DM-01-08 ► 證明 Euclid 演算法 (輾轉相除法)：給定自然數 a 與 b ，而且 b 不為 a 之因數。令 $r_0 = a$ 且 $r_1 = b$，重複應用除數法則可得一串餘數 $r_1, r_3, r_4, \ldots, r_n$，直到 $r_{n+1} = 0$，滿足下列關係式：

$$\begin{cases} r_0 = r_1 \cdot q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2 \cdot q_2 + r_3, & 0 < r_3 < r_2 \\ \vdots & \\ r_{k-1} = r_k \cdot q_k + r_{k+1}, & 0 < r_{k+1} < r_k \\ \vdots & \\ r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n \cdot q_n + r_{n+1}, & \text{且 } r_{n+1} = 0 \end{cases} \tag{1}$$

則 $r_n = \gcd(a, b)$。

【證明】 由 (1) 之最後一式 $r_{n+1} = 0$ 知，$\gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n$ 。因 $r_0 = a$ 且 $r_1 = b$，底下我們只要證明對所有正整數 k，$1 \leq k \leq n$

$$\gcd(r_{k-1}, r_k) = \gcd(r_k, r_{k+1})$$

皆成立，則 $r_n =\gcd(a, b)$ 即可得證。

令 $g = \gcd(r_{k-1}, r_k)$ 且 $h = \gcd(r_k, r_{k+1})$。

因 $g = \gcd(r_{k-1}, r_k)$，$g|r_{k-1}$ 且 $g|r_k$。當考慮 r_{k-1}，r_k 與 r_{k+1} 為給定之自然數，由 (1) 式之 $r_{k-1} = r_k \cdot q_k + r_{k+1}$ 知，$(1, -q_k)$ 為 Diophantine 方程式 $r_{k-1} \cdot x + r_k \cdot y = r_{k+1}$ 的整數解。根據定理 3，$g|r_{k+1}$。換言之，g 為 r_k 與 r_{k+1} 的一個公因數。故 $g \leq h$。

同理，因 $h = \gcd(r_k, r_{k+1})$，$h|r_k$ 且 $h|r_{k+1}$。由 (1) 式之 $r_{k-1} = r_k \cdot q_k + r_{k+1}$ 知，$(q_k, 1)$ 為 Diophantine 方程式 $r_k \cdot x + r_{k+1} \cdot y = r_{k-1}$ 的整數解。根據定理 3，$h|r_{k-1}$。換言之，h 為 r_{k-1} 與 r_k 的一個公因數。故 $h \leq g$。

由 $g \leq h$ 且 $h \leq g$，得證 $g = h$，即 $\gcd(r_{k-1}, r_k) = \gcd(r_k, r_{k+1})$。 □

賴志松提供