DM-01-04 ▶ 試證算術基本定理 (Fundamental Theorem of Arithmetic)：
(1) 對每一大於 1 的自然數 n，n 為一質數 (prime number)，或是某些質數的乘積。
(2) 若 n 可以表為某些質因數的連乘積，且質因數的次序不考慮的話，其表示法是唯一的。

【證明】 (1) 假設存在有大於 1 的自然數它無法表示成質數的乘積，令 S 為這些數所成的集合。則 $S \neq \emptyset$ 且 $S \subset \mathbb{N}$。根據自然數的良序原則 (well-ordering principle) 知，S 中必有一最小元素 m。很顯然，m 不能是質數，因為任何質數都可以表示成自己這個質數的乘積。故 $m = ab$，其中 a 與 b 均為小於 m 且大於 1 的自然數。因為 $m = \min S$，所以 $a, b \notin S$。換言之，a 與 b 二數均可以表示成質數的乘積。且由於 $m = ab$，所以 m 亦可以表示成質數的乘積，此一結果即產生矛盾。

(2) 在證明大於 1 的自然數均有唯一的質因數分解之前，首先我們必需證明底下性質：

『設 p 為一質數且 ab 為一整數的乘積。若 $p \,|\, ab$，則 $p \,|\, a$ 或 $p \,|\, b$。』 (*)

因 $p \,|\, ab$，存在一整數 q 使得 $ab = pq$。假設 p 不整除 a (即 p 與 a 互質)，則存在二整數 x 與 y 使得 $px + ay = 1$ 成立。兩邊同乘 b，得 $pbx + aby = b$。則 $pbx + aby = pbx + pqy = p(bx + qy) = b$，即得 p 可以整除 b。

利用數學歸納法，我們可以將 (*) 式推廣如下：

『設 p 為一質數且 $a_1 a_2 \cdots a_k$ 為一乘積數。若 $p \,|\, a_1 a_2 \cdots a_k$，則 $p \,|\, a_i$ ，其中 i 為介於 1 至 k 之間的一個整數。』 (**)

今假設存在有自然數其質因數分解不是唯一，令 S 表示這些自然數所成的集合。由自然數的良序原則知存在一元素 $n = \min S$。則 n 可以表示為

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad \text{其中 } p_i \text{ 為質數且 } e_i > 0, \forall i = 1, 2, \ldots, k$$

及

$$n = q_1^{f_1} q_2^{f_2} \cdots q_l^{f_l}, \quad \text{其中 } q_i \text{ 為質數且 } f_i > 0, \forall i = 1, 2, \ldots, l$$

兩種不同的質因數分解。不失一般性假設 $p_1 < p_2 < \cdots < p_k$ 且 $q_1 < q_2 < \cdots < q_l$。因 $p_1 \,|\, n$ (即 $p_1 \,|\, q_1^{f_1} q_2^{f_2} \cdots q_l^{f_l}$)，由 (**) 式知存在某一 $j \in \{1, 2, \ldots, l\}$，使得 $p_1 \,|\, q_j^{f_j}$。因 p_1 與 q_j 皆為質數，$p_1 = q_j$。若 $j \neq 1$，則 $q_1 < q_j = p_1$。另外，因 $q_1 \,|\, n$ (即 $q_1 \,|\, p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$)，同理可得存在某一 $i \in \{1, 2, \ldots, k\}$， 使得 $q_1 \,|\, p_i^{e_i}$。因 q_1 與 p_i 皆為質數，$q_1 = p_i$。若 $i \neq 1$，則 $p_1 < p_i = q_1$。故 $i \neq 1$ 與 $j \neq 1$ 不能同時成立，即 $p_1 = q_1$ 成立。

令 $m = \frac{n}{p_1}$。因 $p_1 = q_1$，m 可以同時表示為

$$m = p_1^{e_1 - 1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{與} \quad m = q_1^{f_1 - 1} q_2^{f_2} \cdots q_l^{f_l}$$

因為 $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ 與 $q_1^{f_1} q_2^{f_2} \cdots q_l^{f_l}$ 為 n 的兩種不同質因數分解，當 $p_1 = q_1$ 時，$p_1^{e_1 - 1} p_2^{e_2} \cdots p_k^{e_k}$ 與 $q_1^{f_1 - 1} q_2^{f_2} \cdots q_l^{f_l}$ 亦為不同的質因數分解， 故 $m \in S$。因 $n = \min S$，但 $m < n$，即產生矛盾。 □

賴志松提供