

乘法逆元

乘法逆元一般用来求形同下式的值，一般来说， p 是一个质数

$$\frac{a}{b} \pmod{p}$$

逆元定义

如果 $a * x \equiv 1 \pmod{b}$ ，且 a 与 b 互质，那么称 x 为 a 的逆元，记作 a^{-1}

$$\begin{aligned} \frac{a}{b} \pmod{p} &= \frac{a}{b} * 1 \pmod{p} = \frac{a}{b} * bb^{-1} \pmod{p} = ab^{-1} \pmod{p} \\ bb^{-1} &\equiv 1 \pmod{p} \end{aligned}$$

用快速幂求解逆元

欧拉定理

对于任何正整数 a 和 n 有 $\gcd(a, n) = 1$ ，则 $a^{\phi(n)} \equiv 1 \pmod{n}$

证明：

假设 $A = a_1, a_2, \dots, a_{\phi(n)}$ 是 1 到 n 中 $\phi(n)$ 个互不相同的且与 n 互质的数

$$0 < a_1 < a_2 < \dots < a_{\phi(n)} < n$$

构造一组新的数 $Z = a * a_1, a * a_2, \dots, a * a_{\phi(n)}$

首先， z_i 之间两两模 n 不同余

$$\text{如果 } \exists z_i \equiv z_j \pmod{n}, i \neq j$$

$$z_i - z_j \equiv 0 \pmod{n} \implies a * (a_i - a_j) \equiv 0 \pmod{n} \implies a_i - a_j \equiv 0 \pmod{n} \implies a_i \equiv a_j \pmod{n}$$

矛盾

$$\text{其次, } \gcd(z_i, n) = 1, i = 1, \dots, \phi(n)$$

则 $A = Z$ ，即 $z_i (i = 1.. \phi(n))$ 是 $a_i (i = 1.. \phi(n))$ 的某个排列

$$\begin{aligned} \prod a_i &\equiv \prod z_i \pmod{n} \implies (a^{\phi(n)} - 1) a_1 * \dots * a_{\phi(n)} \equiv 0 \pmod{n} \\ a^{\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

费马小定理

若 p 是质数， a 是正整数，且 a, p 互质。那么， $a^{p-1} \equiv 1 \pmod{p}$

根据费马小定理，可以很容易的知道当 p 是质数， a 是正整数时， $a^{-1} = a^{p-2}$