基礎數論

李華介

國立台灣師範大學數學系

前言

本講義主要目的是針對大一學生介紹有關整數論一些基本的代數和算數上的性質, 以作為將來學習抽象代數之準備. 基於這樣的理由, 在此我們將不介紹有關於整數論之歷史和典故以及其應用. 對整數論之應用 (尤其在資訊方面的應用) 有興趣的讀者, 我們推薦 Silverman 的「A Friendly Introduction to Number Theory」(Prentice Hall, Third Edition 2006). 相信若對本講義內容有相當認識之後應可輕鬆閱讀這本書.

Chapter 4

Congruence Equations

既然在 modulo m 之下 "$\equiv$" 可以如 "$=$" 一樣運算, 我們同樣的可以探討解方程式的問題. 這樣的方程式就稱為 congruence equation. 本講義中, 我們只討論解單變數的 congruence equation. 這一章中, 我們將探討解 congruence equation 的一般原則, 並討論中國剩餘定理以及解一次的 congruence equation.

4.1. 解 Congruence Equation 的原則

給定一整係數多項式 $f(x)$ (即 $f(x) = c_n x^n + \cdots + c_1 x + c_0$, 其中 $c_i \in \mathbb{Z}$), 由於 $f(x)$ 的係數是整數, 將 x 代任一整數 a 時, $f(a)$ 仍為整數. 因此若給定 $m \in \mathbb{N}$, 我們可以問怎樣的整數 a 會使得 $f(a) \equiv 0 \pmod{m}$ (即 $m | f(a)$). 找這樣所有的整數解就是所謂的解 congruence equation.

給定 $f(x) = c_n x^n + \cdots + c_1 x + c_0$, 其中 $c_i \in \mathbb{Z}$. 若已知對於 $m \in \mathbb{N}$, $a \in \mathbb{Z}$ 是 $f(x) \equiv 0 \pmod{m}$ 的一個解, 即 $f(a) \equiv 0 \pmod{m}$. 假設 $b \equiv a \pmod{m}$, 由 Proposition 3.2.2 知, 對任意 $i \in \mathbb{N}$ 皆有 $b^i \equiv a^i \pmod{m}$. 再由同一 Proposition 知 $c_i b^i \equiv c_i a^i \pmod{m}$, 進而得 $f(b) \equiv f(a) \pmod{m}$. 也就是說, 若 $x = a$ 是 $f(x) \equiv 0 \pmod{m}$ 的一個整數解, 則對任意 $b \in \mathbb{Z}$ 滿足 $b \equiv a \pmod{m}$, $x = b$ 亦為 $f(x) \equiv 0 \pmod{m}$ 的一個解. 所以若 $x = a$ 是 $f(x) \equiv 0 \pmod{m}$ 的一個整數解, 我們通常會說 $x \equiv a \pmod{m}$ 是 $f(x) \equiv 0 \pmod{m}$ 的一個解. 當然還有可能有其他在 modulo m 之下和 a 不同餘的整數會是 $f(x) \equiv 0 \pmod{m}$ 的解. 我們必須把這些解用 modulo m 的同餘類的方式全部寫下, 這樣的表達方法才能將所有的整數解寫下. 所以我們在談 $f(x) \equiv 0 \pmod{m}$ 的解時, 談的是 modulo m 的同餘類, 因此當我們說 $f(x) \equiv 0 \pmod{m}$ 的解的個數時, 談的是在 modulo m 之下有多少的相異同餘類會滿足 $f(x) \equiv 0 \pmod{m}$, 而不是談有多少個整數解.

從這個角度來看, 我們只要列出一個 modulo m 的 complete residue system S, 然後將 S 的元素一一帶入 $f(x)$ 中, 看看哪一些會使得 $f(x) \equiv 0 \pmod{m}$, 那麼就可以找到所有的解了. 不過這方法在 m 很大時就顯得不切實際了. 因此我們希望能發展一套理論, 至少能理解

一些較特殊的 congruence equation 其解的特性. 不過不管怎樣, 我們知道一個 congruence equation 在 modulo m 之下其解的個數至多就是 m.

其實上, 我們之前就已接觸到一些解 congruence equation 的問題了. 在 modulo m 之下找 $a\in\mathbb{Z}$ 的乘法反元素的問題事實上就是在解 $ax\equiv 1 \pmod m$ (即 $ax-1\equiv 0 \pmod m$) 這一個 congruence equation. 由 Proposition 3.2.5 知當 a 和 m 不互質時, 此 congruence equation 無解. 另外加上 Proposition 3.2.3, 我們知道當 a 和 m 互質時此 congruence equation 在 modulo m 之下有唯一解.

再如 Lemma 3.4.2 是討論當 p 是質數時 $x^2\equiv 1 \pmod p$ 的解. 此時由 Lemma 3.4.2 我們知當 p 是奇質數時有兩個解, 分別是 $x\equiv 1 \pmod p$ 和 $x\equiv -1 \pmod p$. 我們提過當 m 不是質數時, 雖然 $x\equiv\pm 1 \pmod m$ 仍為 $x^2\equiv 1 \pmod m$ 這一個 congruence equation 的兩個解, 但此 congruence equation 有可能有多於兩個解. 例如 $x^2\equiv 1 \pmod{15}$ 的解就是 $x\equiv\pm 1 \pmod{15}$ 和 $x\equiv\pm 4 \pmod{15}$ 這 4 個解. 這和我們一般熟知一個 n 次多項式至多有 n 個解不同, 應特別注意.

一個 n 次的實係數多項式至多有 n 個解的原因是因為實係數多項式之間也有所謂的除法原理, 這個原理並不能套用在整係數多項式中. 不過當除式是一個最高次項係數為 1 的整係數多項式時, 仍可套用除法原理. 由於我們並不需要一般的性質, 這裡我們僅探討除式是一次多項式的情況.

Lemma 4.1.1. 假設 $f(x)$ 是一個 n 次 $(n\geq 1)$ 的整係數多項式且 $a\in\mathbb{Z}$. 則存在一個 $n-1$ 次的整係數多項式 $h(x)$ 以及 $r\in\mathbb{Z}$ 滿足

$$f(x)=(x-a)h(x)+r.$$

Proof. 對 $f(x)$ 的次數 n 做數學歸納法. 假設 $f(x)$ 是 1 次多項式, 即 $f(x)=c_1x+c_0$, 則令 $h(x)=c_1$ 且 $r=ac_1+c_0$, 我們得 $(x-a)h(x)+r=f(x)$.

應用數學歸納法, 假設對次數 $n<k$ 的整係數多項式 $g(x)$, 皆存在 $n-1$ 次的整係數多項式 $h_0(x)$ 以及 $r_0\in\mathbb{Z}$ 使得 $g(x)=(x-a)h_0(x)+r_0$. 現考慮 $f(x)$ 的次數 $n=k$ 的情形, 也就是說 $f(x)=c_kx^k+c_{k-1}x^{k-1}+\cdots+c_1x+c_0$, 其中 $c_i\in\mathbb{Z}$ 且 $c_k\neq 0$. 令 $g(x)=f(x)-(x-a)c_kx^{k-1}$, 則 $g(x)=(c_{k-1}+c_ka)x^{k-1}+\cdots c_1x+c_0$ 是一個次數小於 k 的整係數多項式. 故套用歸納假設知存在一次數小於 $k-1$ 的整係數多項式 $h_0(x)$ 以及 $r_0\in\mathbb{Z}$ 使得 $g(x)=(x-a)h_0(x)+r_0$. 也就是說 $f(x)=(x-a)c_kx^{k-1}+(x-a)h_0(x)+r_0$. 故令 $h(x)=c_kx^{k-1}+h_0(x)$ 以及 $r=r_0$, 我們有 $h(x)$ 是一個次數為 $k-1$ 的整係數多項式且 $r\in\mathbb{Z}$ 滿足 $f(x)=(x-a)h(x)+r$. □

套用 Lemma 4.1.1, 我們可以證得當 p 是一質數時在 modulo p 之下一個 n 次的 congruence equation 最多有 n 個解. 不過首先我們需對一個 congruence equation 的次數下個定義.

Definition 4.1.2. 假設 $f(x)=c_nx^n+\cdots+c_1x+c_0$ 是一個整係數多項式, 給定 $m\in\mathbb{N}$.

(1) 若 $m\nmid c_n$, 則我們稱 $f(x)$ 在 modulo m 之下是一個次數 (degree) 為 n 的多項式.

(2) 若 $m \nmid c_r$ 但 $m|c_i$, for $r < i \leq n$, 則我們稱 $f(x)$ 在 modulo m 之下是一個次數為 r 的多項式.

如果一個整係數多項式 $g(x)$ 其在 modulo m 之下之次數為 n, 則我們稱 $g(x) \equiv 0 \pmod{m}$ 是一個 n 次的 congruence equation.

由此定義我們知道若 $f(x)$ 是一個在 modulo m 之下次數為 n 的整係數多項式, 有可能 $f(x)$ 本身的次數是大於 n 的. 不過我們可以找到一個次數為 n 的整係數多項式 $g(x)$ (例如刪去 $f(x)$ 中可以被 m 整除的項) 使得對任一整數 a, 皆有 $f(a) \equiv g(a) \pmod{m}$. 所以 $f(x) \equiv 0 \pmod{m}$ 的解會和 $g(x) \equiv 0 \pmod{m}$ 相同. 由於我們只關心 congruence equation 的解, 所以今後當討論一個 n 次的 congruence equation $f(x) \equiv 0 \pmod{m}$ 時, 不失一般性, 我們就直接假設 $f(x)$ 的次數為 n.

Theorem 4.1.3 (Lagrange)**.** 給定一質數 p 以及一整係數多項式 $f(x)$. 如果在 *modulo* p 之下 $f(x) \equiv 0 \pmod{p}$ 是一個次數為 n 的多項式, 則 $f(x) \equiv 0 \pmod{p}$ 在 *modulo* p 之下至多有 n 個解.

Proof. 不失一般性, 我們假設 $f(x) = c_n x^n + \cdots + c_1 x + c_0$, 其中 $p \nmid c_n$. 我們對 n 做歸納法. 首先當 $f(x) = c_1 x + c_0$ 是一次整係數多項式時, 假設 $x \equiv a \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的一個解. 現另假設 $x \equiv b \pmod{p}$ 也是一個解, 亦即 $c_1 a + c_0 \equiv c_1 b + c_0 \pmod{p}$. 因為 $\gcd(p, c_1) = 1$, 由 Lemma 3.2.4 可得 $a \equiv b \pmod{p}$. 也就是說 $n = 1$ 時至多有一個解.

用歸納假設當 $n < k$ 時一個 n 次的 congruence equation 至多有 n 個解. 現考慮 $n = k$ 的情形. 若 $x \equiv a \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的一個解, 利用 Lemma 4.1.1 知存在一個次數為 $k-1$ 的整係數多項式 $h(x)$ 以及 $r \in \mathbb{Z}$ 使得 $f(x) = (x-a)h(x) + r$. 依假設 $x \equiv a \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的一個解, 即 $f(a) \equiv 0 \pmod{p}$, 將 a 代入得 $f(a) = r \equiv 0 \pmod{p}$. 現另假設 $x \equiv b \pmod{p}$ 也是一個解, 則由 $f(b) = (b-a)h(b) + r$ 知 $(b-a)h(b) \equiv 0 \pmod{p}$. 換言之, 若 $b \not\equiv a \pmod{p}$, 即 $p \nmid (b-a)$, 則由 Lemma 1.4.2 知, $p|h(b)$, 也就是說 $x \equiv b \pmod{p}$ 是 $h(x) \equiv 0 \pmod{p}$ 的一個解. 因此我們知道 k 次 congruence equation $f(x) \equiv 0 \pmod{p}$ 的解為 $x \equiv a \pmod{p}$ 或 $h(x) \equiv 0 \pmod{p}$ 的解. 然而 $h(x) \equiv 0 \pmod{p}$ 是一個次數小於 k 的 congruence equation, 故依歸納法假設其至多有 $k-1$ 個解, 故得證 $f(x) \equiv 0 \pmod{p}$ 至多有 k 個解. □

最後我們再次提醒, 要解 congruence equation $f(x) \equiv 0 \pmod{m}$ 需將解的所有情況寫下來, 一般會將解以 $x \equiv a \pmod{m}$ 這樣的形式寫下來. 不過有時為了方便我們會將解以 modulo 別的數的方式寫下. 例如解 $x^2 \equiv 1 \pmod{8}$, 我們發現所有的奇數都滿足, 所以為了方便我們可以將解以 $x \equiv 1 \pmod{2}$ 寫下. 不過要注意這種形式寫下後當我們提及解的個數時需提及在 modulo 什麼之下的解的個數. 例如在此例中我們可以說 $x^2 \equiv 1 \pmod{8}$ 在 modulo 8 之下有 $x \equiv 1, 3, 5, 7 \pmod{8}$, 4 個解, 也可以說在 modulo 2 之下有一個解.

4.2. 兩個常用的方法

我們介紹兩種常用的方法將一個給定的 congruence equation 化成簡單一點的形式, 再來求解.

在這一節中我們都假設 $f(x)=a_nx^n+\cdots+a_1x+a_0$, 其中 $a_i\in\mathbb{Z}$, 而 $m\in\mathbb{N}$ 是一給定的正整數. 我們要談論 $f(x)\equiv 0 \pmod m$ 這一個 congruence equation.

第一種情形是這樣的: 如果 d 是 $a_n,\ldots,a_1,a_0$ 以及 m 的正公因數. 也就是說我們可以將 a_i 及 m 寫成 $a_n=a_n'd,\ldots,a_1=a_1'd,a_0=a_0'd$ 以及 $m=m'd$, 其中這些 $a_i'\in\mathbb{Z}$ 且 $m'\in\mathbb{N}$. 令 $g(x)=a_n'x^n+\cdots a_1'x+a_0'$, 我們來探討 $f(x)\equiv 0 \pmod m$ 及 $g(x)\equiv 0 \pmod{m'}$ 這兩個 congruence equation 之間的關係.

Proposition 4.2.1. 給定 $m\in\mathbb{N}$ 及 $f(x)=a_nx^n+\cdots+a_1x+a_0$, 其中 $a_i\in\mathbb{Z}$. 假設 d 是 $a_n,\ldots,a_1,a_0$ 及 m 的正公因數且 $a_n=a_n'd,\ldots,a_1=a_1'd,a_0=a_0'd$ 以及 $m=m'd$. 令 $g(x)=a_n'x^n+\cdots+a_1'x+a_0'$.

若 $x\equiv c \pmod{m'}$ 是 $g(x)\equiv 0 \pmod{m'}$ 的一個解, 則對任意 $t\in\mathbb{Z}$, $x\equiv c+m't \pmod m$ 為 $f(x)\equiv 0 \pmod m$ 的解. 另一方面, 若 $g(x)\equiv 0 \pmod{m'}$ 無解, 則 $f(x)\equiv 0 \pmod m$ 無解.

Proof. $x\equiv c \pmod{m'}$ 為 $g(x)\equiv 0 \pmod{m'}$ 的一個解, 表示 $m'|a_n'c^n+\cdots+a_1'c+a_0'$. 因此可得 $m'd|a_n'dc^n+\cdots+a_1'dc+a_0'd$, 也就是說 $m|a_nc^n+\cdots a_1c+a_0$. 因此 $x\equiv c \pmod m$ 是 $f(x)\equiv 0 \pmod m$ 的一個解.

現對任意 $t\in\mathbb{Z}$ 考慮 $c'=c+m't$. 由於 $c\equiv c' \pmod{m'}$, 知 $x\equiv c' \pmod{m'}$ 也是 $g(x)\equiv 0 \pmod{m'}$ 的一個解. 故套用上面的討論於 $c'=c+m't$ 的情形, 我們知 $x\equiv c+m't \pmod m$ 是 $f(x)\equiv 0 \pmod m$ 的一個解. 因此證明了對任意 $t\in\mathbb{Z}$, $x\equiv c+m't \pmod m$ 也會是 $f(x)\equiv 0 \pmod m$ 的一個解.

另一方面, 若 $x\equiv c \pmod m$ 為 $f(x)\equiv 0 \pmod m$ 的一個解, 即 $m|a_nc^n+\cdots+a_1c+a_0$, 則 $m'|a_n'c^n+\cdots+a_1'c+a_0'$. 也就是說 $x\equiv c \pmod{m'}$ 為 $g(x)\equiv 0 \pmod{m'}$ 的一個解. 因此若 $g(x)\equiv 0 \pmod{m'}$ 無解, 則 $f(x)\equiv 0 \pmod m$ 亦無解. □

Proposition 4.2.1 告訴我們, 如果 $x\equiv c \pmod{m'}$ 是 $g(x)\equiv 0 \pmod{m'}$ 的一個解, 則對任意 $t\in\mathbb{Z}$, $x\equiv c+m't \pmod m$ 便會是 $f(x)\equiv 0 \pmod m$ 的一個解. 不過這裡由於我們要考慮在 modulo m 的情況, 很多解是重複的. 事實上若 $t\equiv t' \pmod d$, 則由 $d|t-t'$, 可得 $dm'|m'(t-t')$. 也就是說 $c+m't\equiv c+m't' \pmod m$. 因此我們只要考慮 $x\equiv c+m't \pmod m$ 其中 $0\le t\le d-1$, 就可以了. 也就是說, 在 modulo m' 之下 $g(x)\equiv 0 \pmod{m'}$ 的一個解, 便會對應到 $f(x)\equiv 0 \pmod m$ 在 modulo m 之下 d 個解. 然而每個 $f(x)\equiv 0 \pmod m$ 的解都會是 $g(x)\equiv 0 \pmod{m'}$ 的解, 因此有以下的結果.

Corollary 4.2.2. 給定 $m\in\mathbb{N}$ 及 $f(x)=a_nx^n+\cdots+a_1x+a_0$, 其中 $a_i\in\mathbb{Z}$. 假設 d 是 $a_n,\ldots,a_1,a_0$ 及 m 的正公因數且 $a_n=a_n'd,\ldots,a_1=a_1'd,a_0=a_0'd$ 以及 $m=m'd$. 令 $g(x)=$

$a'_n x^n + \cdots + a'_1 x + a'_0$. 若 $g(x) \equiv 0 \pmod{m'}$ 在 *modulo* m' 之下有 k 個解, 則 *congruence equation* $f(x) \equiv 0 \pmod{m}$ 在 *modulo* m 之下會有 kd 個解.

Proposition 4.2.1 將一個 modulo m 的 congruence equation 化成一個 modulo 比較小的 m' 的 congruence equation. 這樣一來由於在 modulo m' 之下要考慮的數較少, 應該將原來的問題簡化了. 然而若 $a_n, \ldots, a_1, a_0$ 和 m 是互質的, 我們仍然可以考慮 modulo 較小的值看看有沒有解. 事實上, 我們有以下之結果.

Lemma 4.2.3. 給定 $m \in \mathbb{N}$ 及一整係數多項式 $f(x)$. 若 $m' | m$ 且 $f(x) \equiv 0 \pmod{m'}$ 無解, 則 $f(x) \equiv 0 \pmod{m}$ 亦無解.

Proof. 假設 $f(x) \equiv 0 \pmod{m}$ 有解且 $x \equiv c \pmod{m}$ 為其中一解, 即 $m | f(c)$. 由於 $m' | m$, 知 $m' | f(c)$, 也就是說 $x \equiv c \pmod{m'}$ 為 $f(x) \equiv 0 \pmod{m'}$ 之一解. 此與假設 $f(x) \equiv 0 \pmod{m'}$ 無解矛盾, 故得證 $f(x) \equiv 0 \pmod{m}$ 無解. □

Lemma 4.2.3 和 Proposition 4.2.1 不同之處在於 Proposition 4.2.1 將原多項式各係數除以公因數後考慮 modulo m' 之解, 而且可利用其解得到原多項式在 modulo m 之解, 而 Lemma 4.2.3 並沒有改變多項式, 且僅知原多項式在 modulo 比較小的 m' 之下無解可推得原多項式在 modulo m 之下無解. 但無從判斷在 modulo m' 之下有解是否可得在 modulo m 之下有解, 而且也無從推得解之形式. 不過若我們多考慮幾個 m 的因數所得的 congruence equations, 確實可以幫我們得知解之情形. 這就是我們要探討的第二種方法.

這一種常用的方法就是先將 m 寫成質因數的分解, 即 $m = p_1^{n_1} \cdots p_r^{n_r}$, 其中這些 p_i 為相異質數. 接著僅要探討對所有 $i = 1, \ldots, r$, $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 之解的情形就可, 因為我們有以下之結果.

Proposition 4.2.4. 假設 $m = p_1^{n_1} \cdots p_r^{n_r}$, 其中這些 p_i 為相異質數且 $f(x)$ 為一整係數多項式. 若存在 $i \in \{1, \ldots, r\}$, 使得 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 無解, 則 $f(x) \equiv 0 \pmod{m}$ 無解. 另一方面, $x \equiv c \pmod{m}$ 為 $f(x) \equiv 0 \pmod{m}$ 之一個解若且唯若對任意 $i \in \{1, \ldots, r\}$, $x \equiv c \pmod{p_i^{n_i}}$ 皆為 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 的解.

Proof. 首先, 由於 $p_i^{n_i} | m$, 因此套用 Lemma 4.2.3 知, 若 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 無解, 則 $f(x) \equiv 0 \pmod{m}$ 無解.

現假設 $x \equiv c \pmod{m}$ 為 $f(x) \equiv 0 \pmod{m}$ 的一個解, 也就是說 $m | f(c)$, 由於對任意 $i \in \{1, \ldots, r\}$ 皆有 $p_i^{n_i} | m$, 知 $p_i^{n_i} | f(c)$. 因此知對所有的 $i \in \{1, \ldots, r\}$, $x \equiv c \pmod{p_i^{n_i}}$ 為 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 的解.

反之, 若對所有 $i \in \{1, \ldots, r\}$, $x \equiv c \pmod{p_i^{n_i}}$ 皆為 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 的解. 即 $p_i^{n_i} | f(c)$. 則由於這些 $p_i^{n_i}$ 是兩兩互質的, 利用 Proposition 1.2.6(2) 知 $p_1^{n_1} \cdots p_r^{n_r} | f(c)$, 亦即 $m | f(c)$. 故得證 $x \equiv c \pmod{m}$ 為 $f(x) \equiv 0 \pmod{m}$ 的一個解. □

Proposition 4.2.4 告訴我們, 若有一個 p_i 使得 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 無解, 那麼 $f(x) \equiv 0 \pmod{m}$ 就無解. 但是如果對所有的 p_i, $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 皆有解, 是否表示 $f(x) \equiv 0$

(mod m) 有解呢? 答案是肯定的. 這是因為雖然對任意的 p_i 解得的解未必相同, 但利用以後會探討的中國剩餘定理可找到一整數同時滿足 modulo $p_i^{n_i}$ 下每個解的形式, 因此可由 Proposition 4.2.4 得知 $f(x) \equiv 0 \pmod{m}$ 有解. 關於此部份以後在探討中國剩餘定理時我們會再說明.

4.3. 一次的 Congruence Equations

我們探討最簡單的一種 congruence equation, 也就是一次的 congruence equation. 我們將會知道其解的個數及解的形式.

給定 $m \in \mathbb{N}$ 所謂 modulo m 的一次 congruence equation 即 $ax \equiv b \pmod{m}$ 這樣形式的 congruence equation, 其中 $a, b \in \mathbb{Z}$ 且 $m \nmid a$. 首先我們來看看如何判別一個一次的 congruence equation 是否有解.

Proposition 4.3.1. 給定 $m \in \mathbb{N}$. 考慮一次的 *congruence equation* $ax \equiv b \pmod{m}$, 其中 $m \nmid a$. 假設 $d = \gcd(m,a)$. 則 $d|b$ 若且唯若 $ax \equiv b \pmod{m}$ 有解.

Proof. 依假設 $d = \gcd(m,a)$, 故 $d \mid m$, 我們可以考慮 congruence equation $ax \equiv b \pmod{d}$. 又由於我們有 $d \mid a$, 因此在 modulo d 之下得 $ax \equiv 0x \pmod{d}$. 現若 $d \nmid b$, 亦即 $b \not\equiv 0 \pmod{d}$, 得 congruence equation $ax \equiv b \pmod{d}$ (即 $0x \equiv b \pmod{d}$) 無解. 故由 Lemma 4.2.3 知 $ax \equiv b \pmod{m}$ 無解.

反之, 若 $d|b$, 則可得 $d = \gcd(d,b) = \gcd(\gcd(m,a),b)$. 令 $a = a'd, b = b'd, m = m'd$. 由 Proposition 4.2.1 知 $ax \equiv b \pmod{m}$ 有解若且唯若 $a'x \equiv b' \pmod{m'}$ 有解. 現由於 $\gcd(a,m) = d$ 我們有 $\gcd(a',m') = 1$, 依 Proposition 3.2.5 知存在 $e \in \mathbb{Z}$ 使得 $a'e \equiv 1 \pmod{m'}$. 故將 $a'x \equiv b' \pmod{m'}$ 之兩邊乘上 e 得

$$x \equiv a'ex \equiv b'e \pmod{m'}.$$

因此可得 $x \equiv b'e \pmod{m'}$ 為 $a'x \equiv b' \pmod{m'}$ 的一個解, 因而由 Proposition 4.2.1 得知 $x \equiv b'e \pmod{m}$ 亦為 $ax \equiv b \pmod{m}$ 的一個解. □

在 Proposition 4.3.1 的證明中, 我們找到 $a'x \equiv b' \pmod{m'}$ 在 modulo m' 之下的一組解. 事實上, 由於 $\gcd(a',m') = 1$, $a'x \equiv b' \pmod{m'}$ 在 modulo m' 之下的解事實上是唯一的.

Lemma 4.3.2. 給定 $m \in \mathbb{N}$. 考慮一次的 *congruence equation* $ax \equiv b \pmod{m}$. 若 $\gcd(a,m) = 1$, 則 $ax \equiv b \pmod{m}$ 在 *modulo* m 之下其解唯一.

Proof. 假設 $x \equiv c \pmod{m}$ 和 $x \equiv c' \pmod{m}$ 皆為 $ax \equiv b \pmod{m}$ 的一個解, 則由 $ac \equiv b \equiv ac' \pmod{m}$ 得 $m \mid a(c-c')$. 再由 $\gcd(m,a) = 1$, 得 $m \mid c - c'$ (Proposition 1.2.6), 亦即 $c \equiv c' \pmod{m}$. □

利用 Lemma 4.3.2 我們馬上可以知道若 congruence equation $ax \equiv b \pmod{m}$ 有解, 則其在 modulo m 之下解的個數.

Proposition 4.3.3. 給定 $m \in \mathbb{N}$. 考慮一次的 *congruence equation* $ax \equiv b \pmod{m}$. 若 $d = \gcd(m,a)$ 且 $d \mid b$, 則 $ax \equiv b \pmod{m}$ 在 *modulo* m 之下共有 d 個解. 事實上, 若 $x \equiv c \pmod{m/d}$ 是 $(a/d)x \equiv (b/d) \pmod{m/d}$ 的一個解, 則 $ax \equiv b \pmod{m}$ 在 *modulo* m 之下所有的解為

$$x = c + t\frac{m}{d}, \quad t = 0, 1, \ldots, d-1.$$

Proof. 若 $d|b$, 則可得 $d = \gcd(d,b) = \gcd(\gcd(m,a),b)$. 令 $a = a'd, b = b'd, m = m'd$. 由於 $\gcd(a',m') = 1$, 依 Lemma 4.3.2 我們知 $a'x \equiv b' \pmod{m'}$ 在 modulo m' 之下其解唯一. 現若 $x \equiv c \pmod{m'}$ 是其解, 則由 Proposition 4.2.1 知 $ax \equiv b \pmod{m}$ 的解皆為 $x = c + tm'$ 其中 $t \in \mathbb{Z}$. 再由 Corollary 4.2.2 得知在 modulo m 之下 $ax \equiv b \pmod{m}$ 共有 d 個解, 即 $x = c + t(m/d), t = 0, 1, \ldots, d-1$. □

為了方便, 我們特別將 Proposition 4.3.1 和 Proposition 4.3.3 綜合成以下的定理.

Theorem 4.3.4. 給定 $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ 考慮一次的 *congruence equation* $ax \equiv b \pmod{m}$. 令 $d = \gcd(m,a)$.

(1) 若 $d \nmid b$, 則 $ax \equiv b \pmod{m}$ 無解.

(2) 若 $d \nmid b$, 則 $ax \equiv b \pmod{m}$, 在 *modulo* m 之下有 d 個解. 且若已知 $x \equiv c \pmod{m}$ 為一解, 則

$$x \equiv c + \frac{m}{d}t, \quad t = 0, 1, \ldots, d-1$$

為 $ax \equiv b \pmod{m}$ 在 *modulo* m 之下所有的解.

特別地, 當 a 和 m 互質時, 對於所有 $b \in \mathbb{Z}$, $ax \equiv b \pmod{m}$ 皆有解, 且其解在 *modulo* m 之下是唯一的.

Example 4.3.5. 我們要解 $16x \equiv 8 \pmod{52}$. 因 $\gcd(52,16) = 4$ 且 $4|8$, 故知此 congruence equation 必有解, 且在 modulo 28 之下共有 4 個解.

首先我們先解 $4x \equiv 2 \pmod{13}$. 由於 $4 \times 10 \equiv 1 \pmod{13}$, 我們得知 $x \equiv 2 \times 10 \equiv 7 \pmod{13}$ 為 $4x \equiv 2 \pmod{13}$ 的一個解. 因而得 $x \equiv 7 \pmod{52}$ 為 $16x \equiv 8 \pmod{52}$ 的一個解 (即 $16 \times 7 = 112 = 52 \times 2 + 8$).

至於其他的解, 由於 $52/4 = 13$ 故依 Theorem 4.3.4 知在 modulo 52 之下 $x \equiv 7, 20, 33, 46 \pmod{52}$ 為 $16x \equiv 8 \pmod{52}$ 的所有解.

最後我們要補充說明, 由 Theorem 4.3.4 知道只要找到 $ax \equiv b \pmod{m}$ 的一個解, 就可以找到其在 modulo m 之下所有的解. 由於此時 $d = \gcd(a,m) \mid b$. 我們也可以利用輾轉相除法先求出 $ax + my = b$ 的一組整數解 $x = r, y = s$. 此時由於 $ar \equiv b \pmod{m}$ 由此可得 $x \equiv r \pmod{m}$ 為 $ax \equiv b \pmod{m}$ 的一個解.

4.4. Chinese Remainder Theorem

假設 $m = p_1^{n_1} \cdots p_r^{n_r}$ 其中 p_i 為相異質數且 $f(x)$ 是一個整係數多項式. Proposition 4.2.4 告訴我們若對所有 $i \in \{1,\ldots,r\}$, $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 皆有解且有共同解, 則 $f(x) \equiv 0 \pmod{m}$ 便有解. 如何找到共同解呢? 中國剩餘定理 (Chinese Remainder Theorem) 告訴我們只要個別地將 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 的解找到, 就可得到共同解.

Theorem 4.4.1 (Chinese Remainder Theorem)**.** 給定一組 $m_1,\ldots,m_r \in \mathbb{N}$ 其中這些 m_i 皆兩兩互質 (即當 $i \neq j$ 時, $\gcd(m_i,m_j) = 1$). 則對任意的一組 $c_1,\ldots,c_r \in \mathbb{Z}$ 皆可找到一整數 c 使得

$$c \equiv c_i \pmod{m_i}, \forall i \in \{1,\ldots,r\}.$$

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) 不失一般性 (變換一下 m_i 的順序), 我們僅需證明 $\gcd(M_1,m_1) = 1$. 假設 M_1,m_1 不互質, 即存在一質數 p 使得 $p|M_1$ 且 $p|m_1$. 然而依定義 $M_1 = m_2 \cdots m_r$, 故由 Corollary 1.4.3 知存在 $i \in \{2,\ldots,r\}$ 使得 $p|m_i$. 但是 $i \neq 1$, 依假設 $\gcd(m_1,m_i) = 1$, 故 $p|m_1$ 且 $p|m_i$ 和 m_1,m_i 互質相矛盾, 故得證 $\gcd(M_1,m_1) = 1$.

接下來我們想要找到一組 $t_1,\ldots,t_r \in \mathbb{Z}$ 使得對所有的 $i \in \{1,\ldots,r\}$,

$$t = c_1 M_1 t_1 + \cdots + c_r M_r t_r$$

皆滿足 $t \equiv c_i \pmod{m_i}$. 然而對任何的一組 $t_1,\ldots,t_r \in \mathbb{Z}$ 以及一給定的 $i \in \{1,\ldots,r\}$, 由 (1) (即 $m_i | M_j$ for $i \neq j$) 我們皆有 $t \equiv c_i M_i t_i \pmod{m_i}$. 故我們僅需找到 $t_i \in \mathbb{Z}$ 使得 $c_i M_i t_i \equiv c_i \pmod{m_i}$ 即可. 然而由 (2) (即 $\gcd(M_i,m_i) = 1$) 以及 Proposition 3.2.5 知存在 $e_i \in \mathbb{Z}$ 使得 $M_i e_i \equiv 1 \pmod{m_i}$, 故若令 $t_i = e_i$, 則得 $t \equiv c_i M_i e_i \equiv c_i \pmod{m_i}$. 因此對所有 $i \in \{1,\ldots,r\}$, 我們先找到 e_i 使得 $M_i e_i \equiv 1 \pmod{m_i}$, 再令 $c = c_1 M_1 e_1 + \cdots + c_r M_r e_r$, 則可得 $c \equiv c_i \pmod{m_i}, \forall i \in \{1,\ldots,r\}$. □

要注意! 當這些 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.

一般來說我們可以將中國剩餘定理看成是解如

$$\begin{cases} x \equiv c_1 & \pmod{m_1} \\ x \equiv c_2 & \pmod{m_2} \\ \quad\vdots & \quad\vdots \\ x \equiv c_r & \pmod{m_r} \end{cases}$$

這樣的聯立方程式. 一般來說聯立方程式是要找到一個共同解同時符合這 r 個式子感覺起來較難. 而在 Theorem 4.4.1 的證明中, 大家可以看出參數 $t_1,\dots t_r$ 的設定, 就是要把這 r 個聯立的式子化成 r 個獨立的式子個別解出 t_i 來, 自然就變簡單了. 我們來看看以下的例子.

Example 4.4.2. 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 $c\equiv c_i \pmod{m_i}, \forall i\in\{1,2,3\}$. 也就是說找到 c 同時滿足

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

依照 Theorem 4.4.1 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 $e_1\in\mathbb{Z}$ 使得 $M_1e_1\equiv 1 \pmod{m_1}$, 即 $20e_1\equiv 1 \pmod 3$, 也就是說滿足 $2e_1\equiv 1 \pmod 3$. 由此找到 $e_1=2$. 同理我們要找到 e_2,e_3 分別滿足 $15e_2\equiv 1 \pmod 4$ (即 $3e_2\equiv 1 \pmod 4$) 以及 $12e_3\equiv 1 \pmod 5$ (即 $2e_3\equiv 1 \pmod 5$). 可得 $e_2=3$ 和 $e_3=3$ 分別滿足上式. 故令 $c=2\times 20\times 2+1\times 15\times 3+3\times 12\times 3=233$ 滿足 $233\equiv 2 \pmod 3$, $233\equiv 1 \pmod 4$ 以及 $233\equiv 3 \pmod 5$.

前面提過, 給定 $m\in\mathbb{N}$, 假設 $m=p_1^{n_1}\cdots p_r^{n_r}$, 其中 p_i 為相異質數. 如果 $f(x)$ 是一個整係數多項式, 要解 $f(x)\equiv 0 \pmod m$, 我們可以先對每個 p_i 考慮解 $f(x)\equiv 0 \pmod{p_i^{n_i}}$. 如果有一個 p_i 發生 $f(x)\equiv 0 \pmod{p_i^{n_i}}$ 無解的情況, 那麼依 Proposition 4.2.4 知 $f(x)\equiv 0 \pmod m$ 無解. 如果每一個 p_i 皆會使得 $f(x)\equiv 0 \pmod{p_i^{n_i}}$, 則依 Proposition 4.2.4 知, 需解聯立方程式

$$\begin{cases} f(x)\equiv 0 & \pmod{p_1^{n_1}} \\ f(x)\equiv 0 & \pmod{p_2^{n_2}} \\ \quad\vdots & \quad\vdots \\ f(x)\equiv 0 & \pmod{p_r^{n_r}} \end{cases}$$

有一共同解才可得 $f(x)\equiv 0 \pmod m$ 的解. 解聯立方程是困難的, 而中國剩餘定理告訴我們可以不必考慮解聯立式子, 先個別將解求出便可得到共同的解.

Corollary 4.4.3. 假設 $m=p_1^{n_1}\cdots p_r^{n_r}$, 其中這些 p_i 為相異質數且 $f(x)$ 為一整係數多項式. 則對任意 $i\in\{1,\dots,r\}$, $f(x)\equiv 0 \pmod{p_i^{n_i}}$ 皆有解若且唯若 $f(x)\equiv 0 \pmod m$ 有解.

Proof. 依 Proposition 4.2.4 知, 如果 $f(x)\equiv 0 \pmod m$ 有解, 則對任意 $i\in\{1,\dots,r\}$, $f(x)\equiv 0 \pmod{p_i^{n_i}}$ 皆有解.

現假設對任意 $i\in\{1,\dots,r\}$, $f(x)\equiv 0 \pmod{p_i^{n_i}}$ 皆有解且 $x\equiv c_i \pmod{p_i^{n_i}}$ 為其一解. 由於這些 $p_i^{n_i}$ 是兩兩互質的故依 Theorem 4.4.1 知, 存在 $c\in\mathbb{Z}$ 滿足對任意 $i\in\{1,\dots,r\}$ 皆有 $c\equiv c_i \pmod{p_i^{n_i}}$. 也就是說任意 $i\in\{1,\dots,r\}$, $x\equiv c \pmod{p_i^{n_i}}$ 為 $f(x)\equiv 0 \pmod{p_i^{n_i}}$ 之一解. 故再利用 Proposition 4.2.4 得知 $x\equiv c \pmod m$ 為 $f(x)\equiv 0 \pmod m$ 之一解. □

我們就來看一個這方面的簡單例子. 雖然底下的例子可以直接代數字得到解答, 但是我們只是希望利用此例來講解這裡所用的概念, 所以希望大家了解應著重於如何應用所學的方法而不在於解答為何.

Example 4.4.4. 我們來解 $x^2 \equiv 1 \pmod{15}$. 依前面結果知我們可以分別考慮 $x^2 \equiv 1 \pmod 3$ 及 $x^2 \equiv 1 \pmod 5$ 的解. 因為 3 和 5 皆為質數, 依 Lemma 3.4.2 知 $x \equiv \pm 1 \pmod 3$ 和 $x \equiv \pm 1 \pmod 5$ 分別為 $x^2 \equiv 1 \pmod 3$ 和 $x^2 \equiv 1 \pmod 5$ 之解. 因此我們要找到以下的四個聯立的 congruence equation:

$$(1)\begin{cases} x \equiv 1 & \pmod 3 \\ x \equiv 1 & \pmod 5 \end{cases}, (2)\begin{cases} x \equiv -1 & \pmod 3 \\ x \equiv -1 & \pmod 5 \end{cases},$$

$$(3)\begin{cases} x \equiv -1 & \pmod 3 \\ x \equiv 1 & \pmod 5 \end{cases}, (4)\begin{cases} x \equiv 1 & \pmod 3 \\ x \equiv -1 & \pmod 5 \end{cases}.$$

(1) 和 (2) 我們很容易看出分別取整數 1 和 -1 就可分別滿足 (1) 和 (2). 而 11 可以滿足 (3), 4 可以滿足 (4). 所以由 Proposition 4.2.4 我們知 $x \equiv 1, -1, 11, 4 \pmod{15}$ 都為 $x^2 \equiv 1 \pmod{15}$ 的解. 我們找到 $x^2 \equiv 1 \pmod{15}$ 在 modulo 15 之下的 4 個解, 並不表示就只有這 4 個解. 不過大家可以自行驗證一下在 modulo 15 之下確實僅有這 4 個解.

在上個例子中我們解出 $x^2 \equiv 1 \pmod{15}$ 在 modulo 15 之下的 4 個解但不敢確定是否僅有這 4 解是因為我們不知在利用中國剩餘定理時, 是否還有其他的解. 也就是說 Theorem 4.4.1 只告訴我們解的存在性, 並未告訴我們是否有其他解. 當然我們都知道會有無窮多解, 但是其他的解如何得知呢? 我們再套用一次常用的老方法, 看看兩個解之間的關係為何, 自然就可將所有的解寫下了.

Theorem 4.4.5. 給定一組 $m_1, \ldots, m_r \in \mathbb{N}$ 其中這些 m_i 皆兩兩互質. 令 $M = m_1 \cdots m_r$, 則對任意的一組 $c_1, \ldots, c_r \in \mathbb{Z}$ 以下聯立的 *congruence equation*

$$\begin{cases} x \equiv c_1 & (\mathrm{mod}\ m_1) \\ x \equiv c_2 & (\mathrm{mod}\ m_2) \\ \quad \vdots & \quad \vdots \\ x \equiv c_r & (\mathrm{mod}\ m_r) \end{cases}$$

在 *modulo* M 之下存在唯一的一個解. 事實上若 $c \in \mathbb{Z}$ 滿足此聯立 *congruence equation,* 則對任意 $c' \in \mathbb{Z}$ 滿足 $c' \equiv c \pmod M$ 皆會滿足此聯立 *congruence equation.*

Proof. Theorem 4.4.1 已證得存在性, 我們要證明在 modulo $m_1 \cdots m_r$ 之下其解唯一.

假設 $c, c' \in \mathbb{Z}$ 皆滿足以上聯立的 congruence equation. 也就是說對任意 $i \in \{1, \ldots, r\}$ 我們皆有 $c \equiv c_i \pmod{m_i}$ 且 $c' \equiv c_i \pmod{m_i}$. 因此之對任意 $i \in \{1, \ldots, r\}$ 皆有 $m_i | c - c'$. 然而這些 m_i 兩兩互質, 故利用 Proposition 1.2.10(2), 我們得 $m_1 \cdots m_r | c - c'$, 即 $c \equiv c' \pmod M$. 也就是說在 modulo M 之下其解唯一.

另一方面, 若 c 滿足聯立 congruence equation 且 $c' \in \mathbb{Z}$ 滿足 $c' \equiv c \pmod M$, 則由於對任意 $i \in \{1, \ldots, r\}$, $m_i | M$, 故知 $c' \equiv c \equiv c_i \pmod{m_i}$. 亦即 c' 滿足此聯立 congruence equation. □

例如在 Example 4.4.2 中, 我們知道 $x = 233$ 滿足

$$\begin{cases} x \equiv 2 & (\mathrm{mod}\ 3) \\ x \equiv 1 & (\mathrm{mod}\ 4) \\ x \equiv 3 & (\mathrm{mod}\ 5) \end{cases}$$

這一組聯立的 congruence equation, 所以由 Theorem 4.4.5 知任意的整數 c 滿足 $c \equiv 233 \equiv 53 \pmod{60}$ 都可以滿足這一組聯立 congruence equation. 當然了也僅有滿足 $c \equiv 53 \pmod{60}$ 的整數會滿足此聯立 congruence equation.

Theorem 4.4.5 比 Theorem 4.4.1 完整. 因為在 Theorem 4.4.1 中我們僅提及解的存在性, 而 Theorem 4.4.5 提及解在 modulo $m_1 \cdots m_r$ 之下是存在且唯一的, 而且因而可由一解找到所有的解. 有的書不會將兩定理分開來談, 而直接談論較完整的 Theorem 4.4.5 並稱之為 Chinese remainder theorem. 我們將兩定理分開主要是因為想先強調中國剩餘定理解的存在性及如何找到一解.