Định nghĩa 4.5. *Cho $a, b \in \mathbb{Z}$ với $a \neq 0$ hoặc $b \neq 0$. Ta nói a, b nguyên tố cùng nhau nếu* $\gcd(a, b) = 1$.

Cho $a, b \in \mathbb{Z}^+$. Xét thuật toán chia a cho b: $a = qb + r$, với $0 \leq r < b$. Khi đó

$$\gcd(a, b) = \gcd(b, r) = \gcd(b, a \bmod b).$$

Định lý 4.6 (Thuật toán Euclid)**.** *Cho $a, b \in \mathbb{Z}^+$. Đặt $r_0 = a$, $r_1 = b$, và áp dụng thuật toán chia như sau*

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1\\
r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2\\
r_2 &= q_3 r_3 + r_4, && 0 < r_4 < r_3\\
&\dots\\
r_{i-1} &= q_i r_i + r_{i+1}, && 0 < r_{i+1} < r_i\\
&\dots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, && 0 < r_n < r_{n-1}\\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Khi đó $\gcd(a, b) = r_n$*, là phần dư khác không cuối cùng.*

Ví dụ 4.25. Tìm $\gcd(91, 287)$.

Giải.

$$\begin{aligned}
91 &= 0 \cdot 287 + 91\\
287 &= 3 \cdot 91 + 14\\
91 &= 6 \cdot 14 + 7\\
14 &= 2 \cdot 7
\end{aligned}$$

nên $\gcd(91, 287) = 7$.

Cách 1: Dùng hàm `gcd` của thư viện `math` hoặc `igcd` của `sympy`

```
import math
math.gcd(91, 287)   # gcd(91, 287) = 7

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

Cách 2: Đệ quy

```python
def gcd(a, b):
    if b == 0:
        return a
    else:
        return gcd(b, a % b)
```

Cách 3: Phương pháp quy hoạch động cho hệ thức đệ quy

$$r_{i+1} = r_{i-1} \bmod r_i, \quad i = 1, 2, \ldots, \quad \text{với } r_0 = a, r_1 = b,$$

đến khi $r_{n+1} = 0$.

```python
def gcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

```python
def gcd(a, b):
    while b != 0:
        r = a % b
        a = b
        b = r
    return a
```

□

Ví dụ 4.26. Với $n \in \mathbb{Z}^+$, chứng minh $8n + 3$ và $5n + 2$ nguyên tố cùng nhau.

Giải.

$$\begin{aligned} 8n + 3 &= 1 \cdot (5n + 2) + (3n + 1) \\ 5n + 2 &= 1 \cdot (3n + 1) + (2n + 1) \\ 3n + 1 &= 1 \cdot (2n + 1) + n \\ 2n + 1 &= 2 \cdot n + 1 \\ n &= n \cdot 1 \end{aligned}$$

nên $\gcd(8n + 3, 5n + 2) = 1$.

```python
from sympy import *
n = symbols('n')
gcd(8*n + 3, 5*n + 2)
```

□