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, 並用這些原則討論解一次以及二次的 congruence equation.

4.1. 解 Congruence Equation 的原則

給定一整係數多項式 $f(x)$ (即 $f(x)=c_nx^n+\cdots+c_1x+c_0$, 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 $f(x)=c_nx^n+\cdots+c_1x+c_0$, 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 $c_ib^i\equiv c_ia^i \pmod m$, 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, 其中 $n\geq 1$, 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 $f(x)=c_nx^n+\cdots+c_1x+c_0$, 其中 $p\nmid c_n$. 我們對 n 做歸納法. 首先當 $f(x)=c_1x+c_0$ 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 $c_1a+c_0\equiv c_1b+c_0 \pmod p$. 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 1.5.2 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.

第一種情形如下: 若 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, $x\equiv c+m't \pmod m$ 的表示法很多是重複的. 事實上若 $c+m't\equiv c+m't' \pmod m$ 表示 $m=dm'|m'(t-t')$，也就是說 $d\mid t-t'$. 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. 所以在 modulo m' 之下 $g(x)\equiv 0 \pmod{m'}$ 的一個解 c, 便會對應到 $f(x)\equiv 0 \pmod m$ 在 modulo m 之下 $c,c+m',\ldots,c+(d-1)m'$ 這 d 個解. 由於每個 $f(x)\equiv 0 \pmod m$ 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.

Example 4.2.3. 考慮 $26x^3+39x^2-91x-13\equiv 0 \pmod{39}$。由於 13 整除各項係數以及所 modulo 的 39，所以依 Proposition 4.2.1，我們僅需考慮 $2x^3+3x^2-7x-1\equiv 0 \pmod 3$。

這又可化簡成 $2x^3-x-1\equiv 0 \pmod 3$。分別代 $x\equiv 0,1,2 \pmod 3$，解得在 modulo 3 之下 $x\equiv 1 \pmod 3$ 為 $2x^3-x-1\equiv 0 \pmod 3$ 的唯一解，所以 $26x^3+39x^2-91x-13\equiv 0 \pmod{39}$ 在 modulo 39 之下有 $1,4,7,\ldots,1+12\times 3=37$ 共 13 解。

另一方面，若改為考慮 congruence equation $26x^3+39x^2+91x-13\equiv 0 \pmod{39}$，則可化簡為 $-x^3+x-1\equiv 0 \pmod 3$。由 Fermat Little Theorem（Corollary 3.3.5）知 $-x^3+x\equiv 1 \pmod 3$ 無解，所以原 congruence equation 無解。

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 4.2.4. 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 4.2.4 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 4.2.4 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 4.2.5. 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 4.2.4 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 $i\in\{1,\dots,r\}$, $x\equiv c \pmod{p_i^{n_i}}$ 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 4.2.5 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 $f(x)\equiv 0 \pmod m$ 有解呢? 依 Proposition 4.2.5 知, 此時需解聯立方程式

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

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 4.2.6. 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 4.2.5 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 3.5.2 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 4.2.5 得知 $x\equiv c \pmod m$ 為 $f(x)\equiv 0 \pmod m$ 之一解. □

我們看一個簡單例子. 雖然此例可以直接代數字得到解答, 但是我們希望利用此例來講解這裡所用的概念. 大家應著重於如何應用所學的方法而不是僅在於得到答案.

Example 4.2.7. 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:

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

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

利用中國剩餘定理我們分別解出 $x\equiv 1,-1,11,4 \pmod{15}$ 這 4 解。所以由 Proposition 4.2.5 我們知 $x\equiv 1,-1,11,4 \pmod{15}$ 都為 $x^2\equiv 1 \pmod{15}$ 的解. 再由中國剩餘定理的唯一性，得知在 modulo 15 之下確實僅有這 4 個解.

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 4.2.4 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 $x \equiv a'ex \equiv b'e \pmod{m'}$. 因此若令 $x \equiv b'e \pmod{m'}$ 可得 $a'x \equiv a'b'e \equiv b' \pmod{m'}$. 證得 $x \equiv b'e \pmod{m'}$ 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 $d\mid b$, 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, 則在 *modulo* m 之下所有的解為：

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

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 52 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 $ax+my=d$ 的一組整數解 $x=r, y=s$. 此時再由 $b=kd$ 知 $ark+msk=b$，亦即 $a(rk)\equiv b \pmod{m}$。故 $x\equiv rk \pmod{m}$ 為 $ax\equiv b \pmod{m}$ 的一個解.

4.4. 二次 Congruence Equation 的化簡

所謂二次的 congruence equation, 即給定 $m\in\mathbb{N}$, 考慮 $ax^2+bx+c\equiv 0 \pmod{m}$, 其中 $a,b,c\in\mathbb{Z}$ 且 $m\nmid a$ 這樣的 equation.

大家看到這樣的方程式, 首先會想到用配方法來解. 沒錯, 我們也是要用配方法. 不過這裡有一點要特別注意, 就是我們都是在整數的情況, 所以須避免用到除法. 例如大家要解 $ax^2+bx+c=0$ 時, 第一個想到的是將 x^2 項的係數 a 除去得 $x^2+(b/a)x+(c/a)=0$. 由於我們在談 congruence equation, 多項式需要求為整係數, 這個方法就行不通了 (除非 $a|b$ 且 $a|c$). 當然了, 當 a 和 m 互質時存在 $e\in\mathbb{Z}$ 使得 $ae\equiv 1 \pmod{m}$, 所以此時我們可以將

$ax^2+bx+c\equiv 0 \pmod m$ 兩邊乘上 e 而得 $x^2+bex+ce\equiv 0 \pmod m$. 不過這個方法要限制在 $\gcd(m,a)=1$ 的情形, 而我們要探討的是一般情況, 所以我們需想辦法處理. 不管怎樣為了讓多項式為整係數, 我們不要用除的方法, 儘量用乘的. 所以為了使用配方法我們可以讓 x^2 項係數成為完全平方, 也就是將 $ax^2+bx+c\equiv 0 \pmod m$ 兩邊乘上 a 而得 $(ax)^2+abx+ac\equiv 0 \pmod m$. 接著處理 x 項係數, 由於不能用除的所以不能將 abx 寫成 $2(ab/2)x$, 但用配方法 x 項係數需偶數, 因此好的方法是將原式兩邊乘以 2. 不過這樣一來又破壞了原先 x^2 項係數為完全平方的好處, 所以我們再多乘一個 2 使得 x^2 項係數仍為完全平方.

也就是說, 在解 $ax^2+bx+c\equiv 0 \pmod m$ 時我們可以將兩邊乘上 $4a$ 使得原式成為 $4a^2x^2+4abx+4ac=(2ax)^2+2(2ax)b+4ac\equiv 0 \pmod m$. 接下來就可用配方法常用步驟將式子寫成 $(2ax+b)^2\equiv b^2-4ac \pmod m$. 因此我們將問題簡化成解 $y^2\equiv b^2-4ac \pmod m$. 今若沒有整數 k 滿足 $k^2\equiv b^2-4ac \pmod m$, 那麼我們便知原 congruence equation, $ax^2+bx+c\equiv 0 \pmod m$ 無解. 若可找到 $k\in\mathbb{Z}$ 滿足 $k^2\equiv b^2-4ac \pmod m$, 那麼我們便可依前面探討一次的 congruence equation 的方法解 $2ax+b\equiv k \pmod m$, 而得到 $ax^2+bx+c\equiv 0 \pmod m$ 的解.

總之, 解二次 congruence equation, $ax^2+bx+c\equiv 0 \pmod m$ 的問題, 可化簡成解 $y^2\equiv d \pmod m$ 其中 $d=b^2-4ac$. 因此不失一般性, 我們接下來僅探討 $x^2\equiv a \pmod m$ 這樣形式的 congruence equation.

假設 $m=p_1^{n_1}\cdots p_t^{n_r}$, 其中這些 p_i 為相異質數. 由 Corollary 4.2.6 知, $x^2\equiv a \pmod m$ 有解若且唯若對所有的 p_i, $x^2\equiv a \pmod{p_i^{n_i}}$ 有解. 因此我們又將問題化簡為求 $x^2\equiv a \pmod{p^n}$, 其中 p 為質數且 $n\in\mathbb{N}$ 的情形.

我們來看一個綜合以上結果的例子.

Example 4.4.1. 我們試著解 $29x^2+15x+1\equiv 0 \pmod{45}$. 首先將式子兩邊乘上 4×29, 得 $(58x)^2+2\times 58\times 15x+116\equiv 0 \pmod{45}$. 接著利用配方法得 $(58x+15)^2\equiv 109 \pmod{45}$, 即 $(13x+15)^2\equiv 19 \pmod{45}$ (別忘了 $58x\equiv 13x \pmod{45}$).

接著因為 $45=3^2\times 5$, 我們可以將式子轉化成解 $(13x+15)^2\equiv 19 \pmod 9$ 及 $(13x+15)^2\equiv 19 \pmod 5$. 也就是說分別解 $(4x+6)^2\equiv 1 \pmod 9$ 以及 $(3x)^2\equiv 4 \pmod 5$. 由於 $y\equiv\pm 1 \pmod 9$ 為 $y^2\equiv 1 \pmod 9$ 之解, 故知 $4x+6\equiv\pm 1 \pmod 9$, 解得 $x\equiv 1,5 \pmod 9$ 為 $(13x+15)^2\equiv 19 \pmod 9$ 之解. 另一方面 $y\equiv\pm 2 \pmod 5$ 為 $y^2\equiv 4 \pmod 5$ 之解, 故得 $3x\equiv\pm 2 \pmod 5$, 解得 $x\equiv 1,4 \pmod 5$ 為 $(13x^2+15)^2\equiv 19 \pmod 5$ 之解.

最後要解 $29x^2+15x+1\equiv 0 \pmod{45}$, 由前知 x 需符合:

$$(1)\begin{cases} x\equiv 1 & \pmod 9\\ x\equiv 1 & \pmod 5\end{cases},\quad (2)\begin{cases} x\equiv 1 & \pmod 9\\ x\equiv 4 & \pmod 5\end{cases},$$

$$(3)\begin{cases} x\equiv 5 & \pmod 9\\ x\equiv 1 & \pmod 5\end{cases}\ \text{或}\ (4)\begin{cases} x\equiv 5 & \pmod 9\\ x\equiv 4 & \pmod 5\end{cases}.$$

因此求得 $x\equiv 1,14,19,41 \pmod{45}$ 為 $29x^2+15x+1\equiv 0 \pmod{45}$ 之解.

回到我們的主題. 我們將要解一般二次的 congruence equation 化解成解 $x^2\equiv a \pmod{p^n}$, 其中 p 為質數且 $n\in\mathbb{N}$ 的情形. 我們先來看 a 和 p 不互質的情形. 假設 $p^n|a$ 等於

解 $x^2 \equiv 0 \pmod{p^n}$, 此時當然有解. 若 $a = p^i a'$ 其中 $p \nmid a'$ 且 $1 \le i \le n-1$ 怎麼辦? 現假若 i 是奇數, 我們要說明此時 $x^2 \equiv p^i a' \pmod{p^n}$ 無解. 若有解且 b 為 $x^2 \equiv p^i a' \pmod{p^n}$ 之一解, 我們將 b 寫成 $b = p^s b'$, 其中 $p \nmid b'$. 此時因假設 $b^2 \equiv p^i a' \pmod{p^n}$, 可得 $p^n | p^{2s} b'^2 - p^i a'$. 由於 $2s$ 是偶數而 i 是奇數, 知 $2s \neq i$. 如果 $2s > i$, 則 $p^{2s} b'^2 - p^i a' = p^i (p^{2s-i} b'^2 - a')$. 但由於 $p | p^{2s-i}$ 且 $p \nmid a'$, 我們知 $p \nmid p^{2s-i} b'^2 - a'$. 換言之 $p^{i+1} \nmid p^{2s} b'^2 - p^i a'$. 此和 $p^n | p^{2s} b'^2 - p^i a'$ 且 $n \ge i+1$ 相矛盾. 同理, 若 $2s < i$, 我們也可得矛盾的情形. 所以當 $i < n$ 且是奇數時 $x^2 \equiv p^i a' \pmod{p^n}$ 無解.

當 $a = p^i a'$ 其中 $p \nmid a'$, $0 < i < n$ 且 $i = 2k$ 是偶數時, 若我們將 x 寫成 $x = p^k t$, 此時解 $x^2 \equiv a \pmod{p^n}$ 等同於解 $(p^k t)^2 \equiv p^{2k} a' \pmod{p^n}$, 也就是解 $p^{2k} t^2 \equiv p^{2k} a' \pmod{p^n}$. 由於 $2k < n$, Proposition 4.2.1 告訴我們此式等同於解 $t^2 \equiv a' \pmod{p^{n-2k}}$. 我們將以上討論寫成結論.

Proposition 4.4.2. 給定一質數 p 及 $n \in \mathbb{N}$. 假設 $a = p^i a'$ 其中 $p \nmid a'$ 且 $1 \le i \le n-1$.

(1) 若 i 是奇數, 則 $x^2 \equiv a \pmod{p^n}$ 無解.

(2) 若 i 是偶數, 則 $x^2 \equiv a \pmod{p^n}$ 有解若且唯若 $x^2 \equiv a' \pmod{p^{n-i}}$ 有解.

從以上的討論我們知道要解一個二次的 congruence equation 都可以簡化到 $x^2 \equiv a \pmod{p^n}$, 其中 $p \nmid a$ 的情況. 因此下一章我們僅專注於 $x^2 \equiv a \pmod{p^n}$ 其中 $p \nmid a$ 的情形.

Exercise 4.1. 令 p 為一質數.

(1) 假設 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 為整係數多項式. 若存在 $r_1, \ldots, r_{n+1} \in \mathbb{Z}$ 滿足 $f(r_i) \equiv 0 \pmod{p}$ 且對任意 $i \neq j$ 皆有 $r_i \not\equiv r_j \pmod{p}$, 試證明對所有 $0 \le i \le n$ 皆有 $p \mid a_i$.

(2) 考慮 $g(x) = (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1)$. 若將 $g(x)$ 展開並將同次項整理得 $g(x) = a_{p-2} x^{p-2} + \cdots + a_1 x + a_0$. 試證明對所有 $0 \le i \le p-2$ 皆有 $p \mid a_i$.

(3) 試利用 (2) 之結果證明 Wilson's Theorem.

Exercise 4.2. 解 congruence equation 的方法也可推廣到多變數多項式的情況.

(1) 假設 $f(x,y) \in \mathbb{Z}[x,y]$ 為以 x,y 為變數的整係數多項式. 試證明若 $m' \mid m$ 且 $f(x,y) \equiv 0 \pmod{m'}$ 無整數解, 則 $f(x,y) \equiv 0 \pmod{m}$ 無整數解.

(2) 試證明 congruence equation $3x^2 - 7y^2 \equiv 2 \pmod{525}$ 無整數解.

Exercise 4.3. 試解以下的 congruence equation.

(1) 求 $9x \equiv 21 \pmod{30}$ 在 modulo 30 之下的所有解.

(2) 求 $18x \equiv 15 \pmod{27}$ 在 modulo 27 之下的所有解.

Exercise 4.4. 解一次的 congruence equation 的方法也可推廣到解多變數的一次 congruence equation.

(1) 考慮 congruence equation $a_1x + a_2y \equiv b \pmod{m}$. 令 $d = \gcd(a_1, a_2, m)$. 試證明若 $d \nmid b$, 則此 congruence equation 無解, 而若 $d \mid b$, 則此 congruence equation 在 modulo m 之下共有 dm 組解.

(2) 試解以下的 congruence equation:

$$(a) \quad 2x+3y \equiv 4 \pmod{7}; \qquad (b) \quad 3x+6y \equiv 2 \pmod{9}.$$

(3) (optional，不考) 試將 (1) 的結果推廣到 n 個變數的一次 congruence equation.

Exercise 4.5. 試利用配方法解以下二次的 congruence equations.

(1) $x^2 + x \equiv 3 \pmod{13}$

(2) $2x^2 + x \equiv 3 \pmod{39}$

(3) $3x^2 + x \equiv 3 \pmod{39}$

(4) $3x^2 + x \equiv 1 \pmod{39}$

Exercise 4.6. 試判斷以下二次的 congruence equations 是否有解。若有解，試寫下所有的解。

(1) $x^2 \equiv 40 \pmod{64}$

(2) $2x^2 \equiv 40 \pmod{32}$

(3) $x^2 \equiv 21 \pmod{9}$

(4) $x^2 \equiv 18 \pmod{27}$