Extended euclid

$$ax_0 + by_0 = d$$

$\leftrightarrow \quad bx_1 + [a - b.\text{int}(\frac{a}{b})]\,y_1 = d$

$\leftrightarrow \quad bx_1 + ay_1 - b.\text{int}(\frac{a}{b})\,y_1 = d$

$\leftrightarrow \quad ay_1 + b(x_1 - \text{int}(\frac{a}{b})\,y_1) = d$

$\rightarrow \left[\begin{array}{l} x_0 = y_1 \\ y_0 = x_1 - y_1 . \text{int}(\frac{a}{b}) \end{array}\right.$

Nghiệm Diophinate

Từ bổ đề bezout, ta có:

$(a, b) \leftrightarrow ax + by = d = (a, b)$

Nếu $d \mid c$ thì $c = d.k \leftrightarrow k = \frac{c}{d}$

Ta có $\leftrightarrow ax.\frac{c}{d} + by.\frac{c}{d} = c$

$\rightarrow \begin{cases} x_0 = x.\frac{c}{d} \\ y_0 = y.\frac{c}{d} \end{cases}$ → Dùng Extended euclid để tìm $(x; y)$

Nghiệm tổng quát diophinate

Xét $ax + by = c$, gọi $d = (a, b)$

$\leftrightarrow \quad a(x_0 + \frac{b}{d}) + b(y_0 - \frac{a}{d}) = c$

Kiểm tra: $ax_0 + by_0 + \frac{ab}{d} - \frac{ab}{d} = c$ (thỏa)

$\rightarrow \begin{cases} x = x_0 + k.\frac{b}{d} \\ y = y_0 - k.\frac{a}{d} \end{cases} \quad (k \in \mathbb{Z})$

* Nghiệm nguyên dương $(x, y > 0)$

$\leftrightarrow \begin{cases} x_0 + k\frac{b}{d} > 0 \\ y_0 - k\frac{a}{d} > 0 \end{cases} \leftrightarrow \begin{cases} k > -x_0 . \frac{d}{b} \\ k < y_0 . \frac{d}{a} \end{cases} \rightarrow -x_0 . \frac{d}{b} < k < y_0 . \frac{d}{a}$