Euclidean 演算法的證明

對於任意兩個非負整數 a 和 b，我們可以使用歐幾里得（Euclidean）演算法來計算它們的最大公因數（greatest common divisor，簡稱 gcd）

- 證明過程：

假設 t 是 a 和 b 的一個公因數，則 $t \mid a$ 且 $t \mid b$；
而 $t \mid bq$，由已知 $a = bq + r$，得 $a - bq = r$
$\because$ $t \mid a$，即 $t \mid r$
$\therefore$ t 也是 b 和 r 的一個公因數。
反之，假設 s 是 b 和 r 的一個公因數，則 $s \mid b$ 且 $s \mid r$；
$\because$ $s \mid bq + r$，即 $s \mid a$，
$\therefore$ s 也是 a 和 b 的公因數。
故 $(a,b) = (b,r)$，兩者公因數一致。

設有任意整數 r_1 和 r_2，且設 $r_2 \neq 0$
$r_1 = r_2 q_1 + r_3$ $(0 < r_3 < r_2)$
$r_2 = r_3 q_2 + r_4$ $(0 < r_4 < r_3)$
$r_3 = r_4 q_3 + r_5$ $(0 < r_5 < r_4)$
$\cdots$
如果餘數 $r_3, r_4, r_5, \ldots$ 都不為 0，則這些餘數構成一個遞減的正整數序列。

$$r_3 > r_4 > r_5 > \cdots > 0$$

因此，在 n 步之後（$n \leq r_2$），必然出現餘數等於 0 的情況，即
$r_{n-1} = r_n q_{n-1} + r_{n+1}$ $(0 < r_{n+1} < r_n)$，$r_n = r_{n+1} q_n + 0$
故 $(a,b) = (r_1,r_2) = (r_2,r_3) = (r_3,r_4) = \cdots = (r_n,r_{n+1}) = (r_{n+1},0) = r_{n+1}$

由於 $0 \leq r_{i+1} < |r_i|$ $(0 \leq i \leq n)$ 且 r_i 序列是一個遞減序列，所以本演算法在有限步驟內必然終止。

又因為 $r_{i+1} = r_{i-1} - r_i q_i$，$(r_{i-1},r_i)$ 和 (r_i,r_{i+1}) 的最大公因數是一樣的，所以最終得到的 r_{n+1} 是 a 和 b 的最大公因數。