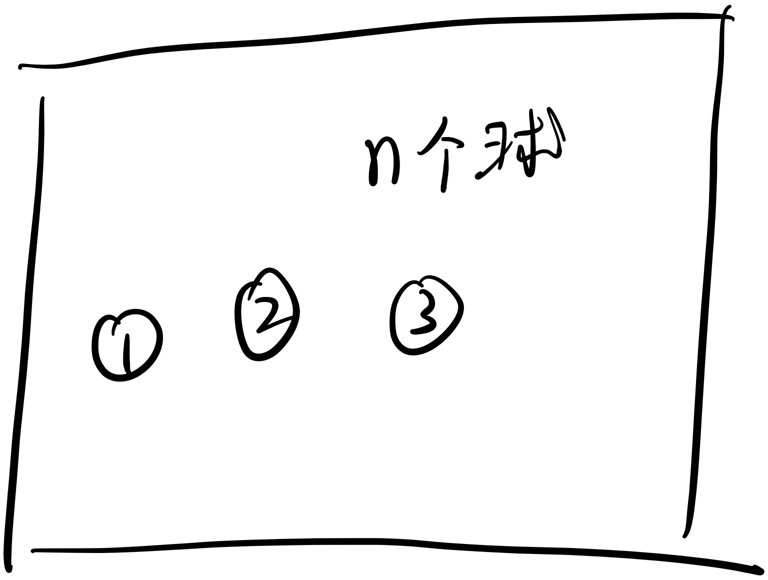
边除边模？

$(128 \div 6) \times 81 \quad \bmod 5$

$\frac{128}{6} \times 81 \rightarrow \text{int} \quad \bmod 5$

$\left(\left\lfloor \frac{128}{6} \right\rfloor \bmod 5\right) \times 81 \quad \bmod 5$

验证：上述结果不对.



取 m 个球

有多少种可能

$\binom{n}{m}$ —— C_n^m

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$$

1 2

2 1

1: 1

2: 2

1 2 3

1 3 2

2 1 3

3: 6

2 3 1
3 1 2
3 2 1

$P(n) = n!$

$P(1)=1$
$P(2)=2$
$P(3)=6$

“归纳法”.

假设已知 $P(n-1)=(n-1)!$

$\Downarrow$

$P(n)=n!$

① ② ... ⓝ

ⓚ $\boxed{n-1\text{个}}$

$P(n)=n\cdot P(n-1) = n\cdot(n-1)! = n!$

"全排列数"：$P(n) = n!$

"排列数"：A_n^m：

在 ① ② …… ⓝ 球里

选 m 个 排成一排，有几种

可能的 序列

① ② ③ ④ 2.

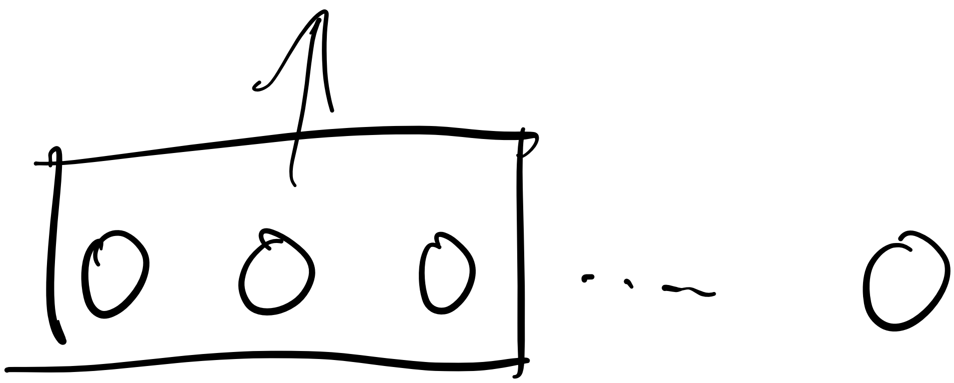
12	23	34
21	32	43
13	24	
31	42	
14		
41		

12

$A_4^2 = 12$

$A_n^n = P(n) = n!$ $\quad m \le n$

A_n^m



n个球

排一排：n! 种序列

截取前 m 个

$n=4$
$m=2$

1 2 3 4

$\boxed{1\ 2}$ 4 3 $\quad (n-2)!$

n

1 2

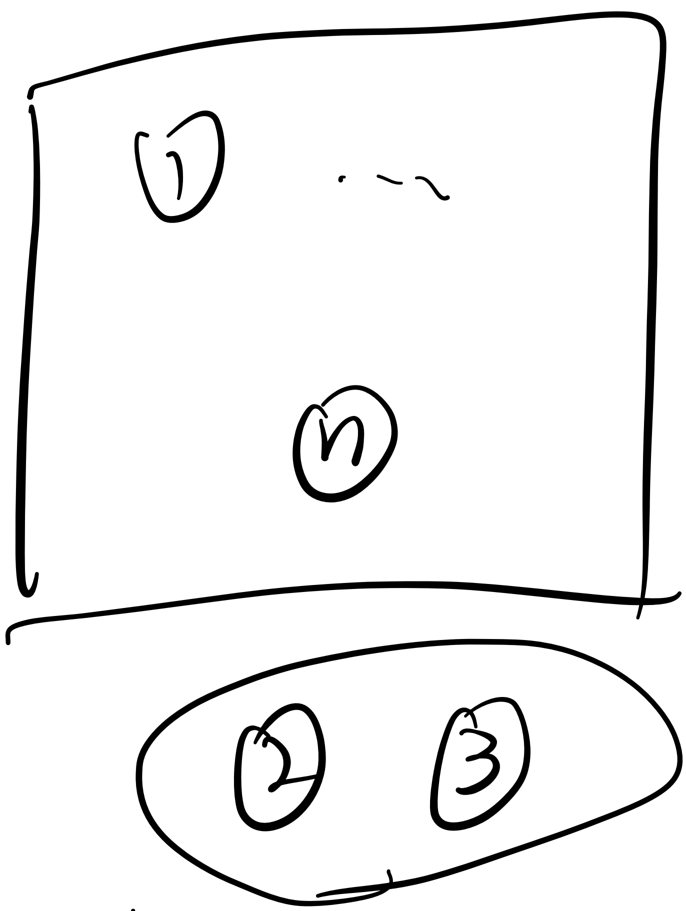
A A $\quad (n-m)!$

m个

被统计了 $(n-m)!$ 次

$$\boxed{A_n^m = \frac{n!}{(n-m)!}}$$

$$\binom{n}{m} = \frac{A_n^m}{m!} = \frac{n!}{m!(n-m)!}$$



杨辉三角

n \ m	0	1	2	3	4	
0	1					1
1	1	1				2
2	1	2	1			4
3	1	3	3	1		8
4	1	4	[illegible]	4	1	16

$\binom{n}{0} = 1$

$\binom{2}{1}$

$C(\;) \quad 4 \;|\; 1 \quad 4 \quad 6 \quad 4 \quad 1$

$$\binom{n}{m} = \binom{n}{n-m} \qquad \binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

$$\binom{n-1}{m} + \binom{n-1}{m-1} = \frac{(n-1)!}{m!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)!}$$

$$= \frac{(n-m)(n-1)!}{m!\,(n-m)!} + \frac{m(n-1)!}{m!(n-m)!}$$

$$= \frac{(n-\cancel{m}+\cancel{m})(n-1)!}{m!\,(n-m)!}$$

$$= \frac{n!}{m!(n-m)!} = \binom{n}{m}$$

```
C[ ][ ]
for i = 0 to n
    C[i][0] = 1
    for j = 1 to i
        C[i][j] = (C[i-1][j]
```

$+ C[i-1][j-1])$

$O(n^2)$ $\% p$

取模 P

$n = 32$

$\binom{n}{n/2}$: $\dfrac{32!}{16! \times 16!}$ 大大大

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$$(x+y)^n = \boxed{1}\, x^n + \boxed{n}\, x^{n-1} y + \cdots$$

$$+ \boxed{}\, x y^{n-1} + \boxed{}\, y^n$$

$$(x+y)^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = (x+y)(x^2+2xy+y^2)$$

$$= x^3 + 3x^2y + 3xy^2 + y^3$$

$(x+y)\cdot(x+y)\cdots\cdots(x+y)$ (n项)

n-1 个括号中选 x

1 个括号中选 y

n 种系.

$\binom{n}{k}x^k y^{n-k}$

k个 () 选x

~~n-k 个 () 选y~~

$\binom{n}{k}$

$= \sum^{n} \binom{n}{k} x^k y^{n-k}$

$$\boxed{(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{k} y^{n-k}}$$

二项式定理.

$x=y=1$ 代入

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Ex. 已知 $k<n$, $m \geq 1$

求 $\binom{n}{k} + \binom{n+1}{k} + \cdots + \binom{n+m}{k}$

结果是两个组合数相减.

HINT: 用杨辉三角.

输入 n, m, p. 求 $\binom{n}{m} \bmod p$.

$O(n^2)$: ✓

$< O(n \log n)$

$n!$ $O(n)$

$fact[i] = i * fact[i-1]$ % p

$$\binom{n}{m} = \frac{fact[n]}{fact[m] * fact[n-m]}$$ 不行

"乘法逆元"

a 模 p 的乘法逆元是 a^{-1}

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

2 模 5 的乘法逆元是 3

$$2 \times 3 \equiv 1 \pmod 5$$

当 p 是质数时，除 0 以外，

$\boxed{\text{每个数都有乘法逆元}}$

求逆元：

Theorem (Fermat)

If p is prime, $a \neq 0$.

Then: $a^{p-2} \equiv a^{-1} \pmod p$

$2^{-1} = 4$

$2^5 \equiv$

$= 32 \% 7$

$= 4$

mod 7

$2 \times 4 \mod 7 = 1$

$2^5 \equiv 4 \mod 7$

$2^{-1} \equiv 4$

$2^{-1} \equiv 2^5 \mod 7$

$3^{-1} \equiv 3^5 \mod 7$

$p = 10^9 + 7$ a^{p-2}

$p = 998244353$ (NTT)

Algorithm. 快速幂 求 $a^n \% p$

```
quick_power(a, n)
    b = quick_power(a, n/2)
    if (n%2==0)
        return (long long) b*b%p
    else
```

else

return (long long) b*b%p *a%p

$O(\log n)$.

```
inv(a)
    return quick_power(a, p-2)
```

$$\binom{n}{m} = fact[n] * inv(fact[m])\%p * inv(fact[n-m])\%p$$

$$\frac{n!}{m!(n-m)!}$$

取模

除 a ⟹ 乘 a^{-1}

$O(n)$ 预处理 fact， $O(\log n)$ 求 $\binom{n}{m}$

$O(n)$ 预处理 $ifact[n]$

$= inv(fact[n])$

$O(1)$: $\binom{n}{m} = fact[n] \times ifact[m] \times ifact[n-m]$

$O(1)$

1) $ifact[n] = inv(fact[n])$

$= \frac{1}{n!}$ $\quad \frac{1}{(n-1)!} = \frac{1}{n!} \times n$

2) for $i = n$ to 1

$ifact[i-1] = ifact[i] * i \% p$

$O(\log p) + \underbrace{O(n)} = O(n)$.