乘法逆元

如果有 $ax \equiv 1 \pmod b$，则称 x 为 $a \mod b$ 的逆元，记作 a^{-1}。

费马小定理

对于质数 p，满足 $a^{p-1} \equiv 1 \pmod p$。

欧拉定理

对于 $a \perp p$，满足 $a^{\varphi(p)} \equiv 1 \pmod p$，由于在 p 为质数时 $\varphi(p) = p - 1$，所以费马定理是欧拉定理的特殊形式。

拓展欧拉定理

对于任意的 $a, p, b \in N^*, b \geqslant \varphi(p)$，$a^b \equiv a^{(b \bmod \varphi(p)) + \varphi(p)} \pmod p$。

扩展欧几里得算法

求解关于 x 和 y 的同余方程的整数特解 $ax + by = \gcd(a, b)$。
不妨令 $a > b$。
则 $a = \left\lfloor \dfrac{a}{b} \right\rfloor \times b + (a \bmod b)$。
所以 $\left[\left\lfloor \dfrac{a}{b} \right\rfloor \times b + (a \bmod b) \right] x + by = \gcd(a, b)$
所以 $b \left(\left\lfloor \dfrac{a}{b} \right\rfloor \times x + y \right) + (a \bmod b)x = \gcd(b, (a \bmod b))$
递归求解 b 与 $a \bmod b$，直到 $a \bmod b = 0$ 即可。

要讨论 a^{-1}，显然有 $\gcd(a, b) = 1$。

那么计算出 $ax + by = 1$，显然有 $ax \equiv 1 \pmod b$。

同余方程求解

因为 $ax \equiv b \pmod n$。

如果 a, n 互质，则有唯一解 $x \equiv ba^{-1} \bmod n$。

否则令 $\gcd(a, n) = g$，如果 $g \nmid b$，则无解。

如果求解 $\dfrac{a}{g} \times x_0 \equiv \dfrac{b}{g} \pmod{\dfrac{n}{g}}$，此时 $\gcd(\dfrac{a}{g}, \dfrac{n}{g}) = 1$，可以解出 x_0。

则有 $x = \dfrac{kn}{g} + x_0, (k \in \mathbb{N})$ 均为同余方程的解。

Lucas定理

对于**质数** p 有：$\dbinom{n}{m} \equiv \dbinom{\lfloor n/p \rfloor}{\lfloor m/p \rfloor} \times \dbinom{n \bmod p}{m \bmod p} \pmod p$。
其中 $\dbinom{n \bmod p}{m \bmod p}$ 可以直接预处理，$\dbinom{\lfloor n/p \rfloor}{\lfloor m/p \rfloor}$ 接着递归处理即可，求单个组合数的复杂度为 $O(f(n) + g(n) \log n)$，其中 $f(n)$ 为预处理复杂度，$g(n)$ 为单次求组合数复杂度。

证明

考虑 $\binom{p}{n} \bmod p$ 的值，发现 $\binom{p}{n} \bmod p = [n = 0 \vee n = p]$。

考虑二项式 $f(x) = ax^n + bx^m$，我们有：

$$f^p(x) \equiv (ax^n + bx^m)^p \equiv \sum_{i=0}^{p} \binom{p}{i} (ax^n)^i (bx^m)^{p-i} = ax^{pn} + bx^{pm} \equiv f(x^p) \pmod{p}。$$

由于 $\binom{n}{m}$ 就是 $[x^m](1+x)^n$，那么就有：

$$\binom{n}{m} \equiv [x^m](1+x)^n \equiv [x^m](1+x)^{p\lfloor n/p \rfloor}(1+x)^{n \bmod p} \equiv [x^m](1+x^p)^{\lfloor n/p \rfloor}(1+x)^{n \bmod p} \pmod{p}$$

而 $(1+x^p)^{\lfloor n/p \rfloor}(1+x)^{n \bmod p}$ 中的 x^m 项需要从 $(1+x^p)^{\lfloor n/p \rfloor}$ 中取 $\lfloor m/p \rfloor$ 个 x^p，从 $(1+x)^{n \bmod p}$ 中取 $m \bmod p$ 个 x 得到，也就是 $\binom{\lfloor n/p \rfloor}{\lfloor m/p \rfloor} \times \binom{n \bmod p}{m \bmod p}$。

exLucas定理

Lucas定理只能处理 p 为质数的情况，对于不是质数的，我们就需要用 exLucas 定理。

求 $\binom{n}{m} \bmod P$，其中 P 可能是合数。

根据唯一分解定理 $P = \prod_{i=1}^{n} p_i^{\alpha_i}$，其中 p_i 为质数。

我们求出每一个 $\binom{n}{m} \bmod p_i^{\alpha_i}$，然后用中国剩余定理即可。

也就是要求 $\dfrac{n!}{m!(n-m)!} \bmod p^{\alpha}$，需要求分母求逆元，但由于 $m!(n-m)!$ 不一定与质数 p 互质。所以考虑先提取出所有的 p。

所求转化为 $\dfrac{\frac{n!}{p^x}}{\frac{m!}{p^y}\frac{(n-m)!}{p^z}} \times p^{x-y-z} \bmod p^{\alpha}$。

记 $S(n)$ 为 $n!$ 除掉所有因数 p 的值。

现在考虑如何求 $S(n) \bmod p^{\alpha}$。

$\because n! = (p \times 2p \times \cdots \times \left\lfloor \dfrac{n}{p} \right\rfloor p) \times (1 \times 2 \times \ldots)$

$$S(n) \equiv S\left(\left\lfloor \frac{n}{p} \right\rfloor\right) \times \left(\prod_{i=1, p \nmid i}^{p^{\alpha}} i\right)^{\left\lfloor \frac{n}{p^{\alpha}} \right\rfloor} \times (n \bmod p^{\alpha})! \pmod{p^{\alpha}}。$$

$S\left(\left\lfloor \dfrac{n}{p} \right\rfloor\right)$ 递归做，后面的暴力做既可。

Wilson 定理的推广

记 $(n!)_p$ 为所有小于等于 n 但不能被 p 整除的正整数的乘积。

> 对于素数 p 和正整数 q 有 $(p^q!)_p \equiv \pm 1 \pmod{p^q}$。
>
> 更具体的，$(p^q!)_p \equiv \begin{cases} 1, & (p=2) \wedge (q \geq 3) \\ -1, & \text{otherwise} \end{cases}$。

下文两个推论中的 ± 1，均特指这样的定义：当模数 p^q 取 8 及以上的 2 的幂时取 1，其余取 -1。

> 对于素数 p，正整数 q，非负整数 n 和 $N_0 = n \bmod p^q$ 有：

> $(n!)_p = (\pm 1)^{\lfloor n/p^q \rfloor}(N_0!)_p \pmod{p^q}$。

CRT

求解同余方程组：

$\begin{cases} x \equiv & a_1 \pmod{p_1} \\ x \equiv & a_2 \pmod{p_2} \\ & \cdots \\ x \equiv & a_n \pmod{p_n} \end{cases}$，其中 $p_1, p_2 \dots p_n$ 两两互质。

我们知道，对于 $L = \prod_{i=1}^{n} p_i$，$\forall\, i \in [1, n] \cap N^*, k \in N^*, k \times L \equiv 0 \pmod{p_i}$。

因为 $p_i \times p_i^{-1} \equiv 1 \pmod{n}$，所以 $\frac{L}{p_i} \times \left(\frac{L}{p_i}\right)^{-1} \bmod p_j = \begin{cases} 1, & i = j \\ 0, & otherwise \end{cases}$，其中 $\left(\frac{L}{p_i}\right)^{-1}$ 为模 p_i 意义下的逆元。

所以对于 $X = \sum_{i=1}^{n} \left(a_i \times \frac{L}{p_i} \times \left(\frac{L}{p_i}\right)^{-1} \bmod p_i \right) \bmod L$ 满足上述同余方程组。

重数

重数指的是质数 p 的出现次数，也就是质因数分解之后的质数。

$n!$ 中 p 的出现次数为 $\sum_{i=1} \left\lfloor \frac{n}{p^i} \right\rfloor$。