Proof. 為了方便, 我們令 $M = m_1 \cdots m_r$ 且對任意 $i \in \{1,\ldots,r\}$, 令 $M_i = M/m_i$.

要注意這裡 M_j 和 m_i 有以下的關係: (1) 若 $i \neq j$, 則 $m_i | M_j$. (2) $\gcd(M_i, m_i) = 1$. 這裡 (1) 由 M_j 的定義相信大家很容易得知；至於 (2) 假設 M_i, m_i 不互質, 即存在一質數 p 使得 $p|M_i$ 且 $p|m_i$. 然而依定義 M_i 是由 m_j, 其中 $j \neq i$ 的這些 m_j 相乘而得，故由 Corollary 1.5.3 知存在 $j \neq i$ 使得 $p|m_j$. 但是 $j \neq i$, 依假設 $\gcd(m_j, m_i) = 1$, 故 $p|m_j$ 且 $p|m_i$ 和 m_j, m_i 互質相矛盾, 故得證 $\gcd(M_i, m_i) = 1$.

接下來，對任意 $i \in \{1,\ldots,r\}$ 我們想要找到一個整數 $e_i \in \mathbb{Z}$ 滿足 (1) 當 $i \neq j$ 時 $e_i \equiv 0 \pmod{m_j}$；(2) $e_i \equiv 1 \pmod{m_i}$。針對 (1) 我們知 e_i 一定是 M_i 的倍數，故可設 $e_i = kM_i$；又因為 (2) 要求 $kM_i \equiv 1 \pmod{m_i}$，故利用 $\gcd(M_i, m_i) = 1$，知存在 $\lambda_i \in \mathbb{Z}$ 使得 $\lambda_i M_i \equiv 1 \pmod{m_i}$（Proposition 3.2.5）. 因此只要令 $e_i = \lambda_i M_i$ 就是我們所要找的整數了。

現對任意的一組給定的 $c_1,\ldots,c_r \in \mathbb{Z}$ 我們只要令 $c = c_1e_1 + \cdots + c_re_r$，則利用 modulo 的運算性質，對任意 $i \in \{1,\ldots,r\}$ 皆滿足 $c \equiv c_i \pmod{m_i}$。因此證得了存在性。至於在 modulo M 之下的唯一性，可先假設 $c, c' \in \mathbb{Z}$ 皆滿足：對任意 $i \in \{1,\ldots,r\}$ 皆有 $c \equiv c_i \pmod{m_i}$ 且 $c' \equiv c_i \pmod{m_i}$. 亦即，對任意 $i \in \{1,\ldots,r\}$ 皆有 $m_i | c - c'$. 然而這些 m_i 兩兩互質, 故利用 Proposition 1.7(2), 我們得 $m_1 \cdots m_r | c - c'$, 即 $c \equiv c' \pmod{M}$. □

Example 3.5.3. 給定 $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ 以及 $c_1 = 2$, $c_2 = 1$, $c_3 = 3$ 我們希望找到一整數 c 使得 $c \equiv c_i \pmod{m_i}, \forall i \in \{1,2,3\}$. 依照 Theorem 3.5.2 的符號訂法我們有 $M_1 = 20$, $M_2 = 15$ 以及 $M_3 = 12$. 首先我們找到 $\lambda_1 \in \mathbb{Z}$ 使得 $\lambda_1 M_1 \equiv 1 \pmod{m_1}$, 即 $20\lambda_1 \equiv 1 \pmod 3$, 也就是說滿足 $2\lambda_1 \equiv 1 \pmod 3$. 由此找到 $e_1 = \lambda_1 M_1 = 2 \times 20 = 40$. 同理我們要找到 λ_2, λ_3 分別滿足 $15\lambda_2 \equiv 1 \pmod 4$ (即 $3\lambda_2 \equiv 1 \pmod 4$) 以及 $12\lambda_3 \equiv 1 \pmod 5$ (即 $2\lambda_3 \equiv 1 \pmod 5$). 可得 $e_2 = 3 \times 15 = 45$ 和 $e_3 = 3 \times 12 = 36$. 故令 $c = 2 \times 40 + 1 \times 45 + 3 \times 36 = 233$ 確實滿足 $233 \equiv 2 \pmod 3$, $233 \equiv 1 \pmod 4$ 以及 $233 \equiv 3 \pmod 5$. 又 $233 \equiv 53 \pmod{60}$，所以只要滿足 $c \equiv 53 \pmod{60}$ 的整數都滿足要求。當然了也僅有滿足 $c \equiv 53 \pmod{60}$ 的整數會滿足。

有些簡單的情況並不需要動用到中國剩餘定理的程序處理。例如 Example 3.5.3 中，若 $c_1 = c_2 = c_3 = 2$，我們馬上就知 $c \equiv 2 \pmod{60}$ 為其解。這就是唯一性的妙用。

Question 3.3. 考慮在 Theorem 3.5.2 的論證中所用的 e_i，說明 $e_1 + e_2 + \cdots + e_r \equiv 1 \pmod{M}$.

Theorem 3.5.2 的證明所用的方法適用於一次解決好幾個同類型的同餘問題。例如 Example 3.5.3 中，一旦知道 $e_1 = 40, e_2 = 45, e_3 = 36$ 就可以解決所有有關 $c \equiv c_1 \pmod 3$, $c \equiv c_2 \pmod 4$ 以及 $c \equiv c_3 \pmod 5$ 的同餘問題。中國剩餘定理還有一個處理方式，就是兩個、兩個處理（這樣就可以利用數學歸納法證明存在性）。這個方法有時在僅處理一次的中國剩餘問題較便捷，我們也順便簡單介紹一下。

首先考慮 Theorem 3.5.2 中 $c \equiv c_1 \pmod{m_1}$ 且 $c \equiv c_2 \pmod{m_1}$ 這一個同餘問題。因為 m_1, m_2 互質，我們先用輾轉相除法解 $m_1x + m_2y = 1$。若解出一組 $a, b \in \mathbb{Z}$ 使得 $am_1 + bm_2 = 1$，則令 $c = c_2am_1 + c_1bm_2$ 就會滿足 $c \equiv c_1 \pmod{m_1}$ 且 $c \equiv c_2 \pmod{m_1}$。這

是因為在 modulo m_1 之下 $c \equiv c_1 bm_2 \pmod{m_1}$ 且因 $am_1 + bm_2 = 1$，所以在 modulo m_1 之下 $bm_2 \equiv 1 \pmod{m_1}$，因此得 $c \equiv c_1 bm_2 \equiv c_1 \pmod{m_1}$。同理在 modulo m_2 之下得

$$c = c_2 am_1 + c_1 bm_2 \equiv c_2 am_1 \equiv c_2 \pmod{m_2}.$$

接著就如法炮製兩個、兩個處理，得到所求。我們看看用此方法如何處理 Example 3.5.3：

Example 3.5.4. 因為 $m_1 = 3, m_2 = 4$，解得 $(-1) \times m_1 + 1 \times m_2 = 1$。因為要找到 $c' \in \mathbb{Z}$ 滿足 $c' \equiv 2 \pmod{m_1}$ 且 $c' \equiv 1 \pmod{m_2}$ 故令 $c' = 1 \times (-1) \times (m_1) + 2 \times 1 \times m_2 = -3 + 8 = 5$ 符合所求。注意，由唯一性我們知 $c' \equiv 5 \pmod{12}$ 皆符合所求。所以最後我們便是要找到 $c \in \mathbb{Z}$ 滿足 $c \equiv c' \equiv 5 \pmod{12}$ 且 $c \equiv 3 \pmod{5}$。利用輾轉相除法 $\left[\begin{array}{c|cc} 12 & 1 & 0 \\ 5 & 0 & 1 \\ 2 & 1 & -2 \\ 1 & -2 & 5 \end{array}\right]$ 得 $(-2) \times 12 + 5 \times 5 = 1$ 故得 $c = 3 \times (-2) \times 12 + 5 \times 5 \times 5 = 53$ 符合所求。

最後提醒！Chinese Remainder Theorem 當 m_i 不是兩兩互質時, 給定任意的 $c_1, \ldots, c_r$ 不見得可找到一個整數 c 使得 $c \equiv c_i \pmod{m_i}$ 對所有的 $i \in \{1, \ldots, r\}$ 都成立. 例如當 $m_1 = 4$, $m_2 = 6$ 時若考慮 $c_1 = 1$, $c_2 = 2$, 則不可能找到一整數 c 同時滿足 $c \equiv 1 \pmod{4}$ 且 $c \equiv 2 \pmod{6}$. 這是因為若 $c \equiv 1 \pmod{4}$ 表示 c 為 $4k+1$ 的形式, 故必為奇數. 然而若 $c \equiv 2 \pmod{6}$, 則 c 為 $6k+2$ 之形式, 必為偶數. 因此當然不可能找到一整數是奇數又是偶數.

Exercise 3.9. 試利用以下兩種方法找到所有可能的整數 c 滿足

$$\begin{cases} c \equiv 1 \pmod{3} \\ c \equiv 2 \pmod{4} \\ c \equiv 3 \pmod{5} \\ c \equiv 4 \pmod{7} \end{cases}$$

(1) 利用 Theorem 3.5.2 的證明所用的方法，先找 $e_1, e_2, e_3, e_4 \in \mathbb{Z}$ 再求出 c。

(2) 先分別解 $\begin{cases} c_1 \equiv 1 \pmod{3} \\ c_1 \equiv 2 \pmod{4} \end{cases}$ 以及 $\begin{cases} c_2 \equiv 3 \pmod{5} \\ c_2 \equiv 4 \pmod{7} \end{cases}$ 再求出 c。

Exercise 3.10. 中國剩餘定理也可推廣到不互質的情況.

(1) 給定 $c_1, c_2 \in \mathbb{Z}$ 且 m_1, m_2 為大於 1 的整數。試證明：存在整數 c 滿足

$$\begin{cases} c \equiv c_1 \pmod{m_1} \\ c \equiv c_2 \pmod{m_2} \end{cases}$$

若且唯若

$$\gcd(m_1, m_2) \mid c_1 - c_2.$$

並證明若有解則其解在 modulo $\operatorname{lcm}(m_1, m_2)$ 之下唯一.

（Hint：找 e_1, e_2 滿足 $e_i \equiv \gcd(m_1, m_2) \pmod{m_i}$ 且 $e_i \equiv 0 \pmod{m_j}$, for $j \neq i$）

(2) 試求 c 分別滿足以下 congruence:

(a) $\begin{cases} c \equiv 3 \pmod{4} \\ c \equiv 1 \pmod{6} \end{cases}$ (b) $\begin{cases} c \equiv 7 \pmod{16} \\ c \equiv 3 \pmod{24} \end{cases}$

(3)（optional，不考）試將 (1) 的結果推廣到 modulo 更多整數的情形.