快速幂

kiri

2024 年 2 月 16 日

1 快速幂

1. 用途: 在 $o(k)$ 的时间复杂度内求出 $a^k \mod p$ (其中 $1 \le a, p, k \le 10^9$)

2. 基本思路: 反复平方法:

   - 首先预处理出 $\overbrace{a^{2^0} \mod p, a^{2^1} \mod p, a^{2^2} \mod p \cdots a^{2^{\log k}} \mod p}^{\log k}$
   - 又 $a^k = a^{2^{x_1}} a^{2^{x_2}} \cdots a^{2^{x_i}} = a^{2^{x_1}+2^{x_2}\cdots+2^{x_i}}$ (也就是把 k 转成二进制)
   - 预处理时的一个快捷方法:$a^1 = a^{2^0}, a^{2^1} = (a^{2^0})^2, a^{2^2} = (a^{2^1})^2 \cdots a^{2^{logk}} = (a^{2^{logk-1}})^2$

2 快速幂求逆元

2.1 逆元

整数 b,m 互质, 且 $b|a$, 如果 $\exists x, st. \frac{a}{b} \equiv a \cdot x \pmod m$ 则 x 为 b 的逆元,$x = b^{-1}$. 在 $\pmod m$ 的情况下除 b 等于乘上 b 的逆元

注意: 如果 b 和 m 不互质, 那么 b 的逆元不存在

2.2 快速幂怎么求逆元

因为 $\frac{a}{b} = a \cdot b^{-1} \pmod m$, 那么两边同时乘上 b 是可以的:$b \cdot \frac{a}{b} \equiv ab \cdot b^{-1} \pmod m$, 即 $a \equiv abb^{-1} \pmod m$, 又因 b 与 m 互质, 所以 $b \cdot b^{-1} = 1 \pmod m$. 又根据费马小定理: 当 m 是质数 p 时,$b^{p-1} \equiv 1 \pmod p$ 那么 $b \cdot b^{p-2} \equiv 1 \pmod p$, 又因 b 与 p 互质, 那么 $b^{-1} \equiv b^{p-2} \pmod p$