欧几里得算法

成都石室中学　　kririae

2018 年 2 月 6 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:

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

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

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**:

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

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

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

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

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

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

$x_1 = y_2$

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