Gọi x_i, y_i là các hệ số của biểu diễn tuyến tính r_i theo a và b, tức là $r_i = ax_i + by_i$. Thay biểu diễn này vào phép chia ở trên:

$$ax_{i-1} + by_{i-1} = q_i(ax_i + by_i) + (ax_{i+1} + by_{i+1}),$$

rồi cân bằng hệ số của a và b, được $x_{i-1} = q_i x_i + x_{i+1}$ và $y_{i-1} = q_i y_i + y_{i+1}$. Ta có hệ thức đệ quy

$$\begin{aligned} x_{i+1} &= x_{i-1} - q_i x_i, \quad \text{và} \\ y_{i+1} &= y_{i-1} - q_i y_i, \end{aligned}$$

trong đó $r_0 = a = 1a + 0b$, cho ta $x_0 = 1, y_0 = 0$, và $r_1 = b = 0a + 1b$, ứng với $x_1 = 0, y_1 = 1$.

Khi thuật toán Euclid dừng, $r_n = ax_n + by_n$. Đặt $x_n = x, y_n = y$, ta có biểu diễn

$$\gcd(a, b) = ax + by,$$

gọi là thuật toán Euclid mở rộng.

Ví dụ 4.27. Tìm khai triển Euclid mở rộng của 91 và 287.

Giải. $\gcd(91, 297) = 7$, và biểu diễn tuyến tính $7 = 19 \cdot 91 + (-6)287$. Quá trình tính được thể hiện trong bảng sau

i	a	b	q_i	x_i	y_i
0	91	287		1	0
1	287	91	0	0	1
2	91	14	3	1	0
3	14	**7**	6	-3	1
4	7	0		**19**	$\mathbf{-6}$

Cách 1: dùng gói lệnh

```
from sympy import *
gcdex(91, 287)
```

kết quả $(19, -6, 7)$ cho ta hệ thức $19 \cdot 91 + (-6)287 = 7$

Cách 2: lập trình

```
def gcdex(a, b):
    x0, y0 = 1, 0
    x1, y1 = 0, 1
    while b != 0:
        q = a // b
```

```
        a, b = b, a % b
        x = x0 - x1 * q
        y = y0 - y1 * q
        x0, y0 = x1, y1
        x1, y1 = x, y
    return x0, y0, a
```

□

Định lý 4.7. *Với $a, b, c \in \mathbb{Z}$, $a \neq 0$ hoặc $b \neq 0$, phương trình Diophant*[‖] $ax + by = c$ *có nghiệm nguyên khi và chỉ khi* $\gcd(a, b) \mid c$.

Đặc biệt, với $c = 1$

$$\gcd(a, b) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z}, \;\; ax + by = 1.$$

Hai số nguyên liên tiếp $a, a+1$ nguyên tố cùng nhau, vì $a(-1) + (a+1) \cdot 1 = 1$.

Định nghĩa 4.6. *Cho $a, b \in \mathbb{Z}^+$. Số $c \in \mathbb{Z}^+$ gọi là một bội chung của a, b nếu c là bội của cả a và b. Số nhỏ nhất trong các bội chung của a, b gọi là bội chung nhỏ nhất của a, b, ký hiệu* $\mathrm{lcm}(a, b)$.

Ví dụ 4.28. Tìm $\mathrm{lcm}(6, 15)$.

Giải.

$$\begin{aligned} A &= \{a \in \mathbb{Z}^+ : 6 \mid a\} = \{6, 12, 18, 24, 30, 36, \ldots\} \\ B &= \{a \in \mathbb{Z}^+ : 15 \mid a\} = \{15, 30, 45, 60, 75, \ldots\} \\ \Rightarrow A \cap B &= \{a \in Z^+ : 6 \mid a \wedge 15 \mid a\} = \{30, 60, \ldots\} \\ \Rightarrow \mathrm{lcm}(6, 15) &= \min A \cap B = 30. \end{aligned}$$

□

Định lý 4.8. *Cho $a, b \in \mathbb{Z}^+$ và $c = \mathrm{lcm}(a, b)$. Nếu d là một ước chung của a và b, thì $c \mid d$.*

Định lý 4.9. $\forall a, b \in \mathbb{Z}^+, \;\; ab = \mathrm{lcm}(a, b) \cdot \gcd(a, b)$.

[‖] Diophantus, thế kỷ 3, nhà toán học Hy Lạp