Euclid mở rộng

$d = \gcd(a, b)$

⇔ Tìm $\overset{(\in \mathbb{Z})}{(x, y)}$ thoả $ax + by = d$

Phương trình Diophantus tuyến tính 2 ẩn

$ax + by = c \quad (a, b, c \in \mathbb{Z})$

Nghịch đảo modulo $\gamma = a^{-1} \pmod{M}$

⇒ Tồn tại khi $\gcd(a, M) = 1$

$$a\gamma + My = 1$$

$$\Rightarrow a\gamma = 1 - My$$

$$a\gamma \equiv 1 \pmod{M}$$

$$\gamma \equiv a^{-1} \pmod{M}$$

Diophantus

$$ax + by = c$$

$$\gcd(a,b) = d \rightarrow d \mid c$$

$$\Leftrightarrow ax' + by' = d$$

$$\left(\times \cancel{d}\,\frac{c}{d}\right)$$

$$a \cdot \boxed{x'\frac{c}{d}} + b\,\boxed{y'\frac{c}{d}} = c$$

$$\Leftrightarrow \begin{cases} x_0 = x' \cdot \frac{c}{d} \\ y_0 = y' \cdot \frac{c}{d} \end{cases}$$

$$\Leftrightarrow \begin{cases} x = x_0 + k \times \frac{b}{d} \\ y = y_0 + k \times \frac{a}{d} \end{cases} \quad (k \in Z)$$

```
                                  // ax + by = d = gcd(a,b)
int extEuclid (a, b, &x, &y):
    if b == 0:
        x, y = 1, 0 ; return a
    q = a / b
    r = a - b.q
    d = extEuclid (b, r, x1, y1)
    x = y1
    y = x1 - q * y1
    return d
                                  // ax + by = c
ll diophantineSolve (a, b, c)
    d = extEuclid (a, b, x, y)
    if c % d ≠ 0: return Invalid_Root
    x *= c/d;   if a<0: x = -x
    y *= c/d;   if b<0: y = -y
    return (x, y)

int modInverse (a, m): // x ≡ a^-1 (mod m)
    gcd = extEuclid (a, m, x, y)
     if gcd ≠ 1 : return -1
     else: return (x % m + m) % m.
```