逆元

定义

逆元是指在数学领域群G中任意一个元 a,都在G中有唯一的逆元a',具有性质:$a \cdot a' = a' \cdot a = e$(·为该群中定义的运算).其中,e为该群的单位元.逆元其实是加法中的相反数以及乘法中的倒数的拓展思想.在模运算中,单位元便是1.
$a\ mod\ p$的逆元便是可以使$a * a'\ mod\ p = 1$的最小a'.
最常见的运用:
因为b'为b的逆元,$b * b'\ mod\ p = a$,所以$(a/b)\ mod\ p = (a * b')mod\ p$
这样我们就可以用$(a * b)\%p = (a\%p * b\%p)\%p$这一条性质缩小中间运算结果.

求逆元

1.枚举法:-O(P)

暴力枚举1~p-1的整数x,找到$b * x\%p = 1$,则x为b mod p的逆元.p显然不是,p+k的话,根据mod的特性,能归回到枚举1~p-1.

2.利用拓展欧几里得(Extend-Eculid)求解同余方程:-O(log...)

求最小整数x,y,使$x * a + y * b = gcd(a, b)$.由欧几里得定理可知:$gcd(a, b) = gcd(b, a\%b)$,所以有$x' * b + y' * (a\%b) = gcd(a, b)$.假设我们已经求得x',y',那么又因为:$a\%b = a - \lfloor \frac{a}{b} \rfloor * b, 则: y' * a + (x' - y' * \lfloor \frac{a}{b} \rfloor) * b = gcd(a, b)$.那么这个问题就可以用递归求解.显然,b=0的时候,x=1,y=0.现在,我们考虑用归化法,将求解$b * b'\ mod\ p = 1$转化为这个问题,即:求解最小整数b',k,使得$b' * b + k * p = 1$.

3.费马小定理(Fermat's little theorem):-O(lg(p-2))

假如p是质数,那么$a^{p-1} = 1\ mod\ p$.推论:$b^{p-2}\%p$即为$b\ mod\ p$的乘法逆元.(这里需要b,p互质才能使用逆元法求解$(a/b)\%p$,否则,如果b,p不互质,只能用$(a/b)\%p = (a\%(b * p))/b$来尝试解决问题,但是一般题目给的p都是质数).