欧几里得算法

成都石室中学　　kririae

2018 年 2 月 7 日

预备知识 1

欧几里得算法:
$gcd(a, b) = gcd(b, a \ mod \ b)$
其实就是小学时候学习的辗转相除法的递归写法

预备知识 2

mod **的定义**:

$a(mod\ b) = a - \lfloor \frac{a}{b} \rfloor b$

$\Leftrightarrow a = a\ mod\ b + \lfloor \frac{a}{b} \rfloor b$

拓展欧几里得

求解不定方程 ax + by = gcd(a, b) **可以求出递推公式**:

$ax_1 + by_1 = gcd(a, b)$

$\Rightarrow bx_2 + (a \bmod b)y_2 = gcd(b, a \bmod b)$

$\Rightarrow ax_1 + by_1 = bx_2 + (a \bmod b)y_2$

$a \bmod b = a - \lfloor \frac{a}{b} \rfloor b$

$\Rightarrow ax_1 + by_1 = bx_2 + (a - \lfloor \frac{a}{b} \rfloor b)y_2$

$\Rightarrow ax_1 + by_1 = ay_2 + b(x_2 - \lfloor \frac{a}{b} \rfloor y_2)$

$x_1 = y_2$

$y_1 = x_2 - \lfloor \frac{a}{b} \rfloor y_2$

小小的总结

$ax - kc = b$，先假设 $ax - kc = gcd(a, c)$，现在的解是乘 $\frac{gcd(a,c)}{b}$ 之后的，在输出结果的时候需要保证是正数。

小小的总结 2

需要证明 $ax \equiv b \ (mod \ c)$ 支持换元

$$\Rightarrow ax - b \equiv 0 \ (mod \ c)$$

由此可得

$$\Rightarrow ax - b = ck$$

移项可得拓展欧几里得式

$$ax - ck = b$$

假设

$$ax - ck = gcd(a, c)$$

小小的总结 2

然后 $exgcd(a, c, x, -k)$ 求出 x 和-k。左右同时乘 $\frac{b}{gcd(a,c)}$，解出 x 的值.

小小的总结 2

如何证明，当且仅当 $gcd(a, c)|b$ 时，才存在解？

小小的总结 2

已经看到了，上面的公式中，结果需要乘一个数 $\frac{b}{gcd(a,b)}$ 当且仅当这个数字是整数，才行。