FORMULA

SysCon

February 6, 2018

https://sysconkonn.github.io/

1 斯特林公式

1.1 式子:

$$n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$$

2 求逆元:

2.1 式子:

设数x的逆元为$inv[x]$, 数p为一个质数，则

$$inv[x] = (p - p/x) \times inv[p\% \ x]$$

2.2 证明方法:

我们假设质数p可以最简的表示为:$p = a \times x + b$
显然的，有$x > b$,因为不然的话可以从b中再提出一个x
所以有以下的递推式:

$$p \equiv 0(mod \ \ p)$$
$$a \times x + b \equiv 0(mod \ \ p)$$

因为我们知道，对于模等式，两边同时加、减、乘一个式子依然成立。
所以两边同时乘以$inv[x] \cdot inv[b]$后:

$$a \times inv[b] + inv[x] \equiv 0(mod \ \ p)$$

为什么就不用详细解释，将式子展开，因为
$x \times inv[x] \equiv 0(mod \ \ p)$
然后:

$$inv[x] \equiv -a \times inv[b](mod \ \ p)$$
$$p \times inv[b] + inv[x] \equiv pinv[b] - a \times inv[b](mod \ \ p)$$

因为$p \times inv[b]\%p == 0$
接下来省略后面的mod符号

$$inv[x] \equiv p \times inv[b] - a \times inv[b]$$
$$inv[x] \equiv (p - a) \times inv[b]$$

此时我们应该把不知道的a, b去掉才好求的。
再回到原来的式子:$p = a \times r + b$
因为$r > b$,所以由计算机的整数相除法则，可以知道$p/r = a$,相应的$p\%r = b$
所以就可以得到最终的式子啦。

$$inv[x] = (p \quad - \quad p \div r) \times inv[p\%r]$$