

解同余方程

$$ax + by = n$$

判断是否有

$$\gcd(a, b) | n$$

其次,根据扩展欧几里得算法可求得方程

$$ax_0 + by_0 = \gcd(a, b)$$

的解,令

$$\gcd(a, b) = d$$

则可以求出原方程的一个解为

$$x = x_0 * \frac{n}{\gcd(a, b)}, y = y_0 * \frac{n}{\gcd(a, b)}$$

于是可得其最小正整数解

$$t = \frac{b}{\gcd(a, b)}, x = (x \bmod t + t) \bmod t$$

可得其通解为

$$x = x_0 + k * t$$

k 为任意正整数