组合数取模问题

摘要: 如何快速求解$\binom{m}{n} \mod p$?

目录

用递推式递推

$$\binom{m}{n} = \binom{m}{n-1} + \binom{m-1}{n-1} \mod p$$

渐进时间复杂度为$O(n^2)$.能处理大约$n \le 10000$的情况.

通过逆元求取

当所求的 n 过大时就不能使用递推式递推了.根据定义式

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

可是对于模运算，$n/m \not\equiv (n/m) \mod p$.因此直接求出阶乘然后算出组合数是不对的.但是可以通过**逆元将**除法运算转化为乘法，这就涉及到数论中一个重要的概念：**逆元.**

对于正整数 a 和 p，如果有 $ax \equiv 1 \mod p$，**那么把这个同余方程中 x 的最小正整数解叫做 a 模 p 的逆元，记为** a^{-1}.

假设 b 为 a 模 p 的逆元，那么满足 $aa^{-1} \equiv 1 \mod p \Rightarrow a^{-1} \equiv \frac{1}{a} \mod p$，那么 $\frac{a}{b} \equiv a \cdot \frac{1}{b} \equiv a \cdot b^{-1} \mod p$.实际上可以将 $\frac{n!}{m!(n-m)!} \equiv n!(m!(n-m)!)^{-1} \mod p$.

使用定义式通过求逆元求取组合数的方法也具有一定的局限性，它仅仅适用于 $n \le p$ 的情况．一旦 $n > p$，就不再适用.

如何求取逆元

常用的快速求取逆元的方式有两种:

扩展欧几里得算法

求取逆元实际上是求取使得 $ax \equiv 1 \mod p$ 成立的最小正整数 x.可以直接通过扩展欧几里得求得.

费马小定理

费马小定理: $a^{p-1} \equiv 1 \mod p$，**其中 p 为质数.**

根据费马小定理，可以得到 $aa^{p-2} \equiv 1 \mod p$，因此直接求得 a^{p-2} 即为逆元.注意能使用费马小定理的情况为所选择的模数为质数.

卢卡斯定理

设 p 为素数，非负整数 m,n 的 p 进制式分别为$(m_k,m_{k-1},\ldots,m_0)$, $(n_k n_{k-1}\ldots n_0)$. 则

$$\binom{m}{n}=\prod_{i=0}^{k}\binom{m_i}{n_i}\mod p$$

证明:

$$\because \mathrm{n}_0\equiv \mathrm{n}, m_0\equiv m \mod p$$

原式相当于是求证

$$\binom{m}{n}\equiv\binom{\left\lfloor\frac{n}{p}\right\rfloor}{\left\lfloor\frac{m}{p}\right\rfloor}\binom{n_0}{m_0}\mod p$$

首先对于任意的素数 p 都有

$$\binom{p}{n}\equiv 0 \mod p\,,(n\neq 0 \text{ and } n\neq p\,)$$

对于任意实数 x 有

$$(\mathrm{x}+1)^{\mathrm{p}}\equiv\sum_{i=0}^{p}\binom{p}{i}x^i$$

在模 p 意义下有

$$(\mathrm{x}+1)^{\mathrm{p}}\equiv(x^p+1)\mod p$$

对于一个正整数 m 有

$$(\mathrm{x}+1)^{\mathrm{m}}=(x+1)^{\left\lfloor\frac{m}{p}\right\rfloor p}\cdot(x+1)^{m-\left\lfloor\frac{m}{p}\right\rfloor p}$$

$$\Rightarrow(\mathrm{x}+1)^{\mathrm{m}}=(x^p+1)^{\left\lfloor\frac{m}{p}\right\rfloor}\cdot(\mathrm{x}+1)^{m-\left\lfloor\frac{m}{p}\right\rfloor p}$$

二项式定理展开得

$$\sum_{i=0}^{m}\binom{i}{m}x^i=\left(\sum_{i=0}^{\left\lfloor\frac{m}{p}\right\rfloor}\binom{i}{\left\lfloor\frac{m}{p}\right\rfloor}x^{p_i}\right)\left(\sum_{i=0}^{m-\left\lfloor\frac{m}{p}\right\rfloor p}\binom{i}{m-\left\lfloor\frac{m}{p}\right\rfloor p}x^i\right)$$

那么唯一能组合出任意x^{n}的就是$\mathrm{x}^{\left\lfloor\frac{n}{p}\right\rfloor p}$和$\mathrm{x}^{n-\left\lfloor\frac{n}{p}\right\rfloor p}$.■

扩展卢卡斯

卢卡斯定理只适用于模数 p 必须为素数的情况，而扩展卢卡斯则能处理任意模数的情况.

因为模数 p 能被唯一的分解成$p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$的形式. 所以能对每个质因子分别求出答案$x_1, x_2, \cdots, x_m$. $s=\binom{m}{n}$满足:

$$s \equiv x_1 \mod p_1^{k_1}$$

$$s \equiv x_2 \mod p_2^{k_2}$$

$$\cdots\cdots$$

$$s \equiv x_n \mod p_n^{k_n}$$

这个同余方程组可以用中国剩余定理得到最终的解 s.

如何求出$\binom{m}{n} \mod p_i^{k_i}$

同样是利用定义式分别求出$n!$, $m!^{-1}, (n-m)^{-1} \mod p_i^{k_i}$从而求出$\binom{m}{n} = n!\, m!^{-1}\,(n-m)^{-1} \mod p_i^{k_i}$.

如何求出$n! \mod p_i^{k_i}$?

$$\begin{aligned} n! &= 1\times 2\times\cdots\times n \\ &= \Bigg(\big(1\times 2\times\cdots\times p_i^{k_i}-1\big)\times\big(p_i^{k_i}+1\times\cdots\times 2p_i^{k_i}-1\big)\times\cdots \\ &\qquad \times\left(\left(\left\lfloor\frac{n}{p_i^{k_i}}-1\right\rfloor p_i^{k_i}+1\right)\times\cdots\times\left(\left\lfloor\frac{n}{p_i^{k_i}}\right\rfloor p_i^{k_i}-1\right)\right)\times\left(\left\lfloor\frac{n}{p_i^{k_i}}\right\rfloor p_i^{k_i}+1 \right. \\ &\qquad \left.\times\cdots\times n\right)\Bigg)\cdot p_i^{\left\lfloor\frac{n}{p_i}\right\rfloor}\cdot\left(\left\lfloor\frac{n}{p_i}\right\rfloor!\right) \end{aligned}$$

可以发现整个阶乘被分成了三块

1) 第一部分是有$\left\lfloor\frac{n}{p_i^{k_i}}\right\rfloor$块，它们在模$\mathrm{p_i}^{k_i}$意义下是结果是相同的，因为每块的每个因子模$\mathrm{p_i}^{k_i}$后分别为$1,2,\cdots,\mathrm{p_i}^{k_i}-1$.所以可以求出一块之后快速幂算出$\left\lfloor\frac{n}{p_i^{k_i}}\right\rfloor$个的乘积.

2) 第二部分是$\mathrm{p_i}^{\left\lfloor\frac{n}{p_i}\right\rfloor}$，它与$\mathrm{p_i}^{k_i}$互质，因此不能直接算逆元，但是可以分别求出$\mathrm{n!},\mathrm{m!},(\mathrm{n}-\mathrm{m})!$中对应的$\mathrm{p_i}^{l}$项的指数l，根据$\frac{\mathrm{n!}}{\mathrm{m!(n-m)!}}$直接相减各自的指数.

3) 第三部分是$\left(\left\lfloor\frac{n}{p_i}\right\rfloor!\right)$，这部分递归计算即可.