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 1

整數的基本性質

雖然有些同學已對整數的性質相當了解, 我們想利用這個大家較熟悉的東西來介紹一下如何用比較"數學"的方法來處理問題. 有些簡單的問題我們可能會故意繞遠路來處理, 主要原因是希望大家能熟悉表達數學的方法和形式以及邏輯推演的過程. 所以這一章會顯得較為冗長. 若大家對這些性質已很熟悉且認為表達數學的能力已很成熟, 可以略過此章,直接進入下一章.

1.1. 因數與倍數

首先我們介紹幾個符號順便複習一下集合的概念. 要知道符號是數學上幫助我們能簡明表達事情的必要工具, 大家應該要學習如何適切的使用符號.

在本講義中我們用 $\mathbb{Z}$ 來表示所有整數所成的集合. 所以 0 在 $\mathbb{Z}$ 中, 2 也在 $\mathbb{Z}$ 中, 2007 和 -365 也在 $\mathbb{Z}$ 中. 這樣一來當我們要說一個數 a 是整數時, 我們只要說 a 在 $\mathbb{Z}$ 中就好了. 在數學上我們要說一個東西在一個集合中就用"$\in$" 這個符號, 也就是"屬於"的意思. 所以以後我們要表達 a 是一個整數就直接說 $a \in \mathbb{Z}$ 即可. 我們也常只考慮正整數, 在本講義中我們用 $\mathbb{N}$ 表示所有正整數所成的集合. 所以我們用 $a \in \mathbb{N}$ 來表示 a 是一個正整數.

對於整數一開始是由自然數出發，利用數數的方法我們定義了加法，接著有了負的概念整個整數加法的體系就建立起來了。給定 $a \in \mathbb{Z}$, 我們用 $2a$ 表示. $a+a$ 一般來說若 $n \in \mathbb{N}$ 我們將 n 個 a 相加的結果表為 na. 我們也將 $(-n)a$ 看成 n 個 $-a$ 相加所得之值. 若我們再將 $0a$ 定為 0, 如此一來對任意的 $m \in \mathbb{Z}$, ma 都有了定義. 如此定義出來的乘法和加法之間所滿足的運算規則如交換率, 結合率和分配率等此處就不再贅述. 我們將可以寫成 ma 其中 $m \in \mathbb{Z}$ 的數稱為 a 的倍數 (multiple). 另一方面若 b 是 a 的倍數, 我們也稱 a 是 b 的因數 (divisor). 符號記為 $a|b$.

我們將 a 的倍數所成的集合用 $a\mathbb{Z}$ 來表示. 也就是說 $a\mathbb{Z}$ 中的元素都是 ma 這樣的形式其中 $m \in \mathbb{Z}$. 這樣的集合可用 $a\mathbb{Z} = \{ma \mid m \in \mathbb{Z}\}$ 來表示. 因此我們可以說 $b \in a\mathbb{Z}$ 和 b 是 a 的倍數 (或 a 是 b 的因數) 是一樣的意思.

接下來我們想用集合的角度處理因數倍數的一些性質. 要注意這些性質大家高中時都已證過, 我們用集合的角度處理並沒有比較方便，介紹這樣的處理方法僅是利用它讓大家熟悉一下集合的語言.

首先注意若 $a \in \mathbb{Z}$, $a\mathbb{Z}$ 這一個集合並不單單是一個集合. 由於整數在加法和乘法之下有所謂的封閉性, $a\mathbb{Z}$ 也有以下兩個重要的封閉性.

Proposition 1.1.1. 假設 $a \in \mathbb{Z}$ 且 $b, c \in a\mathbb{Z}$. 則我們有以下之性質.

(1) $b + c \in a\mathbb{Z}$.

(2) 對任意 $m \in \mathbb{Z}$ 皆有 $mb \in a\mathbb{Z}$.

Proof. 因為 $b, c \in a\mathbb{Z}$ 依定義知存在 $n, n' \in \mathbb{Z}$ 使得 $b = na$ 且 $c = n'a$.

(1) 由分配率知 $b + c = na + n'a = (n + n')a$. 又由於 $n, n' \in \mathbb{Z}$ 我們知 $n + n' \in \mathbb{Z}$, 故得 $b + c \in a\mathbb{Z}$.

(2) 由結合率知 $mb = m(na) = (mn)a$. 又由於 $m, n \in \mathbb{Z}$ 我們知 $mn \in \mathbb{Z}$, 故得 $mb \in a\mathbb{Z}$. □

結合 Proposition 1.1.1 的結果我們有以下之性質.

Corollary 1.1.2. 假設 $a \in \mathbb{Z}$ 且 $b, c \in a\mathbb{Z}$. 若 $m, n \in \mathbb{Z}$ 則 $mb + nc \in a\mathbb{Z}$. 換言之, 若 $a|b$ 且 $a|c$, 則對任意 $m, n \in \mathbb{Z}$ 皆有 $a|mb + nc$.

Proof. 因為 $b, c \in a\mathbb{Z}$ 以及 $m, n \in \mathbb{Z}$, 由 Proposition 1.1.1(2) 知 $mb, nc \in a\mathbb{Z}$. 再利用 Proposition 1.1.1(1) 知 $mb + nc \in a\mathbb{Z}$. 也就是說 $a|mb + nc$. □

大部分一個重要的性質我們都會用 Proposition 來稱呼再冠上編號以便以後引用. 而直接套用 Proposition 所得的性質我們都用 Corollary 來稱呼.

接著我們來看集合單純的性質. 若 A, B 是集合且 A 中的元素都在 B 中, 則我們就用 $A \subseteq B$ 來表示 (稱 A 包含於 B). 很容易有以下之性質:

(1) 若 $A \subseteq B$ 且 $B \subseteq A$ 則 $A = B$.

(2) 若 $A \subseteq B$ 且 $B \subseteq C$ 則 $A \subseteq C$.

結合這集合的性質以及前面提的封閉性我們有以下之結果.

Proposition 1.1.3. 假設 $a, b, c \in \mathbb{Z}$. 我們有以下之結果.

(1) $b\mathbb{Z} \subseteq a\mathbb{Z}$ 若且唯若 $a|b$.

(2) 若 $a|b$ 且 $b|a$ 則 $a = \pm b$.

(3) 若 $a|b$ 且 $b|c$ 則 $a|c$.

Proof. (1) 若 $b\mathbb{Z} \subseteq a\mathbb{Z}$, 由於 $b \in b\mathbb{Z}$, 我們得 $b \in a\mathbb{Z}$. 故知 $a|b$. 反之, 若 $a|b$, 我們要證明 $b\mathbb{Z} \subseteq a\mathbb{Z}$. 一般來說要證明一個集合 B 包含於另一個集合 A, 我們要證明的是 B 中任取一個元素都會在 A 中. 因此此處我們要證的是任取 $b\mathbb{Z}$ 中的一個元素 mb, 其中 $m \in \mathbb{Z}$ 都可以

得到 $mb \in a\mathbb{Z}$. 然而由 $a|b$ 的假設我們知 $b \in a\mathbb{Z}$. 接著我們就可利用 Proposition 1.1.1(2) 知對任意 $m \in \mathbb{Z}$ 皆有 $mb \in a\mathbb{Z}$. 也就是說 $b\mathbb{Z}$ 的元素都在 $a\mathbb{Z}$ 中. 故得證 $b\mathbb{Z} \subseteq a\mathbb{Z}$.

(2) 若 $a|b$ 且 $b|a$, 由 (1) 知 $b\mathbb{Z} \subseteq a\mathbb{Z}$ 且 $a\mathbb{Z} \subseteq b\mathbb{Z}$. 因此由集合性質知 $a\mathbb{Z} = b\mathbb{Z}$. 也就是說 $a\mathbb{Z}$ 和 $b\mathbb{Z}$ 是相同的集合. 由此, 很容易看出當 $a = 0$ 時 $b = 0$. 反之亦然. 因此我們只剩考慮 $a \neq 0$ 且 $b \neq 0$ 的情況. 此時 $a\mathbb{Z}$ 中最小的正數 a (當 $a > 0$) 或 $-a$ (當 $a < 0$) 會等於 $b\mathbb{Z}$ 中最小的正數 b 或 $-b$. 故得證 $a = \pm b$.

(3) 若 $a|b$ 且 $b|c$, 則由 (1) 知 $b\mathbb{Z} \subseteq a\mathbb{Z}$ 且 $c\mathbb{Z} \subseteq b\mathbb{Z}$. 因此由集合性質知 $c\mathbb{Z} \subseteq a\mathbb{Z}$. 故再由 (1) 的等價關係知 $a|c$. □

Remark 1.1.4. 對於整數有一個很重要的性質 "well-ordering principle". 這一個 principle 就是說給定一個非空的整數的子集合 S, 如果 S 有下界(若有一數小於 S 中所有的數, 則稱 S 有下界), 則 S 中必含有一個最小的整數 (通常用 $\min S$ 來表示). 同理若整數的非空子集合 S 有上界 (若有一數大於 S 中所有的數, 則稱 S 有上界), 則此集合中必含有一個最大的整數 (通常用 $\max S$ 來表示). 例如剛才 Proposition 1.1.3(2) 的證明中我們考慮 $a\mathbb{Z}$ 中最小的正整數, 當 $a > 0$ 時 a 就是 $a\mathbb{Z}$ 中最小的正整數. 這裡因為我們確實知道 $a\mathbb{Z}$ 這個集合長什麼樣, 所以並不需這個性質直接可知 a 就是最小的. 以後我們常會碰到一些抽象的正整數子集合, 那時就得經常用到整數的這個性質來確知此集合存在一個最小的正數. 另外要注意此性質在其他的情況如有理數就不對了. 事實上正有理數是有下界的(0 小於所有的正有理數), 但並沒有所謂最小的正有理數.

再次強調一下前面我們用集合較抽象的方法證明整除的性質主要是要大家習慣集合的語言以及學習一些抽象的論證方法. 它並不是什麼特別的好方法. 比方說大家熟知的 $a|b$ 則 $ma|mb$ 就很難用類似上面集合的方法來處理. 總之, 要處裡一個問題並沒有說一定要用什麼方法. 你只要使用一個你認為可行且正確的方法處理. 所以學習數學絕不要僅是背誦定理的證明. 如何將繁瑣的證明整理成你自己習慣且能理解的語言才是重點. 接下來我們就回歸定義來證明前述之性質.

Lemma 1.1.5. 假設 $a, b \in \mathbb{Z}$ 且 $a|b$, 我們有以下之性質.

(1) 若 $m \in \mathbb{Z}$, 則 $ma|mb$.

(2) 若 $d|a$ 且 $d|b$, 則 $(a/d)|(b/d)$.

Proof. 由假設 $a|b$ 知存在 $n \in \mathbb{Z}$ 使得 $b = na$.

(1) 將等式兩邊同乘以 m 可得 $mb = mna = n(ma)$ 故知 $ma|mb$.

(2) $d|a$ 且 $d|b$ 即表示存在 $a', b' \in \mathbb{Z}$ 使得 $a = a'd$ 且 $b = b'd$. 故由 $b = na$ 得 $b'd = na'd$. 因為 $d \neq 0$, 兩邊同除以 d 可得 $b' = na'$, 即 $a'|b'$. 因為 $a/d = a'$ 且 $b/d = b'$ 故得證 $(a/d)|(b/d)$. □

Lemma 1.1.5 是一個簡單的性質. 它本身並不算什麼重大的性質, 但是以後討論許多性質時都要用到它, 我們便用 Lemma 稱呼之以方便引用.

在 Lemma 1.1.5(2) 中 $d|a$ 且 $d|b$ 的假設就是說 d 同時是 a 和 b 的因數, 我們簡稱之為 a, b 的公因數. 討論一些整數之間的關係時公因數和最大公因數以及公倍數和最小公倍數是很重要的工具. 接下來我們是給它們下一個定義.

Definition 1.1.6. 令 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

(1) 若 $c \in \mathbb{Z}$, 且 $c|a_1$, $c|a_2, \ldots$, $c|a_n$, 則稱 c 為 $a_1, a_2, \ldots, a_n$ 的公因數 (common divisor).

(2) 若 $d \in \mathbb{N}$ 是 $a_1, a_2, \ldots, a_n$ 的公因數中最大的, 則稱 d 為 $a_1, a_2, \ldots, a_n$ 的最大公因數 greatest common divisor, 通常我們會用 $\gcd(a_1, a_2, \ldots, a_n)$ 來表示之.

(3) 若 $m \in \mathbb{Z}$, 且 $a_1|m$, $a_2|m, \ldots$, $a_n|m$, 則稱 m 為 $a_1, a_2, \ldots, a_n$ 的公倍數 (common multiple).

(4) 若 $l \in \mathbb{N}$ 是 $a_1, a_2, \ldots, a_n$ 的正的公倍數中最小的, 則稱 l 為 $a_1, a_2, \ldots, a_n$ 的最小公倍數 least common divisor, 通常我們會用 $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$ 來表示之.

通常當有一個符號或名詞需要介紹時, 為了方便找到我們會特別用 Definition 來標示之.

當要下一個定義時要注意是否合理. 不要給的定義的東西根本不存在或沒有用. Definition 1.1.6 中就要注意最大公因數及最小公倍數是否存在: 因為 1 整除所有的整數, 所以若 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ 則其公因數必存在. 又因為 $a_1, a_2, \ldots, a_n$ 有有限多個公因數, 所以我們知 $a_1, a_2, \ldots, a_n$ 的最大公因數必存在. 不過 $a_1, a_2, \ldots, a_n$ 的最大公因數有可能是 1. 若如此 (即 $\gcd(a_1, a_2, \ldots, a_n) = 1$), 則稱 $a_1, a_2, \ldots, a_n$ 互質 (*relatively prime*). 另一方面因為 $a_1 a_2 \cdots a_n$ 是 $a_1, a_2, \ldots, a_n$ 的公倍數, 所以適當的乘上正負號可知 $a_1, a_2, \ldots, a_n$ 正的公倍數必存在, 因此由 well-ordering principle 知 $a_1, a_2, \ldots, a_n$ 的最小公倍數必存在.

下一節我們將會談論最大公因數及最小公倍數的一些基本性質.

1.2. 除法原理

整數中最基本的定理應該就是整數的除法原理 *Division Algorithm*, 幾乎所有整數的基本性質都是由它推導出來.

Theorem 1.2.1 (Division Algorithm)**.** 給定一正整數 n, 對任意的 $m \in \mathbb{Z}$, 皆存在 $h, r \in \mathbb{Z}$, 其中 $0 \le r < n$, 滿足 $m = h \cdot n + r$.

這是一個很重要的性質, 重要到我們以 Theorem 來稱呼它. 這個定理我們習慣稱為除法原理, 如此稱它當然就包含"除"這個概念. 不過因為我們現在僅談加(減)法和乘法的性質, 我們避免用除的概念.

Proof. 給定 $n \in \mathbb{N}$ 且 $m \in \mathbb{Z}$. 首先考慮 $W = \{m - t \cdot n \,|\, t \in \mathbb{Z}\}$ 這一個集合. 也就是收集 $m, m-n, m-2n, \ldots$ 以及 $m+n, m+2n, \ldots$ 等元素所得集合. 因為 t 可取任何整數, 很容易就看出 W 一定包含一些非負的整數. 換言之, 若考慮 W' 為 W 中非負的元素所成的集合, 則 W' 是一個非空的整數的子集合. 故由整數的 well-ordering principle 知 W' 中存

在最小的整數 r. 即 r 是 W 中最小的非負的整數. 因為 $r \in W$, 由定義知存在 $h \in \mathbb{Z}$ 滿足 $r = m - h \cdot n$. 我們最主要的目的就是要證明 $0 \leq r < n$.

假設 r 不合我們的條件, 也就是說 $r \geq n$ (別忘了 r 是非負整數的假設). 若如此, 我們可將 r 寫成 $r = n + r'$, 其中 $r' \geq 0$. 因此利用

$$m = h \cdot n + r = h \cdot n + (n + r') = (h + 1) \cdot n + r',$$

我們得到 $r' = m - (h+1) \cdot n \in W$. 但 $0 \leq r' < r$, 這和 r 是 W 中最小的非負整數相矛盾. 故得證本定理. □

要注意 Theorem 1.2.1 的證明我們用到整數上可以排序的 *well-ordering principle*, 因此雖然證明很簡單, 但並不能直接套用到其他的數系.

接下來我們就要利用除法原理來探討公因數及最大公因數的基本性質. 由於 a 和 $-a$ 的因數是一樣的, 所以不失一般性, 在討論因數時我們僅討論正整數的情形. 我們就從兩個正整數的情形開始討論.

Proposition 1.2.2. 假設 $a, b \in \mathbb{N}$ 且 d 是 a 和 b 的公因數. 若 d' 是 a/d 和 b/d 的公因數, 則 dd' 是 a 和 b 的公因數.

Proof. 首先注意, 由於 d 是 a, b 的公因數, 故存在 $m, n \in \mathbb{Z}$ 使得 $a = dm$ 且 $b = dn$. 也就是說 $a/d = m$ 和 $b/d = n$ 皆為整數. 又 d' 是 m, n 的公因數故存在 $m', n' \in \mathbb{Z}$ 使得 $m = d'm'$ 且 $n = d'n'$. 整理得 $a = dd'm'$ 且 $b = dd'n'$ 故知 dd' 是 a 和 b 的公因數. □

若 Proposition 1.2.2 中我們取 $d = \gcd(a, b)$, 則利用最大公因數的定義我們可得以下之性質.

Corollary 1.2.3. 假設 $a, b \in \mathbb{N}$ 且 $d = \gcd(a, b)$. 則 a/d 和 b/d 互質.

Proof. 要證明 a/d 和 b/d 互質就是證 $\gcd(a/d, b/d) = 1$. 然而要說明 $\gcd(a/d, b/d) = 1$ 就得說明若 d' 是 a/d 和 b/d 的一個正的公因數, 則 $d' = 1$. 事實上若 d' 是 a/d 和 b/d 的一個的公因數, 則由 Proposition 1.2.2 知 dd' 是 a, b 的公因數. 然而已知 d 是 a, b 公因數中最大的, 故知 $d \geq dd'$. 也就是說 $d' \leq 1$. 因此結合當初假設 d' 是 a, b 的一個正的公因數 (即 $d' \geq 1$) 得證 $d' = 1$. □

一般要證明 $d = \gcd(a, b)$ 我們要證明兩件事. 首先要證明 d 是 a, b 的公因數, 再來就是證明 d 是 a 和 b 的公因數中最大的. 前面 Corollary 1.2.3 中我們要證明 $\gcd(a/d, b/d) = 1$. 由於 1 必為 $a/d, b/d$ 的公因數, 所以只要證明任意 a/d 和 b/d 的公因數皆小於等於 1 就可. 接著我們來看另一個最大公因數的性質順便在證明中學習證明最大公因數的方法.

Proposition 1.2.4. 假設 $a, b \in \mathbb{N}$, 令 d 為集合 $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$ 中最小的正整數. 則 $\gcd(a, b) = d$.

Proof. 首先注意由於這裡 m, n 是任意的整數, 所以我們知道集合 $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$ 中必存在正整數. 所以 S 中的正整數必形成一個非空的子集合, 因此我們套用 well-ordering

principle 知 S 中必有最小的正整數. 也就是說敘述中的 d 一定存在. 接著我們要按照前面提的兩個步驟證明 d 為 a, b 的最大公因數.

首先檢查 $d|a$ 且 $d|b$. 依定義存在 $m, n \in \mathbb{Z}$ 使得 $d = ma + nb$. 要檢查是否 $d|a$ 直覺的方法就是將 a 除以 d 看看是否餘數為 0. 利用除法原理我們知存在 $h, r \in \mathbb{Z}$ 使得 $a = dh + r$, 其中 $0 \leq r < d$. 因此有

$$r = a - dh = a - (ma + nb)h = (1 - mh)a - (nh)b.$$

由於 $1 - mh$ 和 $-nh$ 皆為整數依定義知 $r \in S$. 今若 $r \neq 0$ 會導致 r 是 S 中小於 d 的一個正整數. 這和當初假設 d 是 S 中最小的正整數相矛盾, 故知 $r = 0$. 也就是說 $d|a$. 同理可證 $d|b$.

接著我們要證明 d 是 a, b 的公因數中最大的數. 也就是要證明若 d' 是 a, b 的公因數, 則 $d' \leq d$. 今由於 $d'|a$ 且 $d'|b$ 由 Corollary 1.1.2 知 $d'|ma + nb$. 即 $d'|d$, 也就是說存在 $l \in \mathbb{Z}$ 使得 $d = d'l$. 因此由已知 $d > 0$ 當然得 $d' \leq d$. □

在上面證明 d 除以 a 的餘數為 0 的過程中. 我們無法直接證明餘數為 0, 不過發現若餘數不為 0 的話會導致矛盾的結果, 因而確知其餘數非為 0 不可. 這樣證明的方法就是所謂的 "反證法". 這樣的證明方法我們以後還會經常看到.

或許大家會奇怪, 一般來說找 a, b 的最大公因數只要在 a, b 有限多個公因數中找最大的就好了為什麼要自討苦吃在 $\{ma + nb \mid m, n \in \mathbb{Z}\}$ 這個有無窮多個元素的集合中找? 沒有錯如果 a, b 很具體的知道是什麼當然直接找, 然而當我們要討論一般的情形 a, b 是任何可能的整數不能用幾個具體例子代一代就了事. 所以雖然 Proposition 1.2.4 在實際操作時並不實用但要用到理論的推演時他卻是很好用來表達最大公因數的工具. 直接利用 Proposition 1.2.4 我們馬上有以下之性質.

Corollary 1.2.5. 假設 $a, b \in \mathbb{N}$ 且 $d = \gcd(a, b)$ 則存在 $m, n \in \mathbb{Z}$ 使得 $d = ma + nb$. 而且對任意 $d' \in \mathbb{Z}$, d' 是 a, b 的公因數若且唯若 $d'|d$.

Proof. 由 Proposition 1.2.4 我們知 d 在集合 $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$ 中, 故依定義存在 $m, n \in \mathbb{Z}$ 使得 $d = ma + nb$.

注意這裡"若且唯若"的意思就是說如果 d' 是 a, b 的公因數那麼 d 必整除 a, b 的最大公因數 d, 反之若 d' 整除 a, b 的最大公因數, 那麼 d' 一定是 a, b 的公因數. 由 Proposition 1.2.4 的證明我們知若 d' 是 a, b 的公因數則 $d'|d$. 反之若 $d'|d$, 則由於 $d|a$ 且 $d|b$, 利用 Proposition 1.1.3(3) 知 $d'|a$ 且 $d'|b$. 即 d' 為 a, b 的公因數. □

一般來說有的性質可以從甲可推得乙, 但這並不表示從乙可推得甲. 如果兩個性質可以互推, 我們就用"若且唯若"表示之. 特別要注意 Corollary 1.2.5 並不是說若有一個正整數 d 可找到 $m, n \in \mathbb{Z}$ 使得 $d = ma + nb$, 則 d 就是 a, b 的公因數. 這是一開始大家在學習邏輯推論時常犯的錯誤. 其實 d 可以寫成 $ma + nb$ 僅表示 d 會在集合 $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$ 中, 並不表示 d 會是 S 中最小的正整數. 所以當然 d 就未必是 a, b 的最大公因數. 因此當你要證明 d 是 a, b 的最大公因數時, 還是得按部就班如前面所提的兩步驟進行, 千萬不要

找到兩個整數 m,n 使得 $d=ma+nb$ 就說 d 就是 a,b 的最大公因數. 當然了如果你要證明 a,b 互質 (即 $\gcd(a,b)=1$) 時可以利用找到 m,n 使得 $ma+nb=1$ 來處理. 這是因為此時 1 在 S 中, 故當然是 S 中最小的正整數了. 因此我們將此特殊情況列出.

Corollary 1.2.6. 假設 $a,b\in\mathbb{N}$. 則 $\gcd(a,b)=1$ 若且唯若存在 $m,n\in\mathbb{Z}$ 使得 $ma+nb=1$.

Proof. 再強調一次, 要證明若且唯若必需兩個方向都證明.

若 $\gcd(a,b)=1$, 由 Corollary 1.2.5 知存在 $m,n\in\mathbb{Z}$ 使得 $1=ma+nb$. 反之, 若存在 $m,n\in\mathbb{Z}$ 使得 $ma+nb=1$, 則 1 必為集合 $\{ma+nb\mid m,n\in\mathbb{Z}\}$ 中最小的正整數, 故由 Proposition 1.2.4 知 $\gcd(a,b)=1$. □

以上的性質並沒有告訴我們怎麼找到 m,n 使得 $ma+nb=\gcd(a,b)$, 我們將會在下節介紹完輾轉相除法後給一個方法來求 m,n. 雖然目前我們不知如何求得 m,n, 不過從下一個探討 a,b 互質時的重要的性質我們可以看到僅僅知道它們的存在性在理論的推演就很管用了.

Proposition 1.2.7. 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$. 我們有以下的性質:

(1) 若 $k\in\mathbb{Z}$ 且 $a|bk$, 則 $a|k$.

(2) 若 $l\in\mathbb{Z}$ 且 $a|l$ 及 $b|l$, 則 $ab|l$.

Proof. 因為 $\gcd(a,b)=1$, 由 Corollary 1.2.6 我們知存在 $m,n\in\mathbb{Z}$ 使得 $ma+nb=1$.

(1) 將 $ma+nb=1$ 等式兩邊乘上 k 可得 $mak+nbk=k$. 然而假設 $a|bk$ 故利用 $a|ak$ 以及 Corollary 1.1.2 知 $a|k$.

(2) 由 $a|l$ 以及 $b|l$ 知存在 $r,s\in\mathbb{Z}$ 使得 $l=ar=bs$. 因為 $a|ar$ 故得 $a|bs$. 再由 $\gcd(a,b)=1$ 的假設利用 (1) 可得 $a|s$. 換言之存在 $t\in\mathbb{Z}$ 使得 $s=at$. 將之帶回 $l=bs$ 得 $l=bat$, 得證 $ab|l$. □

要注意 Proposition 1.2.7 的條件. 一般來說若沒有 a,b 互質的假設 $a|bc$ 並不能保證 $a|b$ 或 $a|c$. 就拿 $12|6\times4$ 來說吧, 很明顯的 $12\nmid6$ (這裡 $\nmid$ 表示不整除的意思) 而且 $12\nmid4$. 同樣的若 a,b 不互質 $a|c$ 且 $b|c$ 也不能保證 $ab|c$. 例如 $4|12$ 且 $6|12$ 但是 $4\times6\nmid12$.

接下來我們來看看 a,b 的最小公倍數. 若 l 是 a,b 的最小公倍數, 則由於 $gcd(a,b)|l$, 我們自然知存在 $m,n\in\mathbb{Z}$ 使得 $l=ma+nb$. 不過這個表示法對 l 就沒有什麼幫助了. 主要原因是 l 在 $\{ma+nb\mid m,n\in\mathbb{Z}\}$ 這個集合中不像 $\gcd(a,b)$ 有如 Proposition 1.2.4 所述一樣特殊的地位. 不過沒關係, 下一個定理告訴我們一般來說只要了解 a,b 的最大公因數就能掌握 a,b 的最小公倍數.

讓我們先來看看要怎樣知道 l 是 a,b 的最小公倍數. 就如同最大公因數的情形一樣我們要證明兩件事. 首先證明 l 是 a,b 的正的公倍數, 再來就是證明 l 是 a 和 b 的正的公因數中最小的. 如此一來就能擔保 l 是 a,b 的最小公倍數.

Proposition 1.2.8. 假設 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=d$ 及 $\mathrm{lcm}(a,b)=l$, 則 $l=ab/d$. 而且 $m\in\mathbb{Z}$ 是 a,b 的公倍數若且唯若 $l|m$.

Proof. 由假設 $d = \gcd(a,b)$ 知存在 $a', b' \in \mathbb{N}$ 使得 $a = a'd$, $b = b'd$ 且 $\gcd(a', b') = 1$ (Proposition 1.2.3). 現在我們依上述兩個步驟證明 $ab/d = a'b = b'a$ 是 a, b 的最小公倍數.

首先由 $ab/d = b'a$ 知 $a|(ab/d)$ 同理知 $b|(ab/d)$, 也就是說 ab/d 為 a 和 b 的公倍數. 又因為 a, b, d 皆為正數, 所以 ab/d 為 a, b 之正的公倍數.

接著證明若 m 為 a, b 之正的公倍數, 則 $(ab/d) \leq m$. 由假設知存在 $m', n' \in \mathbb{N}$ 使得 $m = m'a = n'b$. 換言之 $m = m'a'd = n'b'd$, 故消掉 d (因 $d \neq 0$) 得 $m'a' = n'b'$. 也就是說 $a'|n'b'$. 但由於 $\gcd(a', b') = 1$, 故由 Proposition 1.2.7(1) 知 $a'|n'$. 也就是說存在 $h \in \mathbb{N}$ 使得 $n' = a'h$. 代回 $m = n'b$ 得 $m = ha'b$, 故得知 $a'b = (ab/d)|m$. 由於 ab/d 及 m 皆為正數, 得證 $(ab/d) \leq m$. 也就是說 $ab/d = \operatorname{lcm}(a, b) = l$.

既然 $ab/d = l$ 由上面的證明我們知若 m 為 a, b 的公倍數, 則 $l = (ab/d)|m$. 反之, 若 $l|m$, 則由 $a|l$ 且 $b|l$, 得知 $a|m$ 且 $b|m$, 故 m 為 a, b 之公倍數. □

要注意雖然 Proposition 1.2.8 中假設 $a, b \in \mathbb{N}$, 但其目的僅是利用其為正數方便描述最小公倍數. 若 $a, b \in \mathbb{Z}$ 不一定為正時, 我們只要適當的加上負號仍可利用 Proposition 1.2.8 的式子寫下最小公倍數. 另外和 Corollary 1.2.5 中所述公因數為最大公因數之因數相輝映 Proposition 1.2.8 告訴我們公倍數為最小公倍數之倍數.

接下來讓我們來看看有關多個 (多於兩個) 整數的最大公因數性質. 我們試著著推廣前面的方法, 看看前面的結果對多個整數是否適用.

Proposition 1.2.9. 假設 $a_1, \ldots, a_n \in \mathbb{N}$, 令 d 為集合 $S = \{m_1a_1 + \cdots + m_na_n \mid m_1, \ldots, m_n \in \mathbb{Z}\}$ 中最小的正整數. 則 $\gcd(a_1, \ldots, a_n) = d$.

Proof. 和前面的情形相同, 利用 well-ordering principle 知 S 中必有最小的正整數. 也就是說敘述中的 d 一定存在. 接著我們要按照前面證明最大公因數的步驟證明 d 為 $a_1, \ldots, a_n$ 的最大公因數.

首先檢查對所有 $i \in \{1, \ldots, n\}$, 皆有 $d|a_i$. 依定義, 存在 $m_1, \ldots, m_n \in \mathbb{Z}$ 使得 $d = m_1a_1 + \cdots + m_na_n$. 利用除法原理我們知對任意 $i \in \{1, \ldots, n\}$ 皆存在 $h_i, r_i \in \mathbb{Z}$ 使得 $a_i = dh_i + r_i$, 其中 $0 \leq r_i < d$. 因此有

$$r_i = a_i - dh_i = a_i - (m_1a_i + \cdots + m_na_n)h_i = -(m_1h_i)a_1 + \cdots + (1 - m_ih_i)a_i + \cdots - (m_nh_i)a_n.$$

故得知 $r_i \in S$. 今若 $r_i \neq 0$ 會導致 r_i 是 S 中小於 d 的一個正整數. 這和當初假設 d 是 S 中最小的正整數相矛盾, 故知 $r_i = 0$. 也就是說對任意 $i = \{1, \ldots, n\}$, 皆有 $d|a_i$.

接著我們要證明 d 是 $a_1, \ldots, a_n$ 的公因數中最大的數. 也就是要證明若 d' 是 $a_1, \ldots, a_n$ 的公因數, 則 $d' \leq d$. 今由於對任意 $i \in \{1, \ldots, n\}$, 皆有 $d'|a_i$ 故知 $d'|m_1a_1 + \cdots + m_na_n$. 即 $d'|d$, 因此由已知 $d > 0$ 當然得 $d' \leq d$. □

有了 Proposition 1.2.9 我們當然可以和前面的方法一樣得到以下之結果, 證明就不再贅述.

Corollary 1.2.10. 假設 $a_1,\dots,a_n\in\mathbb{N}$ 且 $d=\gcd(a_1,\dots,a_n)$ 則存在 $m_1,\dots,m_n\in\mathbb{Z}$ 使得 $d=m_1a_1+\cdots+m_na_n$. 而且對任意 $d'\in\mathbb{Z}$, d' 是 $a_1,\dots,a_n$ 的公因數若且唯若 $d'|d$.

要注意並不是所有有關兩個整數的最大公因數的性質都可以推廣到多個整數的情形. 例如 Proposition 1.2.7(2) 告訴我們若 $\gcd(a,b)=1$ 且 $a|l$ 及 $b|l$, 則 $ab|l$. 此性質在兩個以上整數的情形就不一定對. 主要原因就是依多個整數互質的定義 $a_1,a_2,\dots,a_n$ 互質是表示這些數沒有共同的因數但不表示任取其中兩個數都互質. 其實有可能任意 a_i,a_j 都不互質但是 $a_1,\dots,a_n$ 仍互質. 例如 $a_1=6$, $a_2=15$ 以及 $a_3=10$ 的情形. 我們有 $\gcd(a_1,a_2)=3$, $\gcd(a_2,a_3)=5$ 以及 $\gcd(a_1,a_3)=2$ 但是 $\gcd(a_1,a_2,a_3)=1$. 所以有些情形僅假設 $a_1,\dots,a_n$ 互質是不夠的, 我們須用到任取兩個都互質 (即對任意 $i,j\in\{1,\dots,n\}$ 且 $i\neq j$, 皆有 $\gcd(a_i,a_j)=1$) 這一個較強的互質性才行. 這種較強的互質性我們稱之為 "兩兩互質" (*pairwise relatively prime*). 當然了若 $a_1,\dots,a_n$ 兩兩互質, 則 $a_1,\dots,a_n$ 必互質. 大家一定要清楚這兩種互質性之不同. Proposition 1.2.7(2), 在多個整數的情形之下若改為兩兩互質就會成立. 由於這裡牽涉到任意多個整數, 所以得用到數學歸納法來證明. 數學歸納法的原理我們假設大家在高中時已了解, 此處不再贅述.

Proposition 1.2.11. 假設 $a_1,\dots,a_n\in\mathbb{N}$ 且這些 a_i 兩兩互質. 若令 $M=a_1\cdots a_n$, 則我們有以下之性質.

(1) 對任意 $i\in\{1,\dots,n\}$ 皆有 $\gcd(a_i,M/a_i)=1$.

(2) 若對所有 $i\in\{1,\dots,n\}$ 皆有 $a_i|l$, 則 $M|l$.

Proof. 由於僅在多於一個整數時才談最大公因數, 所以我們數學歸納法從 $n=2$ 開始.

(1) 此處由於和 $a_1,\dots,a_n$ 的排序無關, 我們僅處理 $i=1$ 的情形. 首先看 $n=2$ 的情形. 此時 $M=a_1a_2$ 故由假設 $\gcd(a_1,a_2)=1$ 知 $\gcd(a_1,M/a_1)=1$. 再來由數學歸納法假設 $n=k-1$ 時成立, 即 $\gcd(a_1,a_2\cdots a_{k-1})=1$, 知存在 $m',n'\in\mathbb{Z}$ 使得

$$m'a_1+n'(a_2\cdots a_{k-1})=1. \tag{1.1}$$

現考慮 $n=k$ 之情形, 此時 $M=a_1a_2\cdots a_k$. 將式子 (1.1) 兩邊乘以 a_k 得

$$m'a_1a_k+n'(a_2\cdots a_{k-1}a_k)=m'a_ka_1+n'(M/a_1)=a_k. \tag{1.2}$$

又由兩兩互質的假設知 $\gcd(a_1,a_k)=1$, 即存在 $r,s\in\mathbb{Z}$ 使得 $ra_1+sa_k=1$. 以式子 (1.2) 之 a_k 代入上式得

$$1=ra_1+s(m'a_ka_1+n'(M/a_1))=(r+sm'a_k)a_1+sn'(M/a_1).$$

因為 $r+sm'a_k\in\mathbb{Z}$ 且 $sn'\in\mathbb{Z}$ 故由 Corollary 1.2.6 知 $\gcd(a_1,M/a_1)=1$.

(2) 首先考慮 $n=2$ 的情形, 此時 $M=a_1a_2$ 且 $\gcd(a_1,a_2)=1$ 故 Proposition 1.2.7(2) 告訴我們若 $a_1|l$ 且 $a_2|l$, 則 $M|l$. 再來由數學歸納法假設 $n=k-1$ 時成立, 即若令 $M'=a_1\cdots a_{k-1}$, 則 $M'|l$. 現考慮 $n=k$ 之情形, 此時 $M=a_1\cdots a_{k-1}a_k=M'a_k$. 由 (1) 知 $\gcd(a_k,M')=\gcd(a_k,M/a_k)=1$, 故由假設 $a_k|l$ 且 $M'|l$ 以及 Proposition 1.2.7(2) 知 $M'a_k=M|l$. □

接下來我們來看, 若我們會求兩個整數的最大公因數 (參見下一節之輾轉相除法) 那麼我們就可以兩個兩個地求得多個整數的最大公因數. 也就是說可以先求 $d_1 = \gcd(a_1, a_2)$ 求得 $d_2 = \gcd(a_1, a_2, a_3) = \gcd(d_1, a_3)$, 這樣一直下去以求得 $\gcd(a_1, a_2, \cdots, a_n)$. 我們的證明方法還是利用前述證明最大公因數方法進行.

Proposition 1.2.12. 若 $a_1, \ldots, a_n \in \mathbb{N}$ $(n > 2)$, 則

$$\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n).$$

Proof. 令 $d = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$ 首先我們要證明 d 是 $a_1, \ldots, a_n$ 的公因數. 由於 $d | \gcd(a_1, \ldots, a_{n-1})$ 由 Corollary 1.2.10 知 d 是 $a_1, \ldots, a_{n-1}$ 的公因數. 再加上 $d|a_n$, 故知 d 是 $a_1, \ldots, a_{n-1}, a_n$ 的公因數.

現假設 d' 是 $a_1, \ldots, a_{n-1}, a_n$ 的公因數. 當然 d' 是 $a_1, \ldots, a_{n-1}$ 的公因數, 故由 Corollary 1.2.10 知 $d' | \gcd(a_1, \ldots, a_{n-1})$. 再加上 $d'|a_n$, 故知 d' 是 $\gcd(a_1, \ldots, a_{n-1})$ 和 a_n 的公因數, 故再由 Corollary 1.2.5 知 $d' | \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n) = d$. 得證 d 是 $a_1, \ldots, a_n$ 的公因數中最大的數, 故為 $a_1, \ldots, a_n$ 的最大公因數. □

最後我們看看多個整數的最小公倍數的性質. 首先要注意的是 Proposition 1.2.8 中 $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$ 這個性質在多個整數時並不一定對. 例如前面所提 $a_1 = 6$, $a_2 = 15$ 以及 $a_3 = 10$ 的例子, 我們有 $a_1 a_2 a_3 = 900$, $\gcd(a_1, a_2, a_3) = 1$ 但是 $\operatorname{lcm}(a_1, a_2, a_3) = 30$. 雖然如此, 我們仍有公倍數為最小公倍數之倍數的性質, 而且求多個整數之最小公倍數也可如最大公因數一樣兩個兩個進行. 底下我們將利用數學歸納法同時證明這兩個性質. 這種重要的證明技巧大家或許沒有見過, 不過其原理如同一般的數學歸納法原理, 大家應能理解.

Proposition 1.2.13. 若 $a_1, \ldots, a_n \in \mathbb{N}$ $(n > 2)$, 則

$$\operatorname{lcm}(a_1, \ldots, a_{n-1}, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{n-1}), a_n).$$

而且 $m \in \mathbb{Z}$ 是 $a_1, \ldots, a_n$ 的公倍數若且唯若 $\operatorname{lcm}(a_1, \ldots, a_n) | m$.

Proof. 應用數學歸納法, 當 $n = 3$ 時令 $l = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2), a_3)$. 因為 l 為 $\operatorname{lcm}(a_1, a_2)$ 和 a_3 之公倍數, 知 l 為 $\operatorname{lcm}(a_1, a_2)$ 之倍數, 故由 Proposition 1.2.8 得知 l 為 a_1, a_2 的公倍數. 故 l 為 a_1, a_2, a_3 之公倍數. 現假設 m 為 a_1, a_2, a_3 之公倍數. 當然 m 是 a_1, a_2 之公倍數, 故由 Proposition 1.2.8 知 $\operatorname{lcm}(a_1, a_2) | m$. 又因 m 為 a_3 之倍數, 故知 m 為 $\operatorname{lcm}(a_1, a_2)$ 和 a_3 之公倍數. 因此再由 Proposition 1.2.8 知 $l = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2), a_3) | m$. 我們證得了 l 是 a_1, a_2, a_3 的正公因數中最小的數, 故得 $l = \operatorname{lcm}(a_1, a_2, a_3)$. 我們也同時證得 l 整除所有 a_1, a_2, a_3 的公倍數. 反之, 若 $l|m$, 則由 $a_1|l$, $a_2|l$ 以及 $a_3|l$ 知 m 為 a_1, a_2, a_3 的公倍數. 因此 $n = 3$ 的情形證明完成.

現依數學歸納法假設 $n = k - 1$ 時成立: 即

$$\operatorname{lcm}(a_1, \ldots, a_{k-1}) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{k-2}), a_{k-1})$$

且 $m \in \mathbb{Z}$ 是 $a_1, \ldots, a_{k-1}$ 的公倍數若且唯若 $\operatorname{lcm}(a_1, \ldots, a_{k-1}) | m$. 現考慮 $k = n$ 之情形. 令 $l' = \operatorname{lcm}(a_1, \ldots, a_{k-1})$ 且 $l = \operatorname{lcm}(l', a_k)$ 我們要證明 l 是 $a_1, \ldots, a_k$ 的最小公倍數.

由於 $l = \text{lcm}(l', a_k)$ 是 $l' = \text{lcm}(a_1, \ldots, a_{k-1})$ 的倍數, 故由數學歸納法假設 ($n = k-1$ 之情況) 知 l 為 $a_1, \ldots, a_{k-1}$ 的公倍數. 再加上 l 也是 a_k 的倍數, 故得知 l 是 $a_1, \ldots, a_k$ 的公倍數. 另一方面若 m 是 $a_1, \ldots, a_{k-1}, a_k$ 的公倍數, 當然 m 是 $a_1, \ldots, a_{k-1}$ 的公倍數. 故由數學歸納法假設知 $l' = \text{lcm}(a_1, \ldots, a_{k-1}) | m$. 再加上 $a_k | m$, 知 m 為 l' 和 a_k 之公倍數. 故由 Proposition 1.2.8 知 $l = \text{lcm}(l', a_k) | m$. 因而得知 l 確為 $a_1, \ldots, a_k$ 的正公倍數中最小者, 也就是說 $l = \text{lcm}(a_1, \ldots, a_k)$. 我們也同時證得若 m 為 $a_1, \ldots, a_k$ 的公倍數, 則 $l | m$. 反之若 $l | m$, 則由對所有 $i \in \{1, \ldots, k\}$ 皆有 $a_i | l$, 得證 $a_i | m$. 也就是說 m 為 $a_1, \ldots, a_k$ 的公倍數. □

1.3. 輾轉相除法

輾轉相除法是求最大公因數很有效率的方法. 首先我們介紹輾轉相除法的原理.

Lemma 1.3.1. 若 $a, b \in \mathbb{N}$ 且 $a = bh + r$, 其中 $h, r \in \mathbb{Z}$, 則 $\gcd(a, b) = \gcd(b, r)$.

Proof. 假設 $d_1 = \gcd(a, b)$ 且 $d_2 = \gcd(b, r)$. 我們證明 $d_1 | d_2$ 且 $d_2 | d_1$, 因而可利用 Proposition 1.1.3(2) 以及 d_1, d_2 皆為正數得證 $d_1 = d_2$.

因 $d_1 | a$ 且 $d_1 | b$ 利用 Corollary 1.1.2 我們知 $d_1 | a - bh = r$. 因為 $d_1 | b, d_1 | r$ 且 $d_2 = \gcd(b, r)$ 故由 Proposition 1.2.5 知 $d_1 | d_2$. 另一方面, 因為 $d_2 | b$ 且 $d_2 | r$ 故 $d_2 | bh + r = a$. 因此可得 $d_2 | d_1$. □

Lemma 1.3.1 告訴我們當 $a > b > 0$ 時, 要求 a, b 的最大公因數我們可以先將 a 除以 b 所得餘數若為 r, 則 a, b 的最大公因數等於 b 和 r 的最大公因數. 因為 $0 \leq r < b < a$, 所以當然把計算簡化了. 接著我們就來看看輾轉相除法. 由於 $\gcd(a, b) = \gcd(-a, b)$ 所以我們只要考慮 a, b 都是正整數的情況.

Theorem 1.3.2 (The Euclidean Algorithm)**.** 假設 $a, b \in \mathbb{N}$ 且 $a > b$. 由除法原理我們知存在 $h_0, r_0 \in \mathbb{Z}$ 使得

$$a = bh_0 + r_0, \quad \text{其中 } 0 \leq r_0 < b.$$

若 $r_0 > 0$, 則存在 $h_1, r_1 \in \mathbb{Z}$ 使得

$$b = r_0 h_1 + r_1, \quad \text{其中 } 0 \leq r_1 < r_0.$$

若 $r_1 > 0$, 則存在 $h_2, r_2 \in \mathbb{Z}$ 使得

$$r_0 = r_1 h_2 + r_2, \quad \text{其中 } 0 \leq r_2 < r_1.$$

如此繼續下去直到 $r_n = 0$ 為止. 若 $n = 0$ (即 $r_0 = 0$), 則 $\gcd(a, b) = b$. 若 $n \geq 1$, 則 $\gcd(a, b) = r_{n-1}$.

Proof. 首先注意若 $r_0 \neq 0$, 由於 $r_0 > r_1 > r_2 > \ldots$ 是嚴格遞減的, 因為 r_0 和 0 之間最多僅能插入 $r_0 - 1$ 個正整數, 所以我們知道一定會有 $n \leq r_0$ 使得 $r_n = 0$.

若 $r_0 = 0$, 即 $a = bh_0$, 故知 b 為 a 之因數, 得證 b 為 a, b 的最大公因數. 若 $r_0 > 0$, 則由 Lemma 1.3.1 知

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, 0) = r_{n-1}.$$

□

現在我們來看用輾轉相除法求最大公因數的例子.

Example 1.3.3. 我們求 $a = 481$ 和 $b = 221$ 的最大公因數. 首先由除法原理得 $481 = 2 \cdot 221 + 39$, 知 $r_0 = 39$. 因此再考慮 $b = 221$ 除以 $r_0 = 39$ 得 $221 = 5 \cdot 39 + 26$, 知 $r_1 = 26$. 再以 $r_0 = 39$ 除以 $r_1 = 26$ 得 $39 = 1 \cdot 26 + 13$, 知 $r_2 = 13$. 最後因為 $r_2 = 13$ 整除 $r_1 = 26$ 知 $r_3 = 0$, 故由 Theorem 1.3.2 知 $\gcd(481, 221) = r_2 = 13$.

在利用輾轉相除法求最大公因數時, 大家不必真的求到 $r_n = 0$. 例如在上例中可看出 $r_0 = 39$ 和 $r_1 = 26$ 的最大公因數是 13, 利用 Lemma 1.3.1 馬上得知 $\gcd(a, b) = 13$.

在上一節 Corollary 1.2.5 告訴我們若 $\gcd(a, b) = d$, 則存在 $m, n \in \mathbb{Z}$ 使得 $d = ma + nb$. 當時我們沒有提到如何找到此 m, n. 現在我們利用輾轉相除法來介紹一個找到 m, n 的方法. 我們沿用 Theorem 1.3.2 的符號. 首先看 $r_0 = 0$ 的情形, 此時 $d = \gcd(a, b) = b$ 所以若令 $m = 0$, $n = 1$, 則我們有 $d = b = ma + nb$. 當 $r_0 \neq 0$ 但 $r_1 = 0$ 時, 我們知 $d = \gcd(a, b) = r_0$. 故利用 $a = bh_0 + r_0$ 知, 若令 $m = 1$, $n = -h_0$, 則 $d = r_0 = ma + nb$. 同理若 $r_0 \neq 0$, $r_1 \neq 0$ 但 $r_2 = 0$, 則知 $d = \gcd(a, b) = r_1$. 故利用 $a = bh_0 + r_0$ 以及 $b = r_0h_1 + r_1$ 知

$$r_1 = b - r_0h_1 = b - (a - bh_0)h_1 = -h_1a + (1 + h_0h_1)b.$$

因此若令 $m = -h_1$ 且 $n = 1 + h_0h_1$, 則 $d = r_1 = ma + nb$. 依照此法, 當 r_0, r_1 和 r_2 皆不為 0 時, 由於 $d = \gcd(a, b) = r_{n-1}$ 故由 $r_{n-3} = r_{n-2}h_{n-1} + r_{n-1}$ 知 $d = r_{n-3} - h_{n-1}r_{n-2}$. 利用前面推導方式我們知存在 $m_1, m_2, n_1, n_2 \in \mathbb{Z}$ 使得 $r_{n-3} = m_1a + n_1b$ 且 $r_{n-2} = m_2a + n_2b$ 故代入得

$$d = (m_1a + n_1b) - h_{n-1}(m_2a + n_2b) = (m_1 - h_{n-1}m_2)a + (n_1 - h_{n-1}n_2)b.$$

因此若令 $m = m_1 - h_{n-1}m_2$ 且 $n = n_1 - h_{n-1}n_2$, 則 $d = ma + nb$.

上面的說明看似好像當 $r_0 \neq 0$ 時對每一個 $i \in \{0, 1, \ldots, n-2\}$ 要先將 r_i 寫成 $r_i = m_ia + n_ib$, 最後才可將 $d = r_{n-1}$ 寫成 $ma + nb$ 的形式. 其實這只是論證時的方便, 在實際操作時我們其實是將每個 r_i 寫成 $m_i'r_{i-2} + n_i'r_{i-1}$ 的形式慢慢逆推回 $d = ma + nb$. 請看以下的例子.

Example 1.3.4. 我們試著利用 Example 1.3.3 所得結果找到 $m, n \in \mathbb{Z}$ 使得 $13 = \gcd(481, 221) = 481m + 221n$. 首先我們有 $13 = r_2 = 39 - 26 = r_0 - r_1$. 而 $r_1 = 221 - 5 \cdot 39 = b - 5r_0$, 故得 $13 = r_0 - (b - 5r_0) = 6r_0 - b$. 再由 $r_0 = 481 - 2 \cdot 221 = a - 2b$, 得知 $13 = 6(a - 2b) - b = 6a - 13b$. 故得 $m = 6$ 且 $n = -13$ 會滿足 $13 = 481m + 221n$.

要注意這裡找到的 m, n 並不會是唯一滿足 $d = ma + nb$ 的一組解. 雖然上面的推演過程好像會只有一組解, 不過只能說是用上面的方法會得到一組解, 並不能擔保可找到所有的

解. 比方說若令 $m' = m + b$, $n' = n - a$, 則 $m'a + n'b = (m+b)a + (n-a)b = ma + nb = d$. 所以 m', n' 也會是另一組解. 所以以後當要探討唯一性時, 若沒有充分的理由千萬不能說由前面的推導過程看出是唯一的就斷言是唯一. 一般的作法是假設你有兩組解, 再利用這兩組解所共同滿足的式子找到兩者之間的關係. 我們看看以下的作法.

Proposition 1.3.5. 假設 $a, b \in \mathbb{N}$ 且 $d = \gcd(a, b)$. 若 $x = m_0, y = n_0$ 是 $d = ax + by$ 的一組整數解, 則對任意 $t \in \mathbb{Z}$, $x = m_0 + bt/d, y = n_0 - at/d$ 皆為 $d = ax + by$ 的一組整數解, 而且 $d = ax + by$ 的所有整數解必為 $x = m_0 + bt/d, y = n_0 - at/d$ 其中 $t \in \mathbb{Z}$ 這樣的形式.

Proof. 假設 $x = m, y = n$ 是 $d = ax + by$ 的一組解. 由於已假設 $x = m_0, y = n_0$ 也是一組解, 故得 $am + bn = am_0 + bn_0$. 也就是說 $a(m - m_0) = b(n_0 - n)$. 由於 $d = \gcd(a, b)$, 我們可以假設 $a = a'd$, $b = b'd$ 其中 $a', b' \in \mathbb{Z}$ 且 $\gcd(a', b') = 1$ (參見 Corollary 1.2.3). 因此得 $a'(m - m_0) = b'(n_0 - n)$. 利用 $b' | a'(m - m_0)$, $\gcd(a', b') = 1$ 以及 Proposition 1.2.7(1) 得 $b' | m - m_0$. 也就是說存在 $t \in \mathbb{Z}$ 使得 $m - m_0 = b't$. 故知 $m = m_0 + b't = m_0 + bt/d$. 將 $m = m_0 + bt/d$ 代回 $am + bn = am_0 + bn_0$ 可得 $n = n_0 - at/d$, 因此得證 $d = ax + by$ 的整數解都是 $x = m_0 + bt/d, y = n_0 - at/d$ 其中 $t \in \mathbb{Z}$ 這樣的形式. 最後我們僅要確認對任意 $t \in \mathbb{Z}$, $x = m_0 + bt/d, y = n_0 - at/d$ 皆為 $d = ax + by$ 的一組整數解. 然而將 $x = m_0 + bt/d, y = n_0 - at/d$ 代入 $ax + by$ 得 $a(m_0 + bt/d) + b(n_0 - at/d) = am_0 + bn_0 = d$, 故得證本定理. □

利用 Proposition 1.3.5 我們就可利用 Example 1.3.4 找到 $13 = 481x + 221y$ 的一組整數解 $x = 6, y = -13$ 得到 $x = 6 + 17t, y = -13 - 37t$ 其中 $t \in \mathbb{Z}$ 是 $13 = 481x + 221y$ 所有的整數解.

1.4. 質數

這一節我們要談整數的分解中最基本的元素: 質數. 大家都知道一個質數 p 就是正因數只有 1 和本身的數. 我們仍給一個正式的定義.

Definition 1.4.1. 若 $p \in \mathbb{Z}, p > 1$ 且 p 的正公因數只有 p 和 1 則稱 p 是一個質數 (prime number). 若一正整數有其他的正因數則稱為合成數 (composite number).

簡單來說質數就是無法分解成兩個較小的正整數乘積的數. 質數這一種不可分解的特性讓它有很多特殊性質. 例如給定一質數 p 以及一整數 $a \in \mathbb{Z}$, 我們很容易判定 $\gcd(a, p)$ 為何. 若 $d = \gcd(a, p)$ 則因 $d | p$, 知 $d = 1$ 或 $d = p$. 若 $d = p$ 表示 $p | a$, 所以我們知由 $p \nmid a$, 可得 $d = 1$. 所以利用 Proposition 1.2.7(1) 我們有以下之結論.

Lemma 1.4.2 (Euclid)**.** 假設 p 是一個質數, 且 $a, b \in \mathbb{Z}$. 若 $p | ab$, 則 $p | a$ 或 $p | b$.

Proof. 這裡我們要證明 $p | a$ 或 $p | b$. 如果 $p | a$ 當然就可以了 (不必擔心是否 $p | b$); 但若 $p \nmid a$, 那麼我們就得證明 $p | b$. 不過由前知 $p \nmid a$ 表示 $\gcd(p, a) = 1$, 故利用 Proposition 1.2.7(1) 得證 $p | b$. □

Euclid 這一個 Lemma 告訴我們一個質數若是 ab 的因數那它一定是 a, b 其中之一的因數. 事實上這個性質並不只適用在兩個整數相乘的情況, 我們很容易推廣至更多數相乘之情況.

Corollary 1.4.3. 假設 p 是一個質數, 且 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. 若 $p|a_1a_2\cdots a_n$, 則存在 $i \in \{1, \ldots, n\}$ 滿足 $p|a_i$.

Proof. 我們依然用數學歸納法證明. 當 $k = 2$ 時由 Lemma 1.4.2 知若 $p|a_1a_2$, 則 $p|a_1$ 或 $p|a_2$. 假設 $k = n - 1$ 時成立, 即若有 $n - 1$ 個整數 $a_1, \ldots, a_{n-1}$ 滿足 $p|a_1 \cdots a_{n-1}$, 則存在 $i \in \{1, \ldots, n-1\}$ 使得 $p|a_i$. 現考慮 $k = n$ 的情形, 若 $a_1, \ldots, a_n$ 是 n 個整數滿足 $p|a_1 \cdots a_n$, 則令 $a = a_1 \cdots a_{n-1}$, $b = a_n$. 此時由 $p|ab$ 及 Lemma 1.4.2 知 $p|a$ 或 $p|b$. 若 $p|a$, 則由數學歸納法假設知存在 $i \in \{1, \ldots, n-1\}$ 使得 $p|a_i$, 而若 $p|b$ 即 $p|a_n$, 故得證本定理. □

若一質數 p 是一整數 a 的因數, 則我們稱 p 是 a 的一個質因數. 當然了質數 p 本身就是 p 的質因數, 而一個合成數會不會有質因數呢? 大家很自然的覺得一定有, 我們還是給一個正式的證明.

Lemma 1.4.4. 假設 $a \in \mathbb{Z}$ 且 $a > 1$. 則必存在一質數 p 使得 $p|a$.

Proof. 我們用數學歸納法. 首先若 $a = 2$, 則由於 2 是質數我們得 $p = 2$ 為所求. 現假設對任意 $b \in \mathbb{Z}$ 滿足 $2 \le b \le n$ 的數皆存在質數 p 使得 $p|b$, 我們考慮 $a = n + 1$ 的情形. 若 a 本身是質數那當然 $p = a$ 為所求. 反之, 如果 a 不是質數依定義存在 $b \in \mathbb{Z}$ 且 $2 \le b < a$ 使得 $b|a$. 故由數學歸納法假設知存在一質數 p 滿足 $p|b$. 因此利用 Proposition 1.1.3(2) 得證 $p|a$. □

雖然正整數有無窮多個而 Lemma 1.4.4 告訴我們每一個大於 1 的正整數都有質因數, 但這並不代表會有無窮多個質數. 接著我們就是要探討質數確有無窮多個. 一般來說要證明質數有無窮多個或許會有的想法是希望利用現有的質數創造更大的質數. 不過這個想法是不可行的, 主要的原因是到目前為止我們沒有一個判別一個數是否為質數好的方法. 另類的思考是用反證法, 假設只有有限個質數而得到矛盾. 這個方法就不會碰到判別質數的問題, 相信由此大家更能體會到反證法的妙用.

Theorem 1.4.5 (Euclid)**.** 質數有無窮多個.

Proof. 我們用反證法假設只有有限個質數. 既然只有有限個我們可以將之一一列出, 就假設 $p_1, \ldots, p_n$ 是所有的質數. 現考慮 $a = p_1 \cdots p_n + 1$, 由 Lemma 1.4.4 知必有一質數 p_i, $i \in \{1, \ldots, n\}$ 滿足 $p_i|a$. 然而 p_i 本身整除 $p_1 \cdots p_n$ 故由 Corollary 1.1.2 知 $p_i|a - p_1 \cdots p_n$, 也就是說 $p_i|1$ 而得到矛盾. 故知不可能僅有有限多個質數, 而得證有無窮多個質數. □

質數雖然有無窮多個不過他們的分布不是非常稠密的. 例如給定任意大的整數 n 我們可以找到 n 個連續整數都不是質數. 我們的找法是考慮

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1$$

這 n 個連續整數. 很容意看出它們都不是質數. 就是質數這麼不容易出現加上很難判別一個很大的數是否為質數, 所以質數常被應用在密碼學中. 底下我們介紹一種最簡單判斷質數的方法.

Proposition 1.4.6. 若 $n>1$ 是一整數且對任意小於等於 $\sqrt{n}$ 的質數 p 皆不能整除 n, 則 n 為一質數.

Proof. 因為我們無法直接證明 n 會是質數, 所以需用反證法. 假設 n 不是質數, 依定義知存在 $a,b\in\mathbb{Z}$ 滿足 $1<a\leq b<n$ 且 $n=ab$. 由此我們可以確定 $a\leq\sqrt{n}$, 否則若 $a>\sqrt{n}$ 會造成 $ab>(\sqrt{n})^2=n$ 而與 $n=ab$ 不合. 而由 Lemma 1.4.4 知存在質數 p 使得 $p|a$. 既然 $p|a$ 我們得 $p\leq a\leq\sqrt{n}$ 且 $p|n$. 此與假設所有小於等於 $\sqrt{n}$ 的質數皆不整除 n 不符, 故知 n 為質數. □

Proposition 1.4.6 所提判別質數方法稱為篩法 (sieve method). 它可以幫助我們篩得哪些數是質數. 例如若要找出所有小於 100 的質數. 我們只要將小於 $\sqrt{100}=10$ 的質數 (即 $2,3,5,7$) 找出, 留下 $2,3,5,7$ 然後將其餘 $2,3,5,7$ 的倍數刪除, 經過這樣篩選後留下來小於 100 的數就都是小於 100 的質數. 這是因為若 $n<100$ 且不是質數, 則由 Proposition 1.4.6 知 n 必有一質因數小於等於 $\sqrt{n}<\sqrt{100}=10$. 因此被我們所刪除 $2,3,5,7$ 的倍數就是所有小於 100 的合成數, 自然剩下的便都是質數了.

質數既然有無窮多個, 接下來我們可以問是否有些特定形式的質數也會有無窮多個? 例如我們知道偶數中只有 2 是質數, 因此可以將所有奇數分類, 分成 $4n+1$ 和 $4n+3$ 這兩類然後問哪一類會有無窮多個質數. 要注意 $4n+1$ 這一類的數有一重要特性就是兩個 $4n+1$ 形式的數相乘仍然是 $4n+1$ 的形式. 因此任意有限多個 $4n+1$ 形式的數相乘仍是 $4n+1$ 的形式, 也就是說這一類的數有乘法封閉性. 另一方面 $4n+3$ 的形式的數就沒有這個特性, 事實上兩個 $4n+3$ 形式的數相乘會變成 $4n+1$ 的形式. 利用這兩類數的特性以及類似 Lemma 1.4.4 的證明, 我們有以下之結果.

Lemma 1.4.7. 假設 $a=4n+3$ 其中 $n\in\mathbb{N}\cup\{0\}$, 則必存在一質數 $p=4n'+3$ 其中 $n'\in\mathbb{N}\cup\{0\}$ 滿足 $p|a$.

Proof. 我們利用數學歸納法證明. 首先若 $a=3$, 則由於 3 是質數我們得 $p=3$ 為所求. 現假設對任意 $b=4k+3\in\mathbb{Z}$ 滿足 $0\leq k\leq n-1$ 的數皆存在質數 $p=4k'+3$ 使得 $p|b$, 我們考慮 $k=n$ 的情形. 若 a 本身是質數那當然 $p=a$ 為所求. 反之, 如果 a 不是質數依定義存在 $b,c\in\mathbb{N}$ 其中 $b<a$ 且 $c<a$ 使得 $a=bc$. 注意 b,c 中必有一個元素是 $4k+3$ 形式, 否則 b,c 都是 $4k+1$ 形式會造成 $bc=a$ 也是 $4k+1$ 形式的矛盾現象. 就假設 $b=4k+3$ 吧! 此時 $0\leq k\leq n-1$ (因 $b<a$), 故由歸納假設知存在 $p=4k'+3$ 使得 $p|b$, 因而得證 $p|a$. □

注意 $4n+1$ 形式的數並不一定有 $4n+1$ 形式的質因數. 9 就是最簡的的例子. 觀察由 Lemma 1.4.4 推得 Theorem 1.4.5 的關係, 同樣的我們也可利用 Lemma 1.4.7 推得 $4n+3$ 形式的質數有無窮多個.

Proposition 1.4.8. 集合 $S = \{4n+3 \mid n \in \mathbb{Z}, n \geq 0\}$ 中有無窮多個質數.

Proof. 我們依然用反證法假設 S 中只有有限多個質數並令 $p_0 = 3, p_1, \ldots, p_n$ 是 S 中所有的相異質數. 現考慮 $a = 4(p_1 \cdots p_n) + 3$. 由於 $a \in S$ 利用 Lemma 1.4.7 知必有一質數 $p \in S$ 滿足 $p|a$, 故由假設知存在 $i \in \{0, \ldots, n\}$ 使得 $p = p_i$, .

若 $p = p_0 = 3$, 則由 $3|a$, $3|3$ 以及 $a - 3 = 4(p_1 \cdots p_n)$ 得知 $3|4(p_1 \cdots p_n)$, 故由 Corollary 1.4.3 得到 $3|4$ 或者 $3|p_i$, $i \in \{1, \ldots, n\}$ 這樣的矛盾.

若 $p = p_i$ 其中 $i \in \{1, \ldots, n\}$, 則由 p_i 本身整除 $p_1 \cdots p_n$ 知 $p_i|a - 4(p_1 \cdots p_n)$, 也就是說 $p_i|3$ 而得到矛盾. 故得證 S 中不可能僅有有限多個質數. □

因為 Lemma 1.4.7 並不適用於 $4n+1$ 形式的整數, 所以 Proposition 1.4.8 的方法不能用來討論 $4n+1$ 形式的質數, 不過 $4n+1$ 形式的質數仍有無窮多個. 事實上數論一個很重要的定理 (Dirichlet Theorem) 告訴我們對任意互質的兩整數 a, b 皆有無窮多個 $an+b$ 形式的質數. 這個定理的證明超出本講義範圍, 我們就不再多談了.

1.5. 算數基本定理

算術基本定理 (The fundamental theorem of arithmetic) 即唯一分解定理, 告訴我們每一個大於 1 的整數若不是質數都可以寫成有限多個質因數的乘積且經過適當排序其寫法唯一. 此定理看似自然且明顯, 但仍需一個正式的證明.

這裡我們又碰到一個典型的有關存在性與唯一性的問題. 這裡的存在性指的就是對一大於 1 的整數可以找到有限多個質數使其可以寫成這些質數的乘積, 而唯一性就是指的就是寫法唯一. 由於正整數和負整數的分解只差一個負號, 我們只需考慮正整數的情況.

Theorem 1.5.1 (The Fundamental Theorem of Arithmetic)**.** 假設 $a \in \mathbb{N}$ 且 $a > 1$, 則存在 $p_1, \ldots, p_r$, 其中 p_i 是相異的質數, 滿足

$$a = p_1^{n_1} \cdots p_r^{n_r}, \quad n_i \in \mathbb{N}, \forall i \in \{1, \ldots, r\}.$$

如果 a 可以分解成另外的形式 $a = q_1^{m_1} \cdots q_s^{m_s}$, 其中 q_i 是相異的質數, 則 $r = s$ 且經過變換順序可得 $p_i = q_i$, $n_i = m_i$, $\forall\, i \in \{1, \ldots, r\}$.

Proof. 我們分開來證存在性與唯一性.

首先來看存在性: 簡單來說存在性就是要證明每一個大於 1 的整數都可以寫成有限多個(可以相同)質數的乘積. 如果 a 本身是個質數, 則 $a = p_1$ (即 $r = 1$, $n_1 = 1$), 得證存在性. 如果 a 不是質數呢? 由定義知存在 $a_1, b_1 \in \mathbb{N}$ 且 $a_1 \neq 1$, $b_1 \neq 1$ 滿足 $a = a_1 \cdot b_1$. 接下來就是看 a_1, b_1 是不是質數了. 如果其中有一個不是質數, 我們就繼續分解下去直到得到質數為止. 這個過程一定會停下來因為每次分解後得的數越來越小. 當然最後就可以將 a 寫成一些質數的乘積了. 這樣的證明方式, 相信大家會有一種說不清楚的感覺, 所以我們還是用數學歸納法來證明. 當 $a = 2$ 時由於 2 是質數, 所以在這情況存在性是對的. 接著假設對所有從 2 到 $a-1$ 的整數存在性是對的. 如果 a 是質數, 那存在性自然成立. 如果 a

不是質數, 則知 $a = a_1 \cdot b_1$ 其中 $a_1, b_1 \in \mathbb{N}$ 且 $1 < a_1 < a$ 及 $1 < b_1 < a$. 故利用歸納假設知 a_1 和 b_1 都可寫成有限多個質數的乘積, 所以得證 a 也可以寫成有限多個質數的乘積.

我們依然用歸納法證唯一性, 假設

$$a = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

其中 $p_1, \ldots, p_r$ 是兩兩相異的質數, 且 $q_1, \ldots, q_s$ 也是兩兩相異的質數. 由於 p_1 是質數, 故由 $p_1 \,|\, a = q_1^{m_1} \cdots q_s^{m_s}$ 以及 Corollary 1.4.3 知存在某個 $j \in \{1, \ldots, s\}$ 滿足 $p_1 \,|\, q_j$. 變換一下順序我們可以假設 $p_1 \,|\, q_1$. 由於 q_1 是質數, q_1 的因數只能是 ± 1 或 $\pm q_1$. 故由 $p_1 \,|\, q_1$ 知 $p_1 = q_1$. 現在考慮

$$\frac{a}{p_1} = p_1^{n_1 - 1} \cdots p_r^{n_r} = q_1^{m_1 - 1} \cdots q_s^{m_s}.$$

由於 $a/p_1 < a$, 故利用唯一性的歸納法假設我們得 $r = s$ 且 $p_1 = q_1, \ldots, p_r = q_r$ 以及 $n_1 = m_1$, $n_2 = m_2, \ldots, n_r = m_r$, 故得證唯一性. □

一般來說我們將一正整數 a 寫成質數之乘積 $a = p_1^{n_1} \cdots p_r^{n_r}$ 時, 為了唯一性我們要求每個質數 p_i 的次方 n_i 都是正的, 也就是說我們只挑出 a 的質因數 $p_1, \ldots, p_r$. 不過當要討論兩正數 a, b 時為了方便比較, 我們通常會挑出 a 和 b 所有的質因數再將 a, b 寫成這些質數之乘積的樣子. 也就是說可寫成 $a = p_1^{n_1} \cdots p_r^{n_r}$ 以及 $b = p_1^{m_1} \cdots p_r^{m_r}$ 其中對於 $i \in \{1, \ldots, r\}$, $p_i | a$ 或 $p_i | b$, 且 $n_i \geq 0$, $m_i \geq 0$. 注意這裡由於 a 的質因數未必就是 b 的質因數, 反之亦然, 所以 n_i, m_i 有可能為 0. 這樣寫法的方便性就是我們不必區分哪些 p_i 是 a 的質因數, 哪些是 b 的質因數. 利用這樣的寫法我們很容易將 a, b 的最大公因數表示出來.

Proposition 1.5.2. 假設 $a, b \in \mathbb{N}$ 且 $a, b > 1$. 若 $a = p_1^{n_1} \cdots p_r^{n_1}$ 且 $b = p_1^{m_1} \cdots p_r^{m_r}$, 其中 $p_1, \ldots, p_r$ 為相異質數且 $n_i, m_i \geq 0$, 則 a, b 的正公因數都可寫成 $p_1^{t_1} \cdots p_r^{t_r}$ 的形式, 其中 $0 \leq t_i \leq \min\{n_i, m_i\}$. 特別地, 我們有

$$\gcd(a, b) = p_1^{\min\{n_1, m_1\}} \cdots p_r^{\min\{n_r, m_r\}}.$$

Proof. 首先回顧一下 $\min\{x, y\}$ 表示 x, y 中最小之數. 現假設 d 是 a, b 的正公因數, 則由 $d|a$ 我們知若 p 是 d 的質因數, 則由 $p|d$ 知 $p|a$. 故由 Corollary 1.4.3 知存在 $i \in \{1, \ldots, r\}$ 使得 $p|p_i$. 因此由 p, p_i 皆為質數得 $p = p_i$. 也就是說 d 的質因數必在 $\{p_1, \ldots, p_r\}$ 中, 故 d 一定可以寫成 $p_1^{t_1} \cdots p_r^{t_r}$ 的形式, 其中 $t_i \geq 0$. 又由於對任意 $i \in \{1, \ldots, r\}$ 皆有 $p_i^{t_i} | d$ 故 $p_i^{t_i} | a$, 亦即 $p_i^{t_i} | p_1^{n_1} \cdots p_r^{n_r}$. 由於若 $i \neq j$ 則 $p_i \neq p_j$, 知此時 $\gcd(p_i^{t_i}, p_j^{n_j}) = 1$, 故由 1.2.7(1) 得 $p_i^{t_i} | p_i^{n_i}$, 也就是說 $t_i \leq n_i$. 同理由 $d|b$ 可得 $t_i \leq m_i$, 故得證 $0 \leq t_i \leq \min\{n_i, m_i\}$.

現令 $d = p_1^{\min\{n_1, m_1\}} \cdots p_r^{\min\{n_r, m_r\}}$, 馬上得知 d 為 a, b 之公因數. 又由上知任意 a, b 的公因數 d' 皆滿足 $d' | d$, 故知 $d = \gcd(a, b)$. □

雖然 Proposition 1.5.2 也是一個求得兩個數之最大公因數之方法, 不過在實際情況 (尤其是處理很大的數時) 由於分解質因數是很困難的事情, 所以仍是以輾轉相除法得最大公因數較管用. Proposition 1.5.2 重要之處是它很明確的告訴我們最大公因數長什麼樣子, 這在一些抽象理論的推導是有用的.

接下來我們可以利用 Proposition 1.2.8 將最小公倍數寫下.

Corollary 1.5.3. 假設 $a, b \in \mathbb{N}$ 且 $a, b > 1$. 若 $a = p_1^{n_1} \cdots p_r^{n_1}$ 且 $b = p_1^{m_1} \cdots p_r^{m_r}$, 其中 $p_1, \ldots, p_r$ 為相異質數且 $n_i, m_i \geq 0$, 則

$$\operatorname{lcm}(a, b) = p_1^{\max\{n_1, m_1\}} \cdots p_r^{\max\{n_r, m_r\}}.$$

Proof. 由於 $ab = p_1^{n_1+m_1} \cdots p_r^{n_r+m_r}$ 利用 Proposition 1.2.8 以及 Proposition 1.5.2 知

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)} = p_1^{n_1+m_1-\min\{n_1, m_1\}} \cdots p_r^{n_r+m_r-\min\{n_r, m_r\}}.$$

對任意二數 x, y, 不失一般性我們假設 $x \geq y$, 此時我們有 $\min\{x, y\} = y$ 且 $\max\{x, y\} = x$, 因此得 $x + y = \min\{x, y\} + \max\{x, y\}$. 所以對任意 $i \in \{1, \ldots, r\}$ 我們皆有 $\max\{n_i, m_i\} = n_i + m_i - \min\{n_i, m_i\}$, 因此得證本定理. □

當我們有多於兩個的整數時, 我們就可以利用質因數分解以及 Proposition 1.2.12 和 Proposition 1.2.13 將他們的最大公因數和最小公倍數寫下. 例如若 $a = p_1^{n_1} \cdots p_r^{n_1}$, $b = p_1^{m_1} \cdots p_r^{m_r}$ 且 $c = p_1^{t_1} \cdots p_r^{t_r}$, 其中 $p_1, \ldots, p_r$ 為相異質數且 $n_i, m_i, t_i \geq 0$, 則

$$\gcd(a, b, c) = p_1^{\min\{n_1, m_1, t_1\}} \cdots p_r^{\min\{n_r, m_r, t_r\}},$$
$$\operatorname{lcm}(a, b, c) = p_1^{\max\{n_1, m_1, t_1\}} \cdots p_r^{\max\{n_r, m_r, t_r\}}.$$

Chapter 2

Arithmetic Function

當我們要探討一數系時, 考慮定義在它上面的函數通常是一個重要的方法. 在數論中我們當然就是要探討定義在正整數上的函數, 我們稱之為 arithmetic function. 這一章中我們將討論幾個常見的 arithmetic function.

2.1. Multiplicative Arithmetic Functions

並不是所有的 arithmetic function 都很有趣, 到底要探討哪些 arithmetic function 呢? 這完全決定於於要探討的是有關哪些整數的特性. 因為在此我們著重於整數的分解性質, 所以我們探討所謂的 multiplicative arithmetic function.

Definition 2.1.1. 我們稱從 $\mathbb{N}$ 到 $\mathbb{C}$ 的函數為 *arithmetic function.* 若 $f:\mathbb{N}\to\mathbb{C}$ 是一個 arithmetic function 滿足對任意 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$ 皆有 $f(ab)=f(a)f(b)$, 則稱 f 是一個 *multiplicative arithmetic function.*

要注意當一個 arithmetic function f 是 multiplicative 時, $f(ab)=f(a)f(b)$ 並不一定成立. 這是要在 $\gcd(a,b)=1$ 時才可以確定是對的. 如果 f 的性質強到對任意 $a,b\in\mathbb{N}$ 皆有 $f(ab)=f(a)f(b)$, 那麼我們稱 f 是 *completely multiplicative.* 由於 completely multiplicative arithmetic function 的條件較強, 且並無太多這類有趣的函數, 所以這裡我們只專注於 multiplicative arithmetic function.

我們先來看一個 multiplicative arithmetic function 的例子.

Example 2.1.2. 我們考慮 Möbius μ-function, 其定義為

$$\mu(n)=\begin{cases}1, & \text{若 } n=1;\\ 0, & \text{若存在質數 } p \text{ 使得 } p^2|n;\\ (-1)^r, & \text{若 } n=p_1\cdots p_r, \text{ 其中 } p_1,\ldots,p_r \text{ 為相異質數.}\end{cases}$$

我們來驗證 μ 確為 multiplicative. 考慮 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$. 今若 $a=1$ 則由 $\mu(a)=\mu(1)=1$ 得 $\mu(ab)=\mu(b)=\mu(a)\mu(b)$. 同理若 $b=1$ 也得 $\mu(ab)=\mu(a)\mu(b)$. 所以我們僅要考慮 $a>1$ 且 $b>1$ 的情形. 由算數基本定理 (Theorem 1.5.1) 我們可以將 a,b

分別寫成 $a = p_1^{n_1} \cdots p_r^{n_r}$ 以及 $b = q_1^{m_1} \cdot q_t^{m_t}$ 的形式其中 n_i, m_j 皆大於 0 且由於 a, b 互質所有的質數 p_i 和 q_j 皆相異. 今若 n_i 或 m_j 中有一個大於 1, 不失一般性就假設 $n_1 \geq 2$, 則由 $p_1^2 | a$ 且 $p_1^2 | ab$, 知 $\mu(a) = 0$ 且 $\mu(ab) = 0$, 故得 $\mu(ab) = \mu(a)\mu(b)$. 最後我們只剩下 $n_1 = \cdots = n_r = 1$ 且 $m_1 = \cdots = m_t = 1$ 的情況. 此時由於 $ab = p_1 \cdots p_r \cdot q_1 \cdots q_t$ 且 $p_1, \ldots, p_r, q_1, \ldots, q_t$ 為相異質數得 $\mu(ab) = (-1)^{r+t}$. 然而 $\mu(a) = (-1)^r$ 且 $\mu(b) = (-1)^t$, 故得證 $\mu(ab) = \mu(a)\mu(b)$. 也就是說 μ 是一個 multiplicative arithmetic function.

要注意 μ 並非 completely multiplicative. 我們可以從 $a = b = p$, 其中 p 為質數的情形看出. 此時 $\mu(a) = \mu(b) = 1$ 但是 $\mu(ab) = 0$, 故知 $\mu(ab) \neq \mu(a)\mu(b)$. 要知道你要證一個 arithmetic function f 是 multiplicative 時, 你必須考慮所有的情況, 即對所有滿足 $\gcd(a, b) = 1$ 的正整數 a, b 皆要符合 $f(ab) = f(a)f(b)$, 而不能僅代個例子驗證. 但當你要說 f 不是 multiplicative 時, 只要找到一組 $a, b \in \mathbb{N}$ 且 $\gcd(a, b) = 1$ 會使得 $f(ab) \neq f(a)f(b)$ 即可.

接下來我們來看 multiplicative arithmetic function 的基本性質.

Proposition 2.1.3. 假設 f 是一個非 0 的 *multiplicative arithmetic function.* 則 $f(1) = 1$, 且若對任意的質數 p 以及 $t \in \mathbb{N}$, 都可知 $f(p^t)$ 的值則對任意 $n \in \mathbb{N}$, $f(n)$ 之值就可以確定.

Proof. 因 f 是 multiplicative 且 $\gcd(1, 1) = 1$, 故知 $f(1) = f(1)f(1)$ 得知 $f(1) = 1$ 或 $f(1) = 0$. 若 $f(1) = 0$, 則對任意 $n \in \mathbb{N}$, 由於 $\gcd(n, 1) = 1$, 可得 $f(n) = f(n)f(1) = 0$. 也就是說 f 是 0 函數, 此和 f 是非 0 含數之假設矛盾, 故知 $f(1) = 1$.

現對任意 $n \in \mathbb{N}$, 若 $n = 1$, 則由前知 $f(n) = f(1) = 1$. 若 $n > 1$, 則由算數基本定理知 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數且 $n_i \in \mathbb{N}$. 故由 f 是 multiplicative 且 $\gcd(p_1^{n_1}, p_2^{n_2} \cdots p_r^{n_r}) = 1$ 知 $f(n) = f(p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}) = f(p_1^{n_1}) f(p_2^{n_2} \cdots p_r^{n_r})$. 繼續下去使用數學歸納法知 $f(n) = f(p_1^{n_1}) \cdots f(p_r^{n_r})$. 故由假設已知這些 $f(p_i^{n_i})$ 之值我們可確定 $f(n)$ 之值. □

依 Proposition 2.1.3 我們知如果 f 是 multiplicative arithmetic function, 那麼若能掌握所有質數 p 以及 $t \in \mathbb{N}$ 中 $f(p^t)$ 之值那麼就可以完全了解 f 這一個函數. 不過前題是要確認 f 是否為 multiplicative. 底下我們會給一個常用來確認是 multiplicative 的方法. 這個方法不只可以拿來確認 multiplicative arithmetic function 而且可以幫助我們創造許多 multiplicative arithmetic function. 不過首先我們需要一個補助定理.

Lemma 2.1.4. 假設 $a, b \in \mathbb{N}$ 且 $\gcd(a, b) = 1$. 若 d 是 ab 的正因數, 則存在唯一的 a 的正因數 d_1 以及 b 的正因數 d_2 使得 $d = d_1 d_2$.

Proof. 這又是一個存在及唯一的問題. 存在就是要證存在 $d_1 | a$ 且 $d_2 | b$ 使得 $d = d_1 d_2$, 而唯一就是要證滿足這條件的寫法只有一種.

首先證明存在性. 給定 $d | ab$, 要如何找到 $d_1 | a$ 且 $d_2 | b$ 使得 $d = d_1 d_2$ 呢? 由於要求 $d_1 d_2 = d$ 以及 $d_1 | a$ 所以 d_1 必須是 a 和 d 的公因數. 思考一下, 我們可考慮取 d_1 為 a, d 的最大公因數, 這樣一來 $d_2 = d/d_1$ 會比較小比較可能整除 b. 就讓我們取 $d_1 = \gcd(a, d)$ 看

看是否可行. 此時令 $d_2 = d/d_1$, 我們確實有 $d = d_1d_2$ 且 $d_1|a$. 只剩下要驗證是否 $d_2|b$. 然而 $d|ab$ 故知 $(d/d_1)|(a/d_1)b$. 又由 $d_1 = \gcd(a,d)$ 知 $\gcd(a/d_1, d/d_1) = 1$ (Corollary 1.2.3), 故由 Proposition 1.2.7(1) 知 $d/d_1|b$, 也就是說 $d_2|b$.

接下來證唯一性. 給定 $d|ab$ 假設存在 $d_1, d_1', d_2, d_2' \in \mathbb{N}$ 分別滿足 $d = d_1d_2$, $d_1|a$ 且 $d_2|b$ 以及 $d = d_1'd_2'$, $d_1'|a$ 且 $d_2'|b$, 我們要證明 $d_1 = d_1'$ 且 $d_2 = d_2'$. 由於 $d_1d_2 = d_1'd_2'$, 我們知 $d_1|d_1'd_2'$. 又由於 $d_1|a$, $d_2'|b$ 以及 $\gcd(a,b) = 1$, 我們知 $\gcd(d_1, d_2') = 1$. 所以再利用 Proposition 1.2.7(1) 得知 $d_1|d_1'$. 同理可證 $d_1'|d_1$ 再加上 $d_1, d_1' \in \mathbb{N}$ 故知 $d_1 = d_1'$, 且得 $d_2 = d_2'$. □

在 Lemma 2.1.4 有關於存在性的證明中我們發現並未用到 $\gcd(a,b) = 1$ 的假設, 也就是說並不需假設 $\gcd(a,b) = 1$, 對任意 ab 的正因數都可以找到 $d_1|a$, $d_2|b$ 使得 $d = d_1d_2$. 不過在證明唯一性時, $\gcd(a,b) = 1$ 的假設就需要了. 比方說考慮 $a = 6$, $b = 4$ 和 $d = 6$ 的情形, 我們可以取 $d_1 = 6, d_2 = 1$ 和 $d_1' = 3, d_2' = 2$ 都滿足要求, 所以唯一性在此情況並不成立. 由此我們也再次強調唯一性絕不能用因為 a 和 d 的最大公因數是唯一的知 d_1 是唯一的而得證唯一性. 這是因為無從得知為何 d_1 非得是 a, b 的最大公因數不可. 所以在證明唯一性時, 大家還是要按部就班地先假設有兩種寫法再去說明這兩種寫法是一樣, 這樣的方法來處理比較不會出錯.

事實上 Lemma 2.1.4 告訴我們當 $\gcd(a,b) = 1$ 時, 若 $d_1, \ldots, d_i, \ldots, d_r$ 和 $e_1, \ldots, e_j, \ldots, e_s$ 分別是 a 和 b 所有的相異正因數, 則 $d_1e_1, \ldots, d_ie_j, \ldots, d_re_s$ 會是 ab 所有的相異正因數. 這是因為這些 d_ie_j 一定是 ab 的正因數, 再加上 Lemma 2.1.4 告訴我們 ab 的正公因數一定可以寫成 d_ie_j 的形式而且這些 d_ie_j 一定相異. 接下來我們就是要用這性質來利用一個已知的 multiplicative arithmetic function 得到新的 multiplicative arithmetic function.

Theorem 2.1.5. 假設 $f : \mathbb{N} \to \mathbb{C}$ 是一個 *multiplicative arithmetic function.* 考慮函數 $F : \mathbb{N} \to \mathbb{C}$ 其定義為對任意 $n \in \mathbb{N}$,

$$F(n) = \sum_{d|n, d>0} f(d),$$

則 F 是一個 *multiplicative arithmetic function.*

Proof. 首先解釋一下 $F(n) = \sum_{d|n,d>0} f(d)$ 這符號表示如果 $d_1, \ldots, d_r$ 是 n 的所有相異正因數那麼 $F(n) = f(d_1) + \cdots + f(d_r)$. 我們要證明 F 是 multiplicative 就是要證明當 $a, b \in \mathbb{N}$ 且 $\gcd(a,b) = 1$ 時 $F(ab) = F(a)F(b)$.

現假設 $d_1, \ldots, d_i, \ldots d_r$ 和 $e_1, \ldots, e_j, \ldots, e_s$ 分別是 a 和 b 所有的正因數. 我們有 $F(a) = f(d_1) + \cdots + f(d_i) + \cdots + f(d_r)$ 以及 $F(b) = f(e_1) + \cdots + f(e_j) + \cdots + f(e_s)$. 因此知 $F(a)F(b) = f(d_1)f(e_1) + \cdots + f(d_i)f(e_j) + \cdots + f(d_r)f(e_s)$. 由於 $\gcd(a,b) = 1$ 而 d_i, e_j 分別是 a, b 的因數, 我們知 $\gcd(d_i, e_j) = 1$. 再加上 f 是 multiplicative, 故得對所有 d_i, e_j 皆有 $f(d_i)f(e_j) = f(d_ie_j)$. 因此得 $F(a)F(b) = f(d_1e_1) + \cdots + f(d_ie_j) + \cdots + f(d_re_s)$. 然而 Lemma 2.1.4 告訴我們由於 $\gcd(a,b) = 1$, 這些 $d_1e_1, \ldots, d_ie_j, \ldots, d_re_s$ 剛好就是 ab 所有的相異正因數, 故得證 $F(ab) = F(a)F(b)$. □

最後我們來看看 Example 2.1.2 中的 μ 利用 Theorem 2.1.5 所創造出來的 multiplicative arithmetic function 為何.

Example 2.1.6. 令 $\delta : \mathbb{N} \to \mathbb{C}$ 是一個 arithmetic function 其定義為, 對任意 $n \in \mathbb{N}$,

$$\delta(n) = \sum_{d|n, d>0} \mu(d),$$

其中 μ 是 möbius μ-function. 因為 μ 是 multiplicative, 由 Theorem 2.1.5 知 δ 是 multiplicative. 故要決定 δ 之值由 Proposition 2.1.3 知只要先考慮 $\delta(p^t)$ 之值即可, 其中 p 是質數 $t \in \mathbb{N}$. 然而 p^t 所有的正因數為 $1, p, p^2, \ldots, p^t$, 故由定義知

$$\delta(p^t) = \mu(1) + \mu(p) + \mu(p^2) + \cdots \mu(p^t) = 1 - 1 + 0 + \cdots + 0 = 0.$$

故若 $n > 1$, 則由 $n = p_1^{n_1} \cdots p_r^{n_r}$ 知 $\delta(n) = \delta(p_1^{n_1}) \cdots \delta(p_r^{n_r}) = 0$. 然而由定義 $\delta(1) = \mu(1) = 1$, 所以我們可得

$$\delta(n) = \sum_{d|n, d>0} \mu(d) = \begin{cases} 1, & \text{當 } n = 1; \\ 0, & \text{當 } n > 1. \end{cases}$$

2.2. 正因數個數及正因數和

我們可以用 multiplicative arithmetic function 的概念很快的求出一正整數其正因數之個數及正因數和.

給定一正整數 n, 令 $v(n)$ 表示 n 的正因數個數. 既然對任意 $n \in \mathbb{N}$, $v(n)$ 都有取值, 所以我們可以將其看成是一個函數 $v : \mathbb{N} \to \mathbb{N}$. 從函數的角度來看, v 就是一個 arithmetic function. 給定 $n \in \mathbb{N}$ 如何求 $v(n)$ 值呢? 直接的作法就是將 n 的正因數一一列出然後數有多少個. 例如 6 的正因數有 $1, 2, 3, 6$, 所以 $v(6) = 4$. 這樣的求法如何用式子表示呢? 我們可以善用 summation $\sum$ 的符號, 將 $v(n)$ 寫成

$$v(n) = \sum_{d|n, d>0} 1.$$

上式的意思就是每次你看到 d 滿足 $d|n$ 且 $d > 0$ 就加一次, 所以很自然得到 n 的正因數個數.

Proposition 2.2.1. 對任意 $n \in \mathbb{N}$, 令 $v(n)$ 表示 n 的正因數個數. 則 $v : \mathbb{N} \to \mathbb{N}$ 是一個 *multiplicative arithmetic function.* 而且若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數, 則 $v(n) = (n_1 + 1) \cdots (n_r + 1)$.

Proof. 若令 $\mathbf{1} : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}$, $\mathbf{1}(n) = 1$, 則 $v(n)$ 可表為

$$v(n) = \sum_{d|n, d>0} \mathbf{1}(d).$$

由於對任意 $a, b \in \mathbb{N}$, $\mathbf{1}(ab) = \mathbf{1}(a)\mathbf{1}(b) = 1$, 我們知 $\mathbf{1}$ 為 (completely) multiplicative. 因此由 Theorem 2.1.5 知 v 為 multiplicative.

既然 v 是 multiplicative, 我們可以利用 Proposition 2.1.3 求對任意 $n \in \mathbb{N}$, $v(n)$ 之值. 也就是說我們要先探討對任意質數 p 以及正整數 t, $v(p^t)$ 之值. 由於 p^t 的正因數就是 p^i, 其中 $i \in \{0, 1, \ldots, t\}$, 我們得到 $v(p^t) = t + 1$. 因此對任意 $n \in \mathbb{N}$, 若 $n = 1$, 我們知 $v(n) = v(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 p_i 為相異質數, 則由 v 是 multiplicative 知

$$v(n) = v(p_1^{n_1}) \cdots v(p_r^{n_r}) = (n_1 + 1) \cdots (n_r + 1).$$

□

舉例來說, 我們要求 360 的正因數個數, 由於 $360 = 2^3 \cdot 3^2 \cdot 5$, 利用 Proposition 2.2.1, 我們很快就可得 $v(360) = (3+1)(2+1)(1+1) = 24$. 從這裡大家應更能體會 multiplicative arithmetic function 的好處. 或許求 $v(n)$ 的公式大家在高中時學排列組合時就用乘法原理得到過. 可以用乘法原理的原因其實就和 v 是 multiplicative 息息相關.

接下來我們探討正因數和. 給定一正整數 n, 令 $\sigma(n)$ 表示 n 的所有正因數之和. 既然對任意 $n \in \mathbb{N}$, $\sigma(n)$ 都有取值, 所以我們可以將其看成是一個函數 $\sigma : \mathbb{N} \to \mathbb{N}$. 從函數的角度來看, σ 就是一個 arithmetic function. 給定 $n \in \mathbb{N}$ 如何求 $\sigma(n)$ 值呢? 直接的作法就是將 n 的正因數一一列出然後全部加起來. 例如 6 的正因數有 $1, 2, 3, 6$, 所以 $\sigma(6) = 1 + 2 + 3 + 6 = 12$. 這樣的求法如何用式子表示呢? 我們再一次善用 summation $\sum$ 的符號, 將 $\sigma(n)$ 寫成

$$\sigma(n) = \sum_{d|n, d>0} d.$$

上式的意思就是每次你看到 d 滿足 $d|n$ 且 $d > 0$ 就加 d, 所以很自然得到 n 的正因數和.

Proposition 2.2.2. 對任意 $n \in \mathbb{N}$, 令 $\sigma(n)$ 表示 n 的正因數個數. 則 $\sigma : \mathbb{N} \to \mathbb{N}$ 是一個 *multiplicative arithmetic function.* 而且若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數, 則

$$\sigma(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{n_r+1} - 1}{p_r - 1}.$$

Proof. 若令 $\mathcal{I} : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}$, $\mathcal{I}(n) = n$, 則 $\sigma(n)$ 可表為

$$\sigma(n) = \sum_{d|n, d>0} \mathcal{I}(d).$$

由於對任意 $a, b \in \mathbb{N}$, $\mathcal{I}(ab) = ab = \mathcal{I}(a)\mathcal{I}(b)$, 我們知 $\mathcal{I}$ 為 (completely) multiplicative. 因此由 Theorem 2.1.5 知 σ 為 multiplicative.

既然 σ 是 multiplicative, 我們可以利用 Proposition 2.1.3 求對任意 $n \in \mathbb{N}$, $\sigma(n)$ 之值. 也就是說我們要先探討對任意質數 p 以及正整數 t, $\sigma(p^t)$ 之值. 由於 p^t 的正因數就是 p^i, 其中 $i \in \{0, 1, \ldots, t\}$, 我們得到 $\sigma(p^t) = 1 + p + \cdots + p^t$. 由於 $1, p, \ldots, p^t$ 是一個公比為 p 的等比數列, 我們得

$$\sigma(p^t) = \frac{p^{t+1} - 1}{p - 1}.$$

因此對任意 $n \in \mathbb{N}$, 若 $n = 1$, 我們知 $\sigma(n) = \sigma(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 p_i 為相異質數, 則由 σ 是 multiplicative 知

$$\sigma(n) = \sigma(p_1^{n_1}) \cdots \sigma(p_r^{n_r}) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{n_r+1} - 1}{p_r - 1}.$$

□

舉例來說, 我們要求 360 的正因數和, 由於 $360 = 2^3 \cdot 3^2 \cdot 5$, 利用 Proposition 2.2.2, 我們很快就可得

$$\sigma(360) = \frac{2^4 - 1}{2 - 1} \frac{3^3 - 1}{3 - 1} \frac{5^2 - 1}{5 - 1} = 15 \cdot 13 \cdot 6 = 1170.$$

2.3. The Euler ϕ-function

我們要探討比 n 小且與 n 互質的正整數個數.

Definition 2.3.1. 給定 $n \in \mathbb{N}$, $\phi(n)$ 表示比 n 小且與 n 互質的正整數個數. 這樣定出的函數 $\phi : \mathbb{N} \to \mathbb{N}$, 稱之為 Euler ϕ-function.

我們要證明 Euler ϕ-function 是 multiplicative, 並求其在任意正整數之取值. 由於不容易找到簡單的 multiplicative arithmetic function f 使得 ϕ 表示成如 Theorem 2.1.5 的形式, 所以我們要直接證明 ϕ 是 multiplicative. 也就是說對任意 $a, b \in \mathbb{N}$ 滿足 $\gcd(a, b) = 1$, 我們要證明 $\phi(ab) = \phi(a)\phi(b)$.

首先我們看一個 $a = 5, b = 4$ 的例子. 我們要說明 $\phi(20) = \phi(5)\phi(4)$. 由於 $\phi(20)$ 表示比 20 小且與 20 互質的正整數個數, 所以我們將小於等於 20 的正整數如下列出:

1	6	11	16
2	7	12	17
3	8	13	18
4	9	14	19
5	10	15	20

很容易看出最後一列 5 10 15 20 中每一個數都是 5 的倍數所以不可能和 20 互質, 因此我們要刪除這一列. 而其餘 4 列每一列中的數除以 5 的餘數都相同且都不等於 0 所以這 4 列的數都和 5 互質. 因此我們只要考慮這 4 列的數哪些和 4 是互質的. 仔細觀察這每一列中的數除以 4 的餘數都相異因此每列中只有餘 1 和餘 3 的兩個數和 4 互質. 總結來說我們發現共有 $\phi(5) = 4$ 列的數和 5 互質, 而這 4 列的數中每列皆有 $\phi(4) = 2$ 個數和 4 互質, 因此 1 到 20 之中共有 $\phi(5)\phi(4) = 8$ 個數和 5 且和 4 互質. 這些數就是 1 到 20 之中和 20 互質的數, 所以知 $\phi(20) = \phi(5)\phi(4)$.

接下來我們就是要用前面的方法證明一般的情形. 要注意前面的方法我們並無真正點出哪些數和 20 互質, 因為我們只想知道個數再加上我們的方法幾乎和 $a = 5, b = 4$ 無關所以比實際找出哪些數和 20 互質更能運用在一般的狀況. 首先我們用到和 20 互質的數就是和 5 且和 4 互質的數, 這個性質在一般的情況都對.

Lemma 2.3.2. 假設 $a, b, c \in \mathbb{Z}$. 則 $\gcd(ab, c) = 1$ 若且唯若 $\gcd(a, c) = 1$ 且 $\gcd(b, c) = 1$.

Proof. 假設 $\gcd(ab,c)=1$. 若 $d=\gcd(a,c)$, 表示 d 是 a,c 的公因數, 所以 d 也是 ab 和 c 的公因數, 故得 $d=1$. 同理知 $\gcd(b,c)=1$.

反之, 假設 $\gcd(a,c)=1$ 且 $\gcd(b,c)=1$. 若 $\gcd(ab,c)\neq 1$, 表示存在一質數 p 滿足 $p|\gcd(ab,c)$. 也就是說 $p|ab$ 且 $p|c$. 但 p 是質數, 故由 Lemma 1.4.2 知 $p|a$ 或 $p|b$. 得知 p 是 a,c 或 b,c 的公因數. 此和 $\gcd(a,c)=1$ 且 $\gcd(b,c)=1$ 相矛盾, 故知 $\gcd(ab,c)=1$. □

在前面求與 20 互質的數中, 另一個重要步驟是任一排中每一個數除以 4 的餘數都相異, 這在一般 $\gcd(a,b)=1$ 的情況都是對的.

Lemma 2.3.3. 假設 $a,b,l\in\mathbb{Z}$, $b>1$ 且 $\gcd(a,b)=1$. 則在 $l,l+a,l+2a,\ldots,l+(b-1)a$, 中每一個數除以 b 的餘數皆相異. 而且其中共有 $\phi(b)$ 個元素和 b 互質.

Proof. 若 $u,v\in\mathbb{Z}$ 且 u,v 除以 b 的餘數相同, 表示 $b|u-v$. 因此要說 $l,l+a,\ldots,l+(b-1)a$ 中的元素除以 b 的餘數皆相異, 就是說任取 $l+ia,l+ja$, 其中 $0\leq i<j\leq b-1$, 都無法使得 b 整除 $(l+ja)-(l+ia)$. 今假設 $b|(l+ja)-(l+ia)$, 也就是說 $b|(j-i)a$. 由於 $\gcd(a,b)=1$, Proposition 1.2.7(1) 告訴我們 $b|j-i$. 但此與 $0\leq i<j\leq b-1$ 相矛盾, 故由反證法知 b 不整除 $(l+ja)-(l+ia)$. 也就是說任取 $l+ia,l+ja$, 其中 $0\leq i<j\leq b-1$, 則它們除以 b 之餘數皆相異.

對於 $i\in\{0,1,\ldots,b-1\}$ 若令 r_i 表示 $l+ia$ 除以 b 的餘數, 由於 $0\leq r_i\leq b-1$ 且這 b 個 r_i 皆相異, 我們知 $\{r_0,r_1,\ldots,r_{b-1}\}$ 這一個集合和 $\{0,1,\ldots,b-1\}$ 是相同的. 然而 Lemma 1.3.1 告訴我們 $\gcd(l+ia,b)=\gcd(r_i,b)$, 所以 $\{l,l+a,\ldots,l+(b-1)a\}$ 中和 b 互質的數和 $\{0,1,\ldots,b-1\}$ 中和 b 互質的數之個數相同. 依定義知 $\{0,1,\ldots,b-1\}$ 中共有 $\phi(b)$ 個數與 b 互質, 故得證. □

接下來我們證明 ϕ 是一個 multiplicative arithmetic function.

Proposition 2.3.4. 若 $a,b\in\mathbb{N}$ 且 $\gcd(a,b)=1$, 則 $\phi(ab)=\phi(a)\phi(b)$.

Proof. 我們將小於 ab 的正整數依下列方法排成 b 列:

$$\begin{array}{cccc} 1 & 1+a & \cdots & 1+(b-1)a \\ 2 & 2+a & \cdots & 2+(b-1)a \\ \vdots & \vdots & \ddots & \vdots \\ a & 2a & \cdots & ba \end{array}$$

其中第 l 列為 $l,l+a,\ldots,l+(b-1)a$. 由 Lemma 1.3.1 知這裡每一數和 a 的最大公因數皆與 l 和 a 的最大公因數相同. 換言之, 若 l 和 a 互質則第 l 列中每一數皆和 a 互質; 而若 l 和 a 不互質則第 l 列中每一數皆和 a 不互質. 又因為 $1\leq l\leq a$, 故依定義共有 $\phi(a)$ 個 l 會與 a 互質. 而我們就僅考慮這 $\phi(a)$ 列的數 (其餘的數都和 a 不互質故和 ab 不互質).

這 $\phi(a)$ 列的數雖都和 a 互質但並不都和 b 互質. 然而每一列皆為 $l,l+a,\ldots,l+(b-1)a$ 的形式, 故由 $\gcd(a,b)=1$ 以及 Lemma 2.3.3 知每一列皆有 $\phi(b)$ 個數和 b 互質. 故 1 到 ab 中總共有 $\phi(a)\phi(b)$ 個元素和 a 且和 b 互質. 由 Lemma 2.3.2 這些數就是和 ab 互質的數. 故得證 $\phi(ab)=\phi(a)\phi(b)$. □

既然 ϕ 是 multiplicative, 我們就可以利用 Proposition 2.1.3 算出 ϕ 之值.

Proposition 2.3.5. 若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數, 則

$$\phi(n) = (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_r^{n_r} - p_r^{n_r-1}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

Proof. 我們先求對任意質數 p 以及正整數 t, $\phi(p^t)$ 之值. 由於 p 是 p^t 唯一的質因數, u 和 p^t 不互質表示 p 必為 u 之因數. 因此要計算小於 p^t 的正整數中有多少與 p^t 互質, 只要算出這些數中有哪些是 p 的倍數再扣掉即可. 然而 1 到 p^t 中共有 p^t/p 個數是 p 的倍數. 故得知 1 到 p^n 中共有 $p^t - p^{t-1}$ 個整數和 p^t 互質.

現考慮任意 $n \in \mathbb{N}$. 若 $n = 1$, 我們知 $\phi(n) = \phi(1) = 1$; 而若 $n = p_1^{n_1} \cdots p_r^{n_r}$ 其中 p_i 為相異質數, 則由 ϕ 是 multiplicative 知

$$\phi(n) = \phi(p_1^{n_1}) \cdots \phi(p_r^{n_r}) = (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_r^{n_r} - p_r^{n_r-1}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

□

既然 ϕ 是 multiplicative, 我們可以利用 Theorem 2.1.5 造出另一個 multiplicative arithmetic function. 考慮 $F : \mathbb{N} \to \mathbb{N}$ 其定義為對任意 $n \in \mathbb{N}$, $F(n) = \sum_{d|n, d>0} \phi(d)$. 由於 F 是 multiplicative, 且對任意質數 p 以及 $t \in \mathbb{N}$, 我們有

$$F(p^t) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^t) = 1 + (p-1) + (p^2 - p) + \cdots + (p^t - p^{t-1}) = p^t.$$

因此我們有以下之結果.

Corollary 2.3.6 (Gauss)**.** 若 $n \in \mathbb{N}$ 則

$$\sum_{d|n, d>0} \phi(d) = n.$$

Proof. 令 $F(n) = \sum_{d|n, d>0} \phi(d)$, 由前知 F 不是 0 函數故由 F 是 multiplicative, 利用 proposition 2.1.3 知 $F(1) = 1$. 若 $n \in \mathbb{N}$ 且 $n > 1$ 時, 將 n 寫成 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數, 再由上面 $F(p^t) = p^t$ 的結果及 Proposition 2.1.3 知

$$F(n) = F(p_1^{n_1}) \cdots F(p_r^{n_r}) = p_1^{n_1} \cdots p_r^{n_r} = n,$$

得證本定理. □

2.4. Convolution

我們可以利用 convolution 定義出新的 multiplicative arithmetic function, 另外 convolution 也提供了一個較簡明的方法來證明下一節要探討的 Möbius inversion formula. 雖然本節及下一節的內容在本講義中以後不會用到, 但希望利用此介紹讓大家知道有時適當定義一些運算對解決問題有很大的幫助.

Definition 2.4.1. 給定兩 arithmetic functions f, g 我們記其 *convolution* 為 $f * g$, 其定義為對任意 $n \in \mathbb{N}$,

$$f * g(n) = \sum_{d|n, d>0} f(d)g(n/d).$$

依照 convolution 的定義, 要求 $f * g(n)$ 之值, 首先找出 n 的所有正因數, 然後對於每一個 n 的正因數 d, 我們求 $f(d)g(n/d)$ 之值, 再將這些值加起來. 若 d 是 n 的正因數, 令 $e = n/d$, 我們自然有 $de = n$. 反之, 若 d, e 是正整數滿足 $de = n$, 則我們自然有 $d|n$. 因此我們也可以用如下的表示法表示 $f * g$. 即,

$$f * g(n) = \sum_{\substack{de=n \\ d,e\in\mathbb{N}}} f(d)g(e).$$

這樣的表示法雖然看來像兩個變數, 但實質上若給定 d, 則 e 自然確定. 我們選用這個表示法是因為底下要推導 convolution 的性質時用這種表法較簡明.

由於 f 和 g 是 arithmetic function, 所以 $f * g$ 在任意正整數皆有取值, 因此 $f * g$ 仍為 arithmetic function. 換言之 convolution 可以看成是一個 arithmetic function 之間的運算 (你可以將它看成是兩個 arithmetic function 之間的乘法). 接下來我們就是要探討這種運算的基本性質.

Proposition 2.4.2. 設 f, g, h 皆為 *arithmetic function.* 令 $\delta : \mathbb{N} \to \mathbb{N}$ 定義為

$$\delta(n) = \begin{cases} 1, & n = 1; \\ 0, & n > 1. \end{cases}$$

關於 *convolution* 我們有以下之性質.

(1) $f * \delta = \delta * f = f$.

(2) $f * g = g * f$.

(3) $(f * g) * h = f * (g * h)$.

Proof. (1) 依定義對任意 $n \in \mathbb{N}$, $f * \delta(n) = \sum_{d|n, d>0} f(d)\delta(n/d)$. 由於當 $n/d > 1$ 時 $\delta(n/d) = 0$. 因此在 $\sum$ 內, 只有 $d = n$ 這一項留下, 故得 $f * \delta(n) = f(n)\delta(1) = f(n)$. 換言之, f 和 $f * \delta$ 在任意 $n \in \mathbb{N}$ 的取值皆相同. 故從函數的觀點來看, 它們是相同的函數. 同理可證 $\delta * f = f$.

(2) 由於對任意 $n \in \mathbb{N}$,

$$f * g(n) = \sum_{\substack{de=n \\ d,e\in\mathbb{N}}} f(d)g(e) = \sum_{\substack{de=n \\ d,e\in\mathbb{N}}} g(e)f(d) = \sum_{\substack{de=n \\ d,e\in\mathbb{N}}} g(d)f(e) = g * f(n).$$

我們得證 $f * g = g * f$.

(3) 依定義, 對任意 $n \in \mathbb{N}$,

$$\begin{aligned}(f*g)*h(n) &= \sum_{\substack{de=n\\ d,e\in\mathbb{N}}} (f*g)(d)h(e)\\ &= \sum_{\substack{de=n\\ d,e\in\mathbb{N}}} \Big(\sum_{\substack{rs=d\\ r,s\in\mathbb{N}}} f(r)g(s)\Big)h(e)\\ &= \sum_{\substack{rse=n\\ r,s,e\in\mathbb{N}}} f(r)g(s)h(e).\end{aligned}$$

同理我們有

$$f*(g*h)(n) = \sum_{\substack{duv=n\\ d,u,v\in\mathbb{N}}} f(d)g(u)h(v).$$

因此得證 $(f*g)*h = f*(g*h)$. □

Proposition 2.4.2 告訴我們, 若將 $*$ 看成是 arithmetic function 之間的運算, 則 δ 這一個 arithmetic function 就如同乘法運算的 1 (這樣的元素, 我們稱之為 identity). 而且 $*$ 這個運算滿足交換率以及結合率. $*$ 這個運算其實對於 multiplicative arithmetic function 也具有封閉性. 也就是說我們有以下之性質.

Theorem 2.4.3. 假設 f, g 皆為 *multiplicative arithmetic function,* 則 $f*g$ 也是 *multiplicative arithmetic function.*

Proof. 假設 $a, b \in \mathbb{N}$ 且 $\gcd(a,b) = 1$, 我們要證明 $f*g(ab) = (f*g(a))(f*g(b))$. 對任意 $d, e \in \mathbb{N}$ 滿足 $de = ab$, 我們皆有 $d|ab$ 且 $e|ab$. 依 Lemma 2.1.4 知分別存在唯一的一組 d_1, d_2 以及 e_1, e_2 滿足 $d = d_1d_2$ 及 $e = e_1e_2$ 其中 d_1, e_1 為 a 的正因數 且 d_2, e_2 為 b 的正因數. 又因 $\gcd(a,b) = 1$, 故 $\gcd(d_1, d_2) = 1$ 且 $\gcd(e_1, e_2) = 1$. 所以由 f, g 是 multiplicative 以及定義知

$$f*g(ab) = \sum_{\substack{de=ab\\ d,e\in\mathbb{N}}} f(d)g(e) = \sum_{\substack{d_1d_2e_1e_2=ab\\ d_1|a,d_2|b,e_1|a,e_2|b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}} f(d_1)f(d_2)g(e_1)g(e_2).$$

現對任意 $d_1, d_2, e_1, e_2 \in \mathbb{N}$ 滿足 $d_1d_2e_1e_2 = ab$ 且 d_1, e_1 和 d_2, e_2 分別是 a 和 b 的因數. 因為 $d_1e_1|ab$, 又因 $\gcd(a,b) = 1$ 且 d_1, e_1 是 a 的因數, 知 $\gcd(d_1e_1, b) = 1$. 因此由 Proposition 1.2.7(1) 知 $d_1e_1|a$. 另一方面 $a|d_1e_1d_2e_2$, 再由 $\gcd(a,b) = 1$ 以及 d_2, e_2 為 b 之因數, 得 $\gcd(a, d_2e_2) = 1$. 因此知 $a|d_1e_1$. 所以得證 $a = d_1e_1$, 同理得證 $b = d_2e_2$. 反之, 若 $d_1, d_2, e_1, e_2 \in \mathbb{N}$ 滿足 $a = d_1e_1$ 且 $b = d_2e_2$, 則我們有 $d_1d_2e_1e_2 = ab$ 且 d_1, e_1 和 d_2, e_2 分別是 a 和 b 的因數. 因此我們有

$$\sum_{\substack{d_1d_2e_1e_2=ab\\ d_1|a,d_2|b,e_1|a,e_2|b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}} f(d_1)f(d_2)g(e_1)g(e_2) = \sum_{\substack{d_1e_1=a,d_2e_2=b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}} f(d_1)f(d_2)g(e_1)g(e_2).$$

另一方面

$$(f*g(a))(f*g(b)) = \sum_{\substack{d_1e_1=a\\ d_1,e_1\in\mathbb{N}}} f(d_1)g(e_1) \sum_{\substack{d_2e_2=b\\ d_2,e_2\in\mathbb{N}}} f(d_2)g(e_2).$$

利用分配率知

$$\sum_{\substack{d_1e_1=a\\ d_1,e_1\in\mathbb{N}}} f(d_1)g(e_1) \sum_{\substack{d_2e_2=b\\ d_2,e_2\in\mathbb{N}}} f(d_2)g(e_2) = \sum_{\substack{d_1e_1=a,d_2e_2=b\\ d_1,d_2,e_1,e_2\in\mathbb{N}}} f(d_1)f(d_2)g(e_1)g(e_2).$$

因此得證本定理. □

若令 $\mathbf{l}:\mathbb{N}\to\mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n\in\mathbb{N}$, $\mathbf{l}(n)=1$, 則對任意的 arithmetic function f, 皆有當 $n\in\mathbb{N}$ 時,

$$f*\mathbf{l}(n) = \sum_{\substack{de=n\\ d,e\in\mathbb{N}}} f(d)\mathbf{l}(e) = \sum_{d|n,d>0} f(d).$$

因為 $\mathbf{l}$ 是一個 multiplicative arithmetic function, 從這個角度看 Theorem 2.1.5 只是 Theorem 2.4.3 的一個特殊情況.

Example 2.4.4. 我們可以利用 Theorem 2.4.3 來求對任意 $n\in\mathbb{N}$,

$$\sum_{d|n,d>0} \mu(d)\frac{n}{d}$$

之值, 其中 μ 為 Möbius μ-function (參見 Example 2.1.2).

令 $\mathcal{I}:\mathbb{N}\to\mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n\in\mathbb{N}$, $\mathcal{I}(n)=n$. 考慮 $F:\mathbb{N}\to\mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n\in\mathbb{N}$,

$$F(n) = \sum_{d|n,d>0} \mu(d)\frac{n}{d} = \sum_{d|n,d>0} \mu(d)\mathcal{I}(\frac{n}{d}).$$

依定義我們知 $F=\mu*\mathcal{I}$. 然而 μ 和 $\mathcal{I}$ 皆為 multiplicative, 故利用 Theorem 2.4.3 知 F 也是 multiplicative. 因此我們只要檢視對任意質數 p 以及 $t\in\mathbb{N}$, $F(p^t)$ 之值為何. 依定義 $\mu(1)=1$, $\mu(p)=-1$ 且當 $i>1$ 時 $\mu(p^i)=0$, 故得

$$F(p^t) = \mu(1)\mathcal{I}(p^t) + \mu(p)\mathcal{I}(p^{t-1}) = p^t - p^{t-1}.$$

注意此和 $\phi(p^t)$ 的值相同 (參見 Proposition 2.3.5), 故利用 F 和 ϕ 皆為 multiplicative 以及 Proposition 2.1.3 知 $F=\phi$. 也就是說對任意 $n\in\mathbb{N}$ 皆有

$$\sum_{d|n,d>0} \mu(d)\frac{n}{d} = \phi(n).$$

2.5. The Möbius Inversion Formula

前面在介紹 Euler's ϕ-function 時, 我們曾提及不容易找到 arithmetic function f 將 ϕ-function 表成 $\phi(n)=\sum_{d|n,d>0} f(d)$ 這樣的形式. 事實上 Möbius inversion formula 可以幫助我們找到這樣的 f.

Theorem 2.5.1 (Möbius Inversion Formula)**.** 假設 F, f 皆為 *arithmetic function,* μ 為 *möbius* μ*-function.* 則對任意 $n \in \mathbb{N}$, F, f 滿足

$$F(n) = \sum_{d|n, d>0} f(d),$$

若且唯若對任意 $n \in \mathbb{N}$, F, f 滿足

$$f(n) = \sum_{d|n, d>0} F(d)\mu(\frac{n}{d}).$$

Proof. 令 $\mathbf{l} : \mathbb{N} \to \mathbb{N}$ 是一個 arithmetic function 滿足對任意 $n \in \mathbb{N}, \mathbf{l}(n) = 1$. 依 convolution 的定義我們要證明 $F = f * \mathbf{l}$ 若且唯若 $f = F * \mu$.

若 $F = f * \mathbf{l}$, 則 $F * \mu = (f * \mathbf{l}) * \mu$. 利用 Proposition 2.4.2(3) 知 $F * \mu = f * (\mathbf{l} * \mu)$. 然而對任意 $n \in \mathbb{N}$, $\mathbf{l} * \mu(n) = \mu * \mathbf{l}(n) = \sum_{d|n, d>0} \mu(d)$, 由 Example 2.1.6 知 $\mathbf{l} * \mu = \mu * \mathbf{l} = \delta$, 其中 $\delta : \mathbb{N} \to \mathbb{N}$ 定義為

$$\delta(n) = \begin{cases} 1, & n = 1; \\ 0, & n > 1. \end{cases}$$

換言之, 我們有 $F * \mu = f * (\mathbf{l} * \mu) = f * \delta$. 因而利用 Proposition 2.4.2(1) 得證 $F * \mu = f$.

反之, 若 $f = F * \mu$, 則 $f * \mathbf{l} = (F * \mu) * \mathbf{l} = F * (\mu * \mathbf{l})$. 故再利用 $\mu * \mathbf{l} = \delta$ 得知 $f * \mathbf{l} = F * \delta = F$. □

注意 Möbius inversion formula 需要對任意 $n \in \mathbb{N}$ 對才能使用. 也就是說你不能看到

$$F(6) = f(1) + f(2) + f(3) + f(6)$$

就下結論說

$$f(6) = F(1)\mu(6) + F(2)\mu(3) + F(3)\mu(2) + F(6)\mu(1) = F(1) - F(2) - F(3) + F(6).$$

需要檢驗所有 $n \in \mathbb{N}$ 都對才可下此結論 (至少在此例中還要多檢查 $F(1) = f(1)$, $F(2) = f(1) + f(2)$ 以及 $F(3) = f(1) + f(3)$).

Example 2.5.2. 現在我們來看看如何利用 Möbius inversion formula, 找到 f 使得 $\phi(n) = \sum_{d|n, d>0} f(d)$. 由 Möbius inversion formula 知此時 $f = \mu * \phi$. 由於 μ 和 ϕ 皆為 multiplicative, 由 Theorem 2.4.3 知 f 亦為 multiplicative. 因此我們先觀察對任意質數 p 以及 $t \in \mathbb{N}$, $f(p^t)$ 之值. 然而

$$f(p^t) = \sum_{d|p^t, d>0} \mu(d)\phi(\frac{p^t}{d}) = \mu(1)\phi(p^t) + \mu(p)\phi(p^{t-1}) = \phi(p^t) - \phi(p^{t-1}).$$

因此知 $f(p) = p - 1 - 1 = p - 2$ 且當 $t \geq 2$ 時 $f(p^t) = p^t - p^{t-1} - (p^{t-1} - p^{t-2}) = p^{t-2}(p-1)^2$. 因此若 $n = p_1^{n_1} \cdots p_r^{n_r}$, 其中 p_i 為相異質數, 可以得 $f(n) = f(p_1^{n_1}) \cdots f(p_r^{n_r})$. 但是接下來很難將 f 寫成很好的形式 (注意要區分有某個 $n_i = 1$ 的情形). 事實上若沒有 Möbius inversion formula, 我們也很難證出這個 f 確實滿足 $\mu(n) = \sum_{d|n, d>0} f(d)$. 所以當初在證明 ϕ 是 multiplicative 時, 我們並沒有利用 Theorem 2.1.5 證得.

事實上利用 Example 2.5.2 的方法我們可以證出任何的 arithmetic function F 皆可找到唯一的 arithmetic function f 使得對任意 $n \in \mathbb{N}$, 皆有 $F(n) = \sum_{d|n,d>0} f(d)$. 當我們找到的 f 是 multiplicative 時, Theorem 2.1.5 告訴我們 F 也是 multiplicative. 反之, 以下 Corollary 告訴我們若已知 F 是 multiplicative, 則找出的 f 一定也是 multiplicative.

Corollary 2.5.3. 假設 F, f 皆為 *arithmetic function.* 若對任意 $n \in \mathbb{N}$, 皆有

$$F(n) = \sum_{d|n,d>0} f(d)$$

且已知 F 是一個 *multiplicative arithmetic function,* 則 f 亦為一個 *multiplicative arithmetic function.*

Proof. 由 Theorem 2.5.1 知 $f = \mu * F$, 故由 μ 是 multiplicative 以及 F 是 multiplicative 的假設, 利用 Theorem 2.4.3 知 $f = \mu * F$ 亦為 multiplicative. □

Example 2.5.4. 前面幾節中我們曾利用 multiplicative arithmetic function 得到一些有趣的等式, 接下來的例子我們將利用 Möbius inversion formula 得到更多等式.

(1) 令 $v(n)$ 表示 n 的正因數個數. 已知對任意 $n \in \mathbb{N}$, 皆有

$$v(n) = \sum_{d|n,d>0} 1 = \sum_{d|n,d>0} \mathbf{l}(d),$$

其中對所有 $n \in \mathbb{N}$, $\mathbf{l}(n) = 1$, 故利用 Möbius inversion formula 知對任意 $n \in \mathbb{N}$,

$$1 = \mathbf{l}(n) = \sum_{d|n,d>0} \mu(d)v(\frac{n}{d}) = \sum_{d|n,d>0} v(d)\mu(\frac{n}{d}).$$

(2) 令 $\sigma(n)$ 表示 n 的所有正因數之和. 已知對任意 $n \in \mathbb{N}$ 皆有

$$\sigma(n) = \sum_{d|n,d>0} d = \sum_{d|n,d>0} \mathcal{I}(d),$$

其中對所有 $n \in \mathbb{N}$, $\mathcal{I}(n) = n$, 故利用 Möbius inversion formula 知對任意 $n \in \mathbb{N}$,

$$n = \mathcal{I}(n) = \sum_{d|n,d>0} \mu(d)\sigma(\frac{n}{d}) = \sum_{d|n,d>0} \sigma(d)\mu(\frac{n}{d}).$$

(3) 由 Corollary 2.3.6 知對任意 $n \in \mathbb{N}$ 皆有

$$n = \mathcal{I}(n) = \sum_{d|n,d>0} \phi(d),$$

故利用 Möbius inversion formula 知對任意 $n \in \mathbb{N}$, 皆有

$$\phi(n) = \sum_{d|n,d>0} \mu(d)\mathcal{I}(\frac{n}{d}) = \sum_{d|n,d>0} \mu(d)\frac{n}{d}.$$

Example 2.5.4(3) 的等式在前一節 Example 2.4.4 中我們曾用 multiplicative 的性質得到. 事實上 Example 2.5.4 中的等式都可以用 multiplicative 的性質得到. 不過要注意的是 Möbius inversion formula 並不侷限於 multiplicative 的情形, 它對一般的 arithmetic function 皆適用.

Chapter 3

Congruences

同餘 (congruence) 的概念就是將整數適當的分成有限多類, 使其仍能和整數一樣的運算, 從而得到一些整數的重要性質. 本章就是探討 congruence 的定義以及得到一些有關 congruence 的重要式子.

3.1. 同餘的分類

Congruence relation 是一個 equivalent relation. 首先我們探討 equivalent relation 的基本概念.

一般來說要將一個集合分類必須符合以下三個要素. 第一個就是, 自己和自己是同類的; 另一要素是若甲和乙是同類的則乙也必須和甲是同類的; 最後一個要素是如果甲和乙同類且乙和丙同類, 則甲必須和丙同類. 很多同學應該知道這樣的分類同類間的關係稱之為 *equivalence relation*. 我們還是用數學的方法給 equivalence relation 正式的定義.

Definition 3.1.1. 若一集合 S 中我們用 $a \sim b$ 表示 a 和 b 是同類的, 則這樣的分類若符合以下性質我們稱之為 equivalence relation:

(equiv1): 對所有 $a \in S$, 我們都有 $a \sim a$ (reflexivity).

(equiv2): 若 $a \sim b$, 則 $b \sim a$ (symmetry).

(equiv3): 若 $a \sim b$ 且 $b \sim c$, 則 $a \sim c$ (transitivity).

我們常用的 "=" 就是一個典型的 equivalent relation.

有些同學可能會覺得奇怪既然 (equiv2) 說: 若 $a \sim b$ 則 $b \sim a$. 那麼再利用 (equiv3) 我們可得 $a \sim a$. 為什麼還要強調 (equiv1) 呢? 主要原因是 (equiv1) 強調是 S 中的任一元素 a 都須符合 $a \sim a$. 如果我們只要求 (equiv2) 和 (equiv3), 那麼如果 S 中有一元素 a 在 S 中找不到任何的元素 b 使得 $a \sim b$, 那麼 a 就不一定滿足 $a \sim a$ 了. 因此會造成有的元素有可能沒有被分類到. 而符合 equivalence relation 的分類就確保每一個元素都會被分到某一類 (不過有可能某一類中只有一個元素).

到底用 equivalence relation 分類有什麼好處呢? 首先當然是如前所說由 (equiv1) 可得每一個元素都會被分到某一類. 另外由 (equiv2) 和 (equiv3) 知兩個不同類的集合不會有交集; 這是因為如果 b 在 A 類且在 B 類中, 則在 A 類中的任一元素 a 因和 b 是同類的故 $a \sim b$ 而 B 類中的任一元素 c 因也和 b 同類故 $b \sim c$. 故由 (equiv2) 和 (equiv3) 知 $a \sim c$. 也就是說 A 中的所有元素和 B 中的所有元素都同類. 這和 A 與 B 是不同類的假設相矛盾. 總而言之利用一個 equivalent relation 我們可以將一集合分割成兩兩互不相交的類別.

接下來我們就來探討同餘的分類法.

Definition 3.1.2. 給定一正整數 m, 如果 $a, b \in \mathbb{Z}$ 在除以 m 之下其餘數相同, 我們稱 a, b 在除以 m 之下是同餘的 (a is *congruent* to b modulo m), 且用符號 $a \equiv b \pmod{m}$ 來表示. 若 a 和 b 在除以 m 之下不同餘 (a is *incongruent* to b modulo m), 則用 $a \not\equiv b \pmod{m}$ 來表示.

要注意在談同餘時一定要先固定一個 m 才能說. 沒有 a 和 b 是同餘的說法, 你必須完整的說出 a 和 b 在除以什麼之下是同餘的才對.

雖然檢查 a, b 在除以 m 之下是否同餘, 依定義要檢查 a 和 b 除以 m 之餘數是否相同, 但事實上只要檢查 m 是否整除 $a - b$.

Lemma 3.1.3. 給定一正整數 m, 且 $a, b \in \mathbb{Z}$, 則 $a \equiv b \pmod{m}$ 若且唯若 $m | a - b$.

Proof. 依定義若 $a \equiv b \pmod{m}$ 則依定義存在 $h_1, h_2 \in \mathbb{Z}$ 使得 $a = mh_1 + r$ 及 $b = mh_2 + r$ 其中 $0 \leq r < m$. 故得 $a - b = m(h_1 - h_2)$ 也就是說 $m | a - b$.

反之假設 a, b 除以 m 之餘數分別為 r_1 及 r_2, 即分別存在 $h_1, h_2 \in \mathbb{Z}$ 使得 $a = mh_1 + r_1$ 及 $b = mh_2 + r_2$, 其中 $0 \leq r_1, r_2 < m$, 則知 $a - b = m(h_1 - h_2) + (r_1 - r_2)$. 故由假設 $m | a - b$ 得 $m | r_1 - r_2$. 又因 $0 \leq r_1, r_2 < m$, 知 $-m < r_1 - r_2 < m$, 故由 $m | r_1 - r_2$ 得 $r_1 = r_2$. □

我們可以利用 Lemma 3.1.3 很快的得到 congruent relation 是一個 equivalent relation.

Proposition 3.1.4. 給定一正整數 m, 則整數在除以 m 同餘的分類之下是一個 *equivalent relation.* 也就是說符合以下三個性質.

(1) 若 $a \in \mathbb{Z}$ 則 $a \equiv a \pmod{m}$.

(2) 若 $a \equiv b \pmod{m}$ 則 $b \equiv a \pmod{m}$.

(3) 若 $a \equiv b \pmod{m}$ 且 $b \equiv c \pmod{m}$, 則 $a \equiv c \pmod{m}$.

Proof. (1) 若 $a \in \mathbb{Z}$, 因 $a - a = 0$, 得 $m | a - a$. 故由 Lemma 3.1.3 知 $a \equiv a \pmod{m}$.

(2) 若 $a \equiv b \pmod{m}$ 由 Lemma 3.1.3 知 $m | a - b$, 故由 $m | b - a$ 得證 $b \equiv a \pmod{m}$.

(3) 若 $a \equiv b \pmod{m}$ 且 $b \equiv a \pmod{m}$, 則知 $m | a - b$ 且 $m | b - c$. 故知 $m | (a - b) + (b - c)$, 即 $m | a - c$. 也就是說 $a \equiv c \pmod{m}$. □

由於同餘的概念用分類的看法是很好的分類且這樣的看法談論一些性質很方便, 今後我們經常會用 "a 和 b 在 modulo m 之下是同類"的說法來表達: a 和 b 除以 m 之餘數相同.

既然用同餘的概念可將整數分類, 我們自然會問給定 $m \in \mathbb{N}$, 在 modulo m 之下可以分成幾類呢? 所有整數在除以 m 之下的餘數總共可能為 $0, 1, \ldots, m-1$, 所以得知共有 m 類. 分類好後在每一類中我們可以挑一個代表元素來代表這一類, 且每類中僅挑出一個代表而不重複, 這樣所挑出的代表我們給它一個特別名稱.

Definition 3.1.5. 給定一正整數 m, 若集合 S 有 m 個元素, 其中元素在 modulo m 之下兩兩不同類, 則稱 S 是一個 *complete residue system modulo* m.

若 S 是一個 complete residue system modulo m, 則因整數在 modulo m 之下是一個 equivalent relation, 所以 S 中的元素都會被分到某一類, 而且又已知 S 中的元素兩兩不同類, 再加上已知 $\mathbb{Z}$ 在 modulo m 之下共能被分成 m 類, 所以由 S 的元素個數為 m 知, 每一類中都可在 S 中找到唯一的元素代表此類. 換言之, S 中的元素足以代表 $\mathbb{Z}$ 在 modulo m 之下之分類. 例如 $\{0, 1, \ldots, m-1\}$ 就是一個常用的 complete residue system modulo m. 不過有時我們會因問題的需要選擇別種 complete residue system modulo m.

利用同餘分類除了是一個 equivalent relation 之外, 還有許多很好的性質. 例如在下一節我們會介紹可以在各類之間定義運算. 另外在 modulo m 之下, 我們發現其實同類的元素和 m 之最大公因數其實是相同的.

Lemma 3.1.6. 給定一正整數 m, 若 $a \equiv b \pmod{m}$, 則 $\gcd(a, m) = \gcd(b, m)$.

Proof. 若 $a \equiv b \pmod{m}$, 由定義知 a 和 b 在除以 m 之下之餘數相同, 設其為 r. 故由 Lemma 1.3.1 知 $\gcd(a, m) = \gcd(r, m) = \gcd(b, m)$. □

特別的若 a 和 m 是互質的, 則在 modulo m 之下和 a 同類的元素都和 m 互質. 也就是說若 S 是一個 complete residue system modulo m, 只要找出 S 中有哪些元素和 m 互質, 那麼這些元素所代表的分類裡每個元素都和 m 互質. 在 modulo m 之下到底有幾類的元素會和 m 互質呢? 我們就考慮 $S = \{0, 1, \ldots, m-1\}$ 這個 complete residue system modulo m 吧! S 中和 m 互質的元素個數依 Euler ϕ-function 的定義就是 $\phi(m)$ 個, 故知整數在 modulo m 之下共有 $\phi(m)$ 類的元素和 m 是互質的. 有時在處理問題時我們需要將這 $\phi(m)$ 類的代表元素列出, 所以我們也給它一個特別名稱.

Definition 3.1.7. 給定一正整數 m, 若集合 S 有 $\phi(m)$ 個元素, 其中的元素皆與 m 互質且在 modulo m 之下兩兩不同類, 則稱 S 是一個 *reduced residue system modulo* m.

當 m 是一質數 p 時, $\{1, \ldots, p-1\}$ 就是最常用的 reduced residue system modulo p.

3.2. 同餘的運算

同餘分類最重要的性質就是, 各類之間可以如整數一般作加法以及乘法的運算 (在有些情況甚至可以作除法).

給定 $m \in \mathbb{N}$, 在 modulo m 之下我們將同一類的元素看成是同樣的東西 (也就是將一整類的元素看成是一個元素), 想看看各類之間要如何相加相乘呢? 很自然的想法是在要相加

的兩類中各挑一個代表元素, 然後相加相乘看看落於哪一類. 不過這會碰到一個問題就是每一類中大家挑的代表元素若不同會不會相加相乘後所得結果不同呢? 例如在 modulo 5 之下, 我們要將除以 5 餘數為 2 的這一類和餘數為 3 的這一類相加. 若餘數為 2 和 3 的這兩類我們分別挑 2 和 3 來代表, 那麼由 $2+3=5$ 及 $2\times 3=6$ 得到相加相乘後會分別落在餘 0 和餘 1 的這兩類中. 如果挑不同的代表元素呢? 比方說餘 2 和餘 3 的這兩類我們分別挑 7 和 -12 當代表, 結果 $7+(-12)=-5$ 及 $7\times(-12)=-84$, 我們仍得到相加後落於除以 5 餘 0 這一類, 而相乘後落於除以 5 餘 1 這一類, 和前面結果一致. 我們不能由這個例子就認為這一定對, 需要想個方法來說明這是事實而不是巧合.

Lemma 3.2.1. 給定 $m\in\mathbb{N}$, 若 $a,b\in\mathbb{Z}$ 滿足 $a\equiv b \pmod m$, 則對任意 $c\in\mathbb{Z}$ 皆有

$$a+c\equiv b+c \pmod m \quad \text{and} \quad ac\equiv bc \pmod m.$$

Proof. 由假設 $a\equiv b \pmod m$ 知 $m|a-b$. 故得 $m|(a+c)-(b+c)$, 也就是說 $a+c\equiv b+c \pmod m$. 另一方面由於 $m|(a-b)c$ 故知 $m|ac-bc$, 得證 $ac\equiv bc \pmod m$.. □

Lemma 3.2.1 告訴我們兩個同類的數分別加上同一個數後所得之數也會同類. 同類的數同乘一個數後所得之數也同類. 依此我們就可以得到兩個同類的數分別加上(或乘上)另兩個同類的數其結果仍會同類.

Proposition 3.2.2. 給定 $m\in\mathbb{N}$, 若 $a,b,c,d\in\mathbb{Z}$ 滿足 $a\equiv b \pmod m$ 且 $c\equiv d \pmod m$, 則

$$a+c\equiv b+d \pmod m \quad \text{and} \quad ac\equiv bd \pmod m.$$

Proof. 因 $a\equiv b \pmod m$, 由 Lemma 3.2.1 知 $a+c\equiv b+c \pmod m$. 同理又因 $c\equiv d \pmod m$ 知 $b+c\equiv b+d \pmod m$, 故利用同餘是 equivalent relation (即 Proposition 3.1.4(3)) 知 $a+c\equiv b+d \pmod m$.

同樣的, 由 $a\equiv b \pmod m$ 及 $c\equiv d \pmod m$ 分別得 $ac\equiv bc \pmod m$ 及 $bc\equiv bd \pmod m$, 故知 $ac\equiv bd \pmod m$. □

由此定理, 我們以後要計算 1752 乘以 388 除以 5 之餘數, 我們不必將它們乘開後再看其除以 5 之餘數為何. 我們可以利用 $1752\equiv 2 \pmod 5$ 以及 $388\equiv 3 \pmod 5$ 很快的得到 $1752\times 388\equiv 6\equiv 1 \pmod 5$.

Proposition 3.1.4 (即 congruence relation 是 equivalent relation) 告訴我們當固定 $m\in\mathbb{N}$ 時 "$\equiv$" 有和等號相同的法則. 另一方面在 Lemma 3.2.1 中若令 $c=-1$, 則當 $a\equiv b \pmod m$ 時我們有 $-a\equiv -b \pmod m$. 所以套用 Proposition 3.2.2 知我們可以將 $\equiv$ "看成"是等號 (即將同餘的元素看成是相同) 而將同餘類的運算如一般整數作加, 減, 乘的運算. 例如在計算 5742 除以 11 的餘數時, 我們可以寫成 $5742=5\times 10^3+7\times 10^2+4\times 10+2$. 由於 $10\equiv -1 \pmod{11}$ 故得 $5742\equiv 5\times(-1)^3+7\times(-1)^2+4\times(-1)+2\equiv -5+7-4+2\equiv 0 \pmod{11}$. 也就是說 5742 可以被 11 整除, 這和我們中學時代所學判別 11 的倍數法則相同. 同理判別 9 的倍數法則也可由 $10\equiv 1 \pmod 9$ 而得. 你也可以利用 $10\equiv 3 \pmod 7$ 整理出一套判別 7 的倍數之法則 (當然會複雜多了).

這裡有兩點要特別注意: 首先, 在 modulo 不同的數之下所得的分類法不同, 所以不能將 $\equiv$ 混用. 例如若 $a = 3$, 我們可以說 $a \equiv 3 \pmod 5$ 且 $a \equiv 3 \pmod 7$, 但你不能因為 $a^2 \equiv 3^2 \equiv 4 \pmod 5$ 而說 $a^2 \equiv 4 \pmod 7$. 另外要注意的就是在一般等式中的除(約)在 congruence 並不一定適用. 也就是說若 $a \neq 0$ 且 $ab = ac$, 我們知 $b = c$ 但這在 congruence 的情況有可能出問題. 例如當 $a = 2, b = 2, c = 5$ 在 modulo 6 之下我們有 $a \not\equiv 0 \pmod 6$ 且 $ab \equiv ac \pmod 6$, 但很明顯的 $b \not\equiv c \pmod 6$. 所以在處理 congruence 的問題時要用除法消去一個數時要特別注意. 以下定理告訴我們何時可消, 何時不可消.

Proposition 3.2.3. 給定 $m \in \mathbb{N}$ 且假設 $a, b, c \in \mathbb{Z}$. 令 $d = \gcd(m, a)$ 則 $ab \equiv ac \pmod m$ 若且唯若 $b \equiv c \pmod{m/d}$.

Proof. 因 $d = \gcd(m, a)$, 我們令 $m = m'd$ 且 $a = a'd$, 由 Corollary 1.2.3 知 $\gcd(m', a') = 1$.

現假設 $ab \equiv ac \pmod m$, 即 $m|ab - ac$. 因此由 Lemma 1.1.5(2) 知 $(m/d)|(a/d)(b - c)$, 即 $m'|a'(b - c)$. 故因 $\gcd(m', a') = 1$ 利用 Proposition 1.2.7(1) 得證 $m'|b - c$, 即 $b \equiv c \pmod{m/d}$.

反之, 若 $b \equiv c \pmod{m/d}$, 即 $m'|b - c$. 因此由 Lemma 1.1.5(1) 得 $dm'|d(b - c)$, 即 $m|d(b - c)$. 也就是說 $db \equiv dc \pmod m$. 故由 Lemma 3.2.1 知 $a'db \equiv a'dc \pmod m$, 得證 $ab \equiv ac \pmod m$. □

例如之前的例子, 因為 $m = 6$ 且 $a = 2$, 得 $\gcd(m, a) = 2$. 故由 $ab \equiv ac \pmod 6$ 得 $b \equiv c \pmod 3$. 事實上, 上例中 $b = 2, c = 5$, 我們確實有 $2 \equiv 5 \pmod 3$.

到底在何時才能把 a 消掉且保持原來 modulo m 的 congruence 呢? 由 Proposition 3.2.3 我們知只有在 $\gcd(m, a) = 1$, 即 m 和 a 互質時才可保證對. 我們將這個重要的性質寫下.

Corollary 3.2.4. 給定 $m \in \mathbb{N}$ 且假設 $a, b, c \in \mathbb{Z}$. 若 m 和 a 互質, 則 $ab \equiv ac \pmod m$ 若且唯若 $b \equiv c \pmod m$.

其實若限制在整數時, 若 $a \neq 0$ 且 $ab = ac$ 可將 a 消去推得 $b = c$, 正確來說不能用"除"的概念來說, 而是用整數 $a \neq 0$ 且 $b \neq 0$ 則 $ab \neq 0$ 的性質得到. 這個概念在 congruence 的情況就不一定對, 例如 $2 \not\equiv 0 \pmod 6$ 且 $3 \not\equiv 0 \pmod 6$ 但是 $2 \times 3 \equiv 0 \pmod 6$. 這也是一般來說在 congruence 不能用約的方法消去的主要原因. 然而在考慮有理數時, 若 $a \neq 0$, 因為必存在另一有理數 a^{-1} 使得 $a \cdot a^{-1} = 1$, 所以若 $ab = bc$, 則兩邊同乘 a^{-1}, 可得 $b = c$. 這就是用除法" 約"的概念消去 a. 由於有理數中對任意非 0 元素 a, 其乘法反元素 (即 a^{-1}) 必存在, 使得我們在解有理數的方程式時更容易找到解. 在一般整數時雖然僅有 ± 1 其乘法反元素為整數, 但在討論 congruence 時有更多元素其乘法反元素會存在.

Proposition 3.2.5. 給定 $m \in \mathbb{N}$, 假設 $a \in \mathbb{Z}$, 則存在 $b \in \mathbb{Z}$ 滿足 $ab \equiv 1 \pmod m$ 若且唯若 a 和 m 互質.

Proof. 假設 $b \in \mathbb{Z}$ 滿足 $ab \equiv 1 \pmod m$, 即 $m|ab - 1$. 令 $d = \gcd(m, a)$, 可得 $d|m$ 且 $d|ab$. 故利用 $m|ab - 1$ 及 $d|m$ 可得 $d|ab - 1$, 再利用 $d|ab$ 得 $d|1$. 也就是說 a 和 m 互質.

反之, 若 a 和 m 互質, 即 $\gcd(m,a)=1$, 則由 Corollary 1.2.5 知存在 $r,s\in\mathbb{Z}$ 使得 $mr+as=1$. 故令 $b=s$, 我們有 $m|ab-1$, 亦即 $ab\equiv 1 \pmod m$. □

最後要強調, 當 a 和 m 互質時雖然有無窮多的整數 b 會滿足 $ab\equiv 1 \pmod m$, 但是這樣的 b 在 modulo m 之下是唯一的. 也就是說若 $c\in\mathbb{Z}$ 亦滿足 $ac\equiv 1 \pmod m$, 則由於 $ab\equiv 1\equiv ac \pmod m$ 以及 $\gcd(m,a)=1$, 套用 Corollary 3.2.4 我們得知 $b\equiv c \pmod m$. 有此唯一性, 我們特別稱 b 為 a 在 modulo m 之下的乘法反元素.

3.3. Euler's Theorem

一般在解方程式時, 我們經常需要乘法反元素來幫忙. 所以當 $m\in\mathbb{N}, a\in\mathbb{Z}$ 且 $\gcd(a,m)=1$ 時, 若能確實知道哪些 $b\in\mathbb{Z}$ 會滿足 $ab\equiv 1 \pmod m$ 將是很有用的. 由 Proposition 3.2.5 的證明中我們知可以利用輾轉相除法解 $mx+ay=1$ 的整數解來得到 b, 但這要在 m 和 a 皆是具體的數時才能操作. 我們將利用 Euler's Theorem 對一般的 m,a 都能將 b 確實找到.

給定 $m\in\mathbb{N}$, 若 $a,b\in\mathbb{Z}$ 滿足 $ab\equiv 1 \pmod m$, 則由 Proposition 3.2.5 知 a 和 b 皆與 m 互質. 換言之, 我們只要考慮和 m 互質的數即可, 所以我們自然考慮 reduced residue system modulo m.

Lemma 3.3.1. 給定 $m\in\mathbb{N}$, 考慮 $a\in\mathbb{Z}$ 滿足 $\gcd(m,a)=1$. 若 $\{r_1,\dots,r_{\phi(m)}\}$ 是一個 *reduced residue system modulo m,* 則 $\{ar_1,\dots,ar_{\phi(m)}\}$ 也是一個 *reduced residue system modulo m.*

Proof. 複習一下, $\{r_1,\dots,r_{\phi(m)}\}$ 是一個 reduced residue system modulo m 表示 $\gcd(m,r_i)=1$ 且對任意 $i\neq j$, 皆有 $r_i\not\equiv r_j \pmod m$. 現要證明 $\{ar_1,\dots,ar_{\phi(m)}\}$ 也是 reduced residue system modulo m, 我們需要證明 $\gcd(m,ar_i)=1$ 且對任意 $i\neq j$ 皆有 $ar_i\not\equiv ar_j \pmod m$.

現假設 $\gcd(m,ar_i)\neq 1$, 即存在一質數 p 滿足 $p|m$ 且 $p|ar_i$. 因 p 是質數, 故由 Lemma 1.4.2 得 $p|a$ 或 $p|r_i$. 換言之, p 為 m,a 的公因數或是 m,r_i 的公因數. 此和 $\gcd(m,a)=1$ 且 $\gcd(m,r_i)=1$ 相矛盾, 故得證 $\gcd(m,ar_i)=1$.

另一方面, 若 $i\neq j$ 且 $ar_i\equiv ar_j \pmod m$, 則由 $\gcd(m,a)=1$, 利用 Corollary 3.2.4 得 $r_i\equiv r_j \pmod m$. 此和 $r_i\not\equiv r_j \pmod m$ 矛盾, 故得證 $ar_i\not\equiv ar_j \pmod m$. □

前面提過, 給定 $m\in\mathbb{N}$, 利用除以 m 同餘的分類, 我們可以將與 m 互質的數分成 $\phi(m)$ 類. 而將每一類中挑出一代表元素所成之集合就是一個 reduced residue system modulo m. 今假若 $S=\{a_1,\dots,a_{\phi(m)}\}$ 和 $T=\{b_1,\dots,b_{\phi(m)}\}$ 皆為 reduced residue system modulo m, 任取 $a_i\in S$, 由於它代表與 m 互質的某一同餘類, 而 T 中也有一元素是在和 a_i 同類的元素中挑出. 換言之, 存在 $b_j\in T$ 滿足 $a_i\equiv b_j \pmod m$. 又由於這些 b_j 兩兩皆不同類, 所以 S 和 T 中元素在 modulo m 之下有一對一的對應關係. 也就是說經過適當的排序, 我們有 $a_i\equiv b_i \pmod m$. 因此得 $a_1\cdots a_{\phi(m)}\equiv b_1\cdots b_{\phi(m)} \pmod m$. 利用這個結果我們可以得證 Euler's Theorem.

Theorem 3.3.2 (Euler's Theorem)**.** 給定 $m \in \mathbb{N}$, 若 $a \in \mathbb{Z}$ 滿足 $\gcd(m,a) = 1$, 則

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof. 取 $S = \{r_1, \ldots . r_{\phi(m)}\}$ 為一個 reduced residue system modulo m. 首先我們證明 $\gcd(m, r_1 \cdots r_{\phi(m)}) = 1$. 若 $\gcd(m, r_1 \cdots r_{\phi(m)}) \neq 1$, 即存在一質數 p 使得 $p|m$ 且 $p|r_1 \cdots r_{\phi(m)}$. 利用 Corollary 1.4.3 知存在 $r_i \in S$ 使得 $p|r_i$, 也就是說 $\gcd(m, r_i) \neq 1$. 此和 S 是 reduced residue system modulo m 且 $r_i \in S$ 相矛盾, 故得證 $\gcd(m, r_1 \cdots r_{\phi(m)}) = 1$.

現由於 $\gcd(m,a) = 1$, 故利用 Lemma 3.3.1 知 $\{ar_1, \ldots, ar_{\phi(m)}\}$ 也是一個 reduced residue system modulo m, 因此得

$$r_1 \cdots r_{\phi(m)} \equiv (ar_1) \cdots (ar_{\phi(m)}) \equiv a^{\phi(m)}(r_1 \cdots r_{\phi(m)}) \pmod{m}.$$

再因為 $\gcd(m, r_1 \cdots r_{\phi(m)}) = 1$, 故利用 Corollary 3.2.4 得證 $a^{\phi(m)} \equiv 1 \pmod{m}$. □

給定 $m \in \mathbb{N}$ 及 $a \in \mathbb{Z}$ 滿足 $\gcd(m,a) = 1$, 若令 $b = a^{\phi(m)-1}$, 則利用 Euler's Theorem 得知 $ab \equiv a^{\phi(m)} \equiv 1 \pmod{m}$. 因此我們找到了 a 在 modulo m 之下的乘法反元素.

Corollary 3.3.3. 給定 $m \in \mathbb{N}$, 若 $a \in \mathbb{Z}$ 滿足 $\gcd(m,a) = 1$, 則令 $b = a^{\phi(m)-1}$, 會滿足 $ab \equiv ba \equiv 1 \pmod{m}$.

特別地, 當 m 是一個質數 p 時, Euler's Theorem 就是所謂的 Fermat's Little Theorem. 我們特別將它寫下來.

Theorem 3.3.4 (Fermat's Little Theorem)**.** 給定一質數 p, 若 $a \in \mathbb{Z}$ 滿足 $p \nmid a$, 則

$$a^{p-1} \equiv 1 \pmod{p}.$$

特別地, 若令 $b = a^{p-2}$, 則 $ab \equiv ba \equiv 1 \pmod{p}$.

Proof. 因 p 是一質數, 由 $p \nmid a$ 之假設知 $\gcd(p,a) = 1$. 又此時 $\phi(p) = p - 1$, 故直接套用 Theorem 3.3.2 得證 $a^{p-1} \equiv 1 \pmod{p}$. □

當 $p|a$ 時 Ferma's Little Theorem 並不對, 因為此時 $a \equiv 0 \pmod{p}$, 故 $a^{p-1} \equiv 0 \pmod{p}$. 不過我們可以推導出下一個對任意整數 a 皆成立的式子.

Corollary 3.3.5. 給定一質數 p, 則對任意整數 a 皆滿足

$$a^p \equiv a \pmod{p}.$$

Proof. 因為 p 是質數所以對任意 $a \in \mathbb{Z}$, 我們可以分成 $p|a$ 和 $p \nmid a$ 之情況處理. 當 $p|a$ 時, 由於 $a \equiv 0 \pmod{p}$, 故得 $a^p \equiv 0 \equiv a \pmod{p}$. 當 $p \nmid a$ 時, 由 Theorem 3.3.4 知 $a^{p-1} \equiv 1 \pmod{p}$, 故兩邊乘上 a 可得 $a^p \equiv a \pmod{p}$. □

3.4. Wilson's Theorem

當 p 是一個質數時, 若 $p \nmid a$, 則 Fermat's Little Theorem 告訴我們 a^{p-2} 在 modulo p 之下是 a 的乘法反元素. 雖然 a 的乘法反元素在 modulo p 之下是唯一的, Wilson's Theorem 給了我們在 modulo p 之下 a 的乘法反元素的另一種表法.

給定 $m \in \mathbb{N}$, 對於任意和 m 互質的整數 a, 由 Proposition 3.2.5 知都可以找到一個和 m 互質的整數 b 使得 $ab \equiv 1 \pmod{m}$, 我們也提及雖然這樣的 b 並不唯一, 但在 modulo m 的分類之下它會是唯一的. 也就是說只有在除以 m 之下和 b 同餘的整數才會符合. 這種在 modulo m 之下乘法反元素的存在唯一性用 modulo m 之下的 reduced residue system 最容易表達.

Lemma 3.4.1. 給定 $m \in \mathbb{N}$, 假設 $S = \{r_1, \ldots, r_{\phi(m)}\}$ 是一個 *reduced residue system modulo* m. 則對於任意 $r_i \in S$ 皆存在唯一的 $r_j \in S$ 使得 $r_i r_j \equiv 1 \pmod{m}$.

Proof. 因為 S 是一個 reduced residue system modulo m, 每一個 S 中的元素 s_i 皆和 m 互質, 故利用 Proposition 3.2.5 知存在 $b \in \mathbb{Z}$ 使得 $r_i b \equiv 1 \pmod{m}$. 由於 b 和 m 也是互質的, 故由 S 是一個 reduced residue system modulo m 之定義知必存在 $r_j \in S$ 和 b 在 modulo m 之下是同類的, 也就是說 $b \equiv r_j \pmod{m}$. 因此由 Lemma 3.1.3 知, $r_i r_j \equiv r_i b \equiv 1 \pmod{m}$. 證得存在性.

對於唯一性, 我們先假設 $r_j, r_k \in S$ 皆滿足 $r_i r_j \equiv 1 \pmod{m}$ 以及 $r_i r_k \equiv 1 \pmod{m}$. 因此得 $r_i r_j \equiv r_i r_k \pmod{m}$. 但由於 $\gcd(m, r_i) = 1$, 利用 Corollary 3.2.4 得 $r_j \equiv r_k \pmod{m}$. 但 S 是 reduced residue system modulo m 表示 S 中相異的元素在 modulo m 之下應是不同類的, 故由 $r_j \equiv r_k \pmod{m}$ 知 $r_j = r_k$. 得證唯一性. □

例如 $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ 是一個 reduced residue system modulo 11, 在 modulo 11 之下我們有

$$1 \times 1 \equiv 2 \times 6 \equiv 3 \times 4 \equiv 5 \times 9 \equiv 7 \times 8 \equiv 10 \times 10 \equiv 1 \pmod{11}.$$

在這個例子, S 中除了 1 和 10 以外其他的元素皆需與另外的元素相乘, 這在 modulo 一般的質數都是對的.

Lemma 3.4.2. 給定一質數 p. 則 $a \in \mathbb{Z}$ 滿足 $a^2 \equiv 1 \pmod{p}$ 若且唯若 $a \equiv \pm 1 \pmod{p}$.

Proof. 首先若 $a \equiv \pm 1 \pmod{p}$, 則 $a^2 \equiv (\pm 1)^2 \pmod{p}$. 得證 $a^2 \equiv 1 \pmod{p}$.

反之, 若 $a^2 \equiv 1 \pmod{p}$, 表示 $p | a^2 - 1$, 也就是說 $p | (a-1)(a+1)$, 故因 p 是質數, 利用 Lemma 1.4.2 得 $p | a-1$ 或 $p | a+1$. 也就是說 $a \equiv 1 \pmod{p}$ 或 $a \equiv -1 \pmod{p}$. □

要注意 Lemma 3.4.2 在 modulo 一般的非質數之下就不一定對了, 例如在 modulo 15 之下除了 1 和 14 外, 還有 4 會滿足 $4^2 \equiv 1 \pmod{15}$, 而且很顯然的 $4 \not\equiv \pm 1 \mod 15$. 所以要利用 Lemma 3.4.2, 我們必須限定在質數的情形, 此時我們可以得到 Wilson's Theorem.

Theorem 3.4.3 (Wilson's Theorem)**.** 給定一質數 p. 設 $\{r_1, \ldots, r_{p-1}\}$ 為一 *reduced residue system modulo p.* 則

$$r_1 \cdots r_{p-1} \equiv -1 \pmod{p}.$$

特別地, 我們有

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. 若 $p = 2$, 則 modulo 2 之下的 reduced residue system 為 $\{r_1\}$ 一個元素, 其中 $r_1 \equiv 1 \pmod{2}$. 但在 modulo 2 之下我們有 $1 \equiv -1 \pmod{2}$, 故得證 $r_1 \equiv -1 \pmod{2}$.

現考慮 $p > 2$ 的情形, 令 $S = \{r_1, \ldots, r_{p-1}\}$ 由於 $\gcd(p, 1) = \gcd(p, -1) = 1$ 且 $1 \not\equiv -1 \pmod{p}$ (否則 $p|2$), 故分別存在 $r_i, r_j \in S$ 其中 $r_i \neq r_j$ 滿足 $r_i \equiv 1 \pmod{p}$ 且 $r_j \equiv -1 \pmod{p}$. 因此不失一般性, 我們可假設 $r_1 \equiv 1 \pmod{p}$ 且 $r_2 \equiv -1 \pmod{p}$. 現考慮 $r_i \in S$, 其中 $3 \leq i \leq p-1$. 依 Lemma 3.4.1 知存在唯一的 $r_j \in S$ 使得 $r_i r_j \equiv 1 \pmod{p}$. 因為 $r_i \not\equiv \pm 1 \pmod{p}$, 故知 $r_j \not\equiv \pm 1 \pmod{p}$, 也就是說 $3 \leq j \leq p-1$. 又若 $r_i = r_j$, 會導致 $r_i^2 \equiv 1 \pmod{p}$, 這與 Lemma 3.4.2 相矛盾, 故知 $i \neq j$. 也就是說在 $T = \{r_3, \ldots, r_{p-1}\}$ 中任取一元素 r_i 必可找到唯一的另一元素 $r_j \in T$ 使得 $r_i r_j \equiv 1 \pmod{p}$. 因此我們可以對 T 中這 $p-3$ 個元素兩兩配對 (注意 p 是奇數), 使得每一對中元素相乘後除以 p 會餘 1. 也就是說 $r_3 \cdots r_{p-1} \equiv 1 \pmod{p}$. 因此我們得證

$$r_1 r_2 r_3 \cdots r_{p-1} \equiv r_1 r_2 \equiv -1 \pmod{p}.$$

最後由於 $\{1, 2, \ldots, p-1\}$ 是一個 modulo p 的 reduced residue system, 故知

$$1 \times 2 \times \cdots \times (p-1) = (p-1)! \equiv -1 \pmod{p}.$$

□

若 p 是一質數且 a 是和 p 互質的整數, 我們可以利用 Wilson's Theorem 找到在 modulo p 之下, a 的乘法反元素. 由於當 $a \equiv \pm 1 \pmod{p}$ 時 $a^2 \equiv 1 \pmod{p}$, 也就是說 a 本身在 modulo p 之下是自己的乘法反元素, 所以我們僅討論 $a \not\equiv \pm 1 \pmod{p}$ 的情況.

Corollary 3.4.4. 給定一質數 p 及 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 假設 $a \equiv i \pmod{p}$, 其中 $2 \leq i \leq p-2$. 若令

$$b = \frac{(p-2)!}{i}$$

則 $ab \equiv 1 \pmod{p}$.

Proof. 由於 $2 \leq i \leq p-2$, 我們知 b 是一個整數. 此時

$$ab \equiv i\frac{(p-2)!}{i} \equiv (p-2)! \pmod{p}$$

又由於 $(p-1)! = (p-1) \cdot (p-2)!$ 且 $p - 1 \equiv -1 \pmod{p}$, 故得證

$$ab \equiv (p-2)! \equiv -((p-1)!) \equiv 1 \pmod{p}.$$

□

我們仍要強調一下雖然 Lemma 3.4.1 在一般的 $m \in \mathbb{N}$ 都成立, 但 Lemma 3.4.2 需限制在質數時才成立, 所以 Wilson's Theorem 在 modulo 一般的 m 並不一定成立. 也就是說若 $\{r_1, \ldots, r_{\phi(m)}\}$ 是一個 reduced residue system modulo m, 並不一定可以得 $r_1 \cdots r_{\phi(m)} \equiv -1 \pmod{m}$. 例如在 modulo 15 之下我們之還有 4 和 -4 滿足 $4^2 \equiv (-4)^2 \equiv 1 \pmod{15}$, 所以利用 Theorem 3.4.3 的證明方法 (或直接計算) 我們可得, 若 $\{r_1, \ldots, r_8\}$ 是一個 reduced residue system modulo 15, 則 $r_1 \cdots r_8 \equiv 1 \pmod{15}$. 雖然利用 Theorem 3.4.3 的方法我們可以將 Wilson's Theorem 推廣到一般 m 的情形, 不過此時對一個 modulo m 的 reduced residue system $\{r_1, \ldots, r_{\phi(m)}\}$ 滿足 $r_i^2 \equiv 1 \pmod{m}$ 的 r_i 會有很多種情形, 討論起來較複雜, 在這裡我們就不多探討了.

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系數多項式中. 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 $f(x) = c_1 x + c_0$, 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 $f(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$, 其中 $c_i \in \mathbb{Z}$ 且 $c_k \neq 0$. 令 $g(x) = f(x) - (x - a)c_k x^{k-1}$, 則 $g(x) = (c_{k-1} + c_k a)x^{k-1} + \cdots c_1 x + c_0$ 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 $f(x) = (x - a)c_k x^{k-1} + (x - a)h_0(x) + r_0$. 故令 $h(x) = c_k x^{k-1} + h_0(x)$ 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 $f(x) = c_n x^n + \cdots + c_1 x + c_0$ 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 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 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 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 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 $m | a_n c^n + \cdots a_1 c + a_0$. 因此 $x \equiv c \pmod{m}$ 是 $f(x) \equiv 0 \pmod{m}$ 的一個解.

對任意 $t \in \mathbb{Z}$ 以及 $r \in \mathbb{N}$, 由於 $(c + m't)^r = c^r + rc^{r-1} m't + \cdots + rc(m't)^{r-1} + (m't)^r$, 我們可以將 $(c + m't)^r$ 寫成 $c^r + m'\lambda_r$, 其中 $\lambda_r \in \mathbb{Z}$. 因此

$$f(c + m't) = a_n (c + m't)^n + \cdots + a_1 (c + m't) + a_0 = f(c) + a_n m' \lambda_n + \cdots + a_1 m' \lambda_1.$$

因為 $d | a_i$, 故知 $dm' | a_i m'$, 也就是說 $a_i m' \equiv 0 \pmod{m}$. 所以我們得

$$f(c + m't) \equiv f(c) \equiv 0 \pmod{m},$$

也就是說對任意 $t \in \mathbb{Z}$, $x \equiv c + m't$ 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 $m | a_n c^n + \cdots + a_1 c + a_0$, 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.

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 4.2.2. 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 4.2.2 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 4.2.2 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 4.2.3. 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. 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, 對任意 $i \in \{1, \ldots, r\}$, $x \equiv c \pmod{p_i^{n_i}}$ 皆為 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 的解若且唯若 $x \equiv c \pmod{m}$ 為 $f(x) \equiv 0 \pmod{m}$ 之一個解.

Proof. 首先, 由於 $p_i^{n_i}|m$, 因此套用 Lemma 4.2.2 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 $i \in \{1, \ldots, r\}$ 皆滿足 $p_i^{n_i}|m$, 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 1.2.7(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 4.2.3 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? 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 4.2.3 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, 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 $d|b$ 若且唯若此 *congruence equation* 有解.

Proof. 因為 $d = \gcd(m, a)$ 故由 Corollary 1.2.5 知存在 $r, s \in \mathbb{Z}$ 使得 $d = rm + sa$.

現假設 $d|b$, 即存在 $b' \in \mathbb{Z}$ 使得 $b = b'd$. 因此 $b = b'd = b'rm + b'sa$, 故若令 $x = sb'$, 則 $ax = asb' = b - b'rm$. 也就是說 $m|ax - b$, 得證 $x \equiv sb' \pmod{m}$ 為 $ax \equiv b \pmod{m}$ 之一解.

反之, 若 $x \equiv c \pmod{m}$ 為 $ax \equiv b \pmod{m}$ 之一解, 即 $m|ac - b$. 換言之, 存在 $r \in \mathbb{Z}$ 使得 $ac - b = mr$, 也就是說 $b = ac - mr$. 現由於 $d = \gcd(m, a)$, 我們有 $d|m$ 且 $d|a$, 故得證 $d|b$. □

由 Proposition 4.3.1 的證明我們知道, 給定 $m \in \mathbb{N}$, 且 $a, b \in \mathbb{Z}$. 假設 $\gcd(m, a) = d$ 且 $d|b$. 若 $r, s, b' \in \mathbb{Z}$ 滿足 $d = rm + sa$ 且 $b = b'd$, 則 $x \equiv sb' \pmod{m}$ 為 $ax \equiv b \pmod{m}$ 的一個解. 不過這並不表示所有的解都可依此得到. 要如何找到所有的解呢? 按照以前我們常用的方法就是先探討兩解之間的關係, 再利用已知的一個解來找到所有的解. 接下來我們來看 $ax \equiv b \pmod{m}$ 其解之間的關係.

Proposition 4.3.2. 給定 $m \in \mathbb{N}$, 考慮一次的 *congruence equation* $ax \equiv b \pmod{m}$. 假設 $d = \gcd(m, a)$ 且已知 $x \equiv c \pmod{m}$ 是 $ax \equiv b \pmod{m}$ 的一個解, 則對任意 $ax \equiv b \pmod{m}$ 的解 c' 都會滿足 $c' \equiv c \pmod{m/d}$. 反之, 對任意的 $t \in \mathbb{Z}$,

$$x = c + \frac{m}{d}t$$

亦為 $ax \equiv b \pmod{m}$ 的一個解.

Proof. 假設 $x \equiv c' \pmod{m}$ 亦為 $ax \equiv b \pmod{m}$ 的一個解, 則由於已知 $x \equiv c \pmod{m}$ 為一解, 故得 $ac \equiv b \equiv ac' \pmod{m}$. 因此由 Proposition 3.2.3 知 $c \equiv c' \pmod{m/d}$.

反之, 若 $c' = c + (m/d)t$, 其中 $t \in \mathbb{Z}$, 則 $ac' = ac + (a/d)mt$. 因 $d = \gcd(m, a)$, 故知 $a/d \in \mathbb{Z}$, 也就是說 $ac' \equiv ac \pmod{m}$. 不過已知 $ac \equiv b \pmod{m}$, 所以得證 $ac' \equiv b \pmod{m}$. □

Proposition 4.3.2 告訴我們考慮 congruence equation $ax \equiv b \pmod{m}$. 若 $x \equiv c \pmod{m}$ 是一個解, 則其它的解皆為 $c + (m/d)t$ 這樣的形式, 其中 $d = \gcd(m, a)$ 且 $t \in \mathbb{Z}$. 因此知在 modulo m 之下 $x \equiv c + (m/d), x \equiv c + 2(m/d), \ldots, x \equiv c + (d-1)(m/d)$ 都會

是 $ax \equiv b \pmod{m}$ 的解. 我們將會證明這些解在 modulo m 之下皆相異, 而且在 modulo m 之下所有的解都可表為這些形式, 因此綜合 Proposition 4.3.1 以及 Proposition 4.3.2, 我們有以下之結果.

Theorem 4.3.3. 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.

Proof. 依 Proposition 4.3.1 以及 Proposition 4.3.2, 我們只剩下要證明 $ax \equiv b \pmod{m}$ 若有解, 則在 modulo m 之下共有 d 個解. 因此我們需證明兩件事: (一) 當 $0 \le i, j \le d-1$ 且 $i \ne j$ 時 $c + mi/d \not\equiv c + mj/d \pmod{m}$ (如此便可得當 $0 \le i \le d-1$ 時 $c + mi/d$ 在 modulo m 之下皆相異). (二) 對任意 $t \in \mathbb{Z}$, 皆存在 $i \in \{0, 1, \ldots, d-1\}$ 使得 $c + mt/d \equiv c + mi/d \pmod{m}$ (如此便得證所有的解確可寫為 $c + mi/d$, 其中 $0 \le i \le d-1$ 的形式).

假設 $0 \le i, j \le d-1$ 且 $i \ne j$. 不失一般性我們假設 $i > j$, 此時 $1 \le i - j \le d-1$. 若 $c + mi/d \equiv c + mj/d \pmod{m}$, 即 $(m/d)i \equiv (m/d)j \pmod{m}$. 由於 $\gcd(m/d, m) = m/d$, 故由 Proposition 3.2.3 知 $i \equiv j \pmod{m/(m/d)}$, 即 $i \equiv j \pmod{d}$. 也就是說 $d | i - j$. 此和 $1 \le i - j \le d-1$ 矛盾, 故得證 $c + mi/d \not\equiv c + mj/d \pmod{m}$.

現已知 $ax \equiv b \pmod{m}$ 的解皆為 $c + mt/d$, 其中 $t \in \mathbb{Z}$ 這樣的形式. 對任意 $t \in \mathbb{Z}$, 由 Theorem 1.2.1 知存在 $h, r \in \mathbb{Z}$ 使得 $t = hd + r$, 其中 $0 \le r \le d-1$. 因此得

$$c + mt/d = c + m(hd + r)/d = c + mh + mr/d.$$

故令 $i = r$, 我們有 $0 \le i \le d-1$ 且 $c + mt/d \equiv c + mi/d \pmod{m}$. 也就是說 $ax \equiv b \pmod{m}$ 的解皆為 $c + mi/d$, 其中 $0 \le i \le d-1$ 這樣的形式. □

由 Theorem 4.3.3 我們知若 $ax \equiv b \pmod{m}$ 有解, 只要解出其中一個解, 其他的解就可得到. 至於找解的方法, 除了 Proposition 4.3.1 的證明中所介紹的方法外, 事實上我們可以利用 Proposition 4.2.1 所提的方法來解. 因為此時若 $d = \gcd(m, a)$, 則 $d | b$, 也就是說 d 是 a, b 和 m 的公因數. 故若將 a, b, m 分別寫成 $a = a'd$, $b = b'd$ 和 $m = m'd$ 的形式 (其中 $a', b', m' \in \mathbb{Z}$ 且 $\gcd(m', a') = 1$), 利用 Proposition 4.2.1 我們知可以先解 $a'x \equiv b' \pmod{m'}$ 這一個 congruence equation. 由於 $\gcd(a', m') = 1$, 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 $x \equiv b'e \pmod{m}$ 為 $ax \equiv b \pmod{m}$ 的一個解. 至於此處 e (即 a' 在 modulo m' 之下的乘法反元素) 若不容易找, 可利用 Corollary 3.3.3 (Euler's Theorem) 找到. 我們看以下的例子.

Example 4.3.4. 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 4.3.3 知在 modulo 52 之下 $x \equiv 7, 20, 33, 46 \pmod{52}$ 為 $16x \equiv 8 \pmod{52}$ 的所有解.

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 4.2.3 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 $t_1, \ldots t_r$ 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 $M_1 e_1 \equiv 1 \pmod{m_1}$, 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 4.2.3 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 4.2.3 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 $i \in \{1, \ldots, r\}$, $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 皆有解若且唯若 $f(x) \equiv 0 \pmod{m}$ 有解.

Proof. 依 Proposition 4.2.3 知, 如果 $f(x) \equiv 0 \pmod{m}$ 有解, 則對任意 $i \in \{1, \ldots, r\}$, $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 皆有解.

現假設對任意 $i \in \{1, \ldots, r\}$, $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 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 $i \in \{1, \ldots, r\}$ 皆有 $c \equiv c_i \pmod{p_i^{n_i}}$. 也就是說任意 $i \in \{1, \ldots, r\}$, $x \equiv c \pmod{p_i^{n_i}}$ 為 $f(x) \equiv 0 \pmod{p_i^{n_i}}$ 之一解. 故再利用 Proposition 4.2.3 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:

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

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

(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 4.2.3 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 1.2.11(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

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

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.

Chapter 5

二次的 Congruence Equations

這一章中我們要專注於解二次的 congruence equation. 我們先從解一般的二次 congruence equation 開始, 然後慢慢化簡成簡單的形式, 最後介紹 quadratic reciprocity law. 整體來說我們會得到一個有效判別二次 congruence equation 是否有解的方法, 至於若有解如何求解就不在本章的討論範圍了. 我們希望能著重於學習如何由繁化簡的步驟.

5.1. 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 $ax^2+bx+c \equiv 0 \pmod m$ 解之情況.

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 $d=b^2-4ac$. 因此我們接下來僅探討 $x^2 \equiv a \pmod m$ 這樣的 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 4.4.3 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 5.1.1. 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:

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

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

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 $a=p^ia'$ 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 $x^2 \equiv p^ia' \pmod{p^n}$ 無解. 若有解且 b 為 $x^2 \equiv p^ia' \pmod{p^n}$ 之一解, 我們將 b 寫成 $b=p^sb'$, 其中 $p \nmid b'$. 此時因假設 $b^2 \equiv p^ia' \pmod{p^n}$, 可得 $p^n | p^{2s}b'^2-p^ia'$. 由於 $2s$ 是偶數而 i 是奇數, 知 $2s \ne i$. 如果 $2s>i$, 則 $p^{2s}b'^2-p^ia'=p^i(p^{2s-i}b'^2-a')$. 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 $p^{i+1} \nmid p^{2s}b'^2-p^ia'$. 此和 $p^n | p^{2s}b'^2-p^ia'$ 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 $x^2 \equiv p^ia' \pmod{p^n}$ 無解.

當 $a=p^ia'$ 其中 $p \nmid a'$, $0<i<n$ 且 $i=2k$ 是偶數時, 若我們將 x 寫成 $x=p^kt$, 此時解 $x^2 \equiv a \pmod{p^n}$ 等同於解 $(p^kt)^2 \equiv p^{2k}a' \pmod{p^n}$, 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 5.1.2. 給定一質數 p 及 $n \in \mathbb{N}$. 假設 $a = p^i a'$ 其中 $p \nmid a'$ 且 $1 \leq i \leq n-1$.

(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. 所以以後我們僅專注於 $x^2 \equiv a \pmod{p^n}$ 其中 $p \nmid a$ 的情形.

5.2. 解 $x^2 \equiv a \pmod{p^n}$

在前一節中我們知道一個二次的 congruence equation 可化簡成 $x^2 \equiv a \pmod{p^n}$, 其中 p 為質數, $n \in \mathbb{N}$ 且 $p \nmid a$ 這種形式的問題. 要注意此時由於 $p \nmid a$, 若 $x^2 \equiv a \pmod{p^n}$ 有解, 則其解必也與 p 互質, 否則會造成 $p|a$ 之矛盾. 接著我們就依 $p = 2$ 和 p 為奇質數兩種情形來討論 $x^2 \equiv a \pmod{p^n}$ 解之情況.

5.2.1. $p = 2$ 的情形. 我們先考慮 $x^2 \equiv a \pmod{2^n}$, 其中 $2 \nmid a$ 的情形. 由於 a 是奇數, 所以若有解其解必為奇數. 一開始當然是考慮 $n = 1$ 的情形, 此時因 a 是奇數, 得 $a \equiv 1 \pmod{2}$. 所以 $x^2 \equiv a \pmod{2}$, 即為 $x^2 \equiv 1 \pmod{2}$, 故必有解且解為 $x \equiv 1 \pmod{2}$.

當 $n = 2$ 時, 因為 $a \equiv 1, 3 \pmod{4}$, 我們僅要考慮 $x^2 \equiv 1 \pmod{4}$ 以及 $x^2 \equiv 3 \pmod{4}$ 兩種 congruence equations. 由於解必為奇數我們可以假設 $2k+1$ 為一解. 因此由 $(2k+1)^2 = 4k(k+1) + 1 \equiv 1 \pmod{8}$, 我們知 $x^2 \equiv 3 \pmod{4}$ 無解. 而 $x^2 \equiv 1 \pmod{4}$ 之解為 $x \equiv \pm 1 \pmod{4}$ (即所有奇數).

由上面討論知當 $n = 3$ 時, $x^2 \equiv 3, 5, 7 \pmod{8}$ 無解, 而 $x^2 \equiv 1 \pmod{8}$ 有解且解為 $x \equiv \pm 1, \pm 3 \pmod{8}$. $n > 3$ 時, 我們知道不能如此硬作下去, 可以利用數學歸納法得到以下結果.

Proposition 5.2.1. 假設 $n \geq 3$ 且 a 是一個奇數. 則 $x^2 \equiv a \pmod{2^n}$ 有解若且唯若 $a \equiv 1 \pmod{8}$.

Proof. 若 $a \equiv 3, 5, 7 \pmod{8}$, 則由前知 $x^2 \equiv a \pmod{8}$ 無解. 因為 $n \geq 3$, 故由 Lemma 4.2.2 知 $x^2 \equiv a \pmod{2^n}$ 無解. 因為 a 為奇數故僅剩下 $a \equiv 1 \pmod{8}$ 的情形未討論. 所以我們只要證明 $a \equiv 1 \pmod{8}$ 時 $x^2 \equiv a \pmod{2^n}$ 有解.

已知 $n = 3$ 時成立. 假設 $n = k-1$ $(k \geq 4)$ 時成立, 即當 $a \equiv 1 \pmod{8}$ 時, $x^2 \equiv a \pmod{2^{k-1}}$ 有解. 假設 $c \in \mathbb{Z}$ 是 $x^2 \equiv a \pmod{2^{k-1}}$ 的一個解 (即 $2^{k-1} | c^2 - a$), 也就是說 $c^2 = a + 2^{k-1}b$, 其中 $b \in \mathbb{Z}$. 我們想利用 c 找到 $x^2 \equiv a \pmod{2^k}$ 之解. 若 $c^2 = a + 2^{k-1}b$ 其中 b 為偶數, 則自然 $2^k | c^2 - a$, 得 c 為 $x^2 \equiv a \pmod{2^k}$ 之一解. 若 b 為奇數, 則考慮 $c' = c + 2^{k-2}$. 此時 $c'^2 = c^2 + 2^{k-1}c + 2^{2k-4} = a + 2^{k-1}(b+c) + 2^{2k-4}$. 由於 b 和 c 皆為奇數知 $2 | b + c$, 而且 $2k - 4 = k + k - 4 \geq k$ (因 $k \geq 4$), 故得 $c'^2 \equiv a \pmod{2^k}$. 得證 $x^2 \equiv a \pmod{2^k}$ 有解. □

我們已知 $x^2 \equiv a \pmod{2^n}$ 何時有解何時無解. 若有解時, 其在 modulo 2^n 之下會有多少解呢? 我們依然用兩個解之間的關係來探討.

Proposition 5.2.2. 假設 $n \geq 3$ 且 $a \equiv 1 \pmod 8$. 若 $x \equiv c \pmod{2^n}$ 是 $x^2 \equiv a \pmod{2^n}$ 的一個解, 則 $x \equiv c, c+2^{n-1}, -c, -c+2^{n-1} \pmod{2^n}$ 為 $x^2 \equiv a \pmod{2^n}$ 所有的解.

Proof. 若 $c' \in \mathbb{Z}$ 亦為一解, 則 $2^n | c^2 - c'^2$, 即 $2^n | (c-c')(c+c')$. 要注意因為 c 和 c' 皆為奇數, 我們可以有 $c \equiv \pm 1 \pmod 4$ 和 $c' \equiv \pm 1 \pmod 4$, 四種情形. 不過不管是哪一種情形 $c-c'$ 和 $c+c'$ 之中必有一個(且僅有一個)不能被 4 整除 (但仍為偶數). 例如在 $c \equiv 1 \pmod 4$ 及 $c' \equiv -1 \pmod 4$ 的情況, 我們有 $c+c \equiv 0 \pmod 4$ 但 $c-c' \equiv 2 \pmod 4$. 即 $2 | c-c'$ 但 $4 \nmid c-c'$. 我們先考慮 $4 \nmid c+c'$ 這種情形. 此時 $c+c' = 2\lambda$, 其中 λ 為奇數. 因此由前面已知 $2^n | (c-c')(c+c')$, 得 $2^n | 2\lambda(c-c')$, 即 $2^{n-1} | \lambda(c-c')$. 現由於 $\gcd(2, \lambda) = 1$, 故由 Proposition 1.2.7(1) 得 $2^{n-1} | c-c'$. 同理若 $4 \nmid c-c'$, 則知 $2^{n-1} | c+c'$.

總結來說, 若 c' 是 $x^2 \equiv a \pmod{2^n}$ 之一解, 則存在 $t \in \mathbb{Z}$ 使得 $c' = c + t2^{n-1}$ 或 $c' = -c + t2^{n-1}$. 反之若 $c' = c + 2^{n-1}$, 則 $c'^2 = c^2 + 2^n ct + 2^{2n-2}t^2$. 由於 $2n-2 \geq n+1$, 得 $c'^2 \equiv c^2 \equiv a \pmod{2^n}$. 故知 c' 為 $x^2 \equiv a \pmod{2^n}$ 之一解. 同理 $c' = -c + t2^{n-1}$ 亦為 $x^2 \equiv a \pmod{2^n}$ 之一解. 然而當 t 是奇數時 $c' = c + t2^{n-1} \equiv c + 2^{n-1} \pmod{2^n}$ 且 $c' = -c + t2^{n-1} \equiv -c + 2^{n-1} \pmod{2^n}$. 而當 t 是偶數時 $c' = c + t2^{n-1} \equiv c \pmod{2^n}$ 且 $c' = -c + t2^{n-1} \equiv -c \pmod{2^n}$. 故得知在 modulo 2^n 之下 $x^2 \equiv a \pmod{2^n}$ 共有 $x \equiv c, c+2^{n-1}, -c+2^{n-1}, -c \pmod{2^n}$ 這 4 個根 (注意因 c 為奇數, 所以這些數在 modulo 2^n 之下皆相異). □

我們來看個例子.

Example 5.2.3. 解 $x^2 \equiv 17 \pmod{32}$. 由於 $17 \equiv 1 \pmod 8$, 由 Proposition 5.2.1 知必有解. 我們利用 Proposition 5.2.1 證明中所用的方法來找出一個解. 首先解 $x^2 \equiv 17 \pmod{2^{5-1}}$, 即 $x^2 \equiv 1 \pmod{16}$. 可知 $x = 1$ 為 $x^2 \equiv 17 \pmod{16}$ 之一解. 但由於 $1^2 - 17 = 2^4 \times (-1)$ 且 -1 是奇數, 故利用 Proposition 5.2.1 的證明知 $1 + 2^{(5-2)} = 9$ 為 $x^2 \equiv 17 \pmod{32}$ 之一解. 找到一解後, 最後利用 Proposition 5.2.2 知 $x \equiv 9, 25, 7, 23 \pmod{32}$ 為 $x^2 \equiv 17 \pmod{32}$ 所有的解.

5.2.2. p **為奇質數的情形.** 當 p 是奇質數時, 我們當然不能如 $p = 2$ 的情形討論. 不過由 Lemma 4.2.2 我們知若 $x^2 \equiv a \pmod p$ 無解, 則對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ 亦無解. 我們要用數學歸納法證明若 $x^2 \equiv a \pmod p$ 有解, 則對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ 亦有解.

Proposition 5.2.4. 假設 p 為一奇質數且 $p \nmid a$. 則 $x^2 \equiv a \mod p$ 有解若且唯若對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ 有解.

Proof. 我們僅要證明若 $x^2 \equiv a \pmod p$ 有解則 $x^2 \equiv a \pmod{p^n}$ 亦有解.

若 c 為 $x^2 \equiv a \pmod p$ 之一解, 即存在 $\lambda \in \mathbb{Z}$ 使得 $c^2 = a + \lambda p$. 現考慮 $c' = c + tp$. 由於 $c'^2 = c^2 + 2ctp + t^2p^2 = a + (2ct + \lambda)p + t^2p^2$. 若要 $c'^2 \equiv a \pmod{p^2}$, 則需找到 $t \in \mathbb{Z}$

使得 $2ct \equiv -\lambda \pmod{p}$. 然而由於 $2c$ 和 p 互質, Theorem 4.3.3 告訴我們這樣的 t 一定存在. 故此時若令 $c' = c + tp$, 則 $x \equiv c' \pmod{p^2}$ 為 $x^2 \equiv a \pmod{p^2}$ 之一解.

現利用數學歸納法假設 $n = k-1$ $(k \geq 2)$ 時 $x^2 \equiv a \pmod{p^{k-1}}$ 有解, 且假設 $x \equiv c \pmod{p^{k-1}}$ 為其一解. 我們想利用 c 找到 $x^2 \equiv a \pmod{p^k}$ 的解. 由於存在 $\lambda \in \mathbb{Z}$ 使得 $c^2 - a = \lambda p^{k-1}$, 我們考慮 $c' = c + tp^{k-1}$. 此時 $c'^2 = c^2 + 2ctp^{k-1} + t^2p^{2k-2} = a + (2ct+\lambda)p^{k-1} + t^2p^{2k-2}$. 由於 $2k - 2 = k + k - 2 \geq k$ (因 $k \geq 2$) 我們得 $c'^2 \equiv a + (2ct + \lambda)p^{k-1} \pmod{p^k}$. 又因為 $2c$ 和 p 互質, 故存在 $t' \in \mathbb{Z}$ 使得 $2ct' + \lambda \equiv 0 \pmod{p}$. 此時若令 $c' = c + t'p$, 則 $x \equiv c' \pmod{p^k}$ 為 $x^2 \equiv a \pmod{p^k}$ 之一解. □

如果 $x^2 \equiv a \pmod{p^n}$ 有解, 我們當然有興趣知道在 modulo p^n 之下, $x^2 \equiv a \pmod{p^n}$ 其解的個數.

Proposition 5.2.5. 假設 p 為一奇質數, $p \nmid a$ 且 $n \in \mathbb{N}$. 若 $x^2 \equiv a \mod p^n$ 有解且 $x \equiv c \pmod{p^n}$ 為其一解, 則 $x \equiv \pm c \pmod{p^n}$ 為 $x^2 \equiv a \pmod{p^n}$ 所有的解.

Proof. 假設 c' 為 $x^2 \equiv a \pmod{p^n}$ 之另一解, 知 $p^n | c^2 - c'^2$. 由於 c 和 c' 皆與 p 互質, $c + c'$ 和 $c - c'$ 知中必有一個與 p 互質, 否則由 $p|c + c'$ 及 $p|c - c'$ 可得 $p|2c$, 而又 $p \neq 2$, 可得 $p|c$ 之矛盾. 現假設 $c + c'$ 與 p 互質, 此時 $\gcd(c + c', p^n) = 1$, 故由 $p^n|(c + c')(c - c')$ 及 Proposition 1.2.7(1), 得知 $p^n|c - c'$, 即 $c' \equiv c \pmod{p^n}$. 同理, 若 $c - c'$ 與 p 互質, 可得 $c' \equiv -c \pmod{p^n}$.

另一方面, 由 $c^2 \equiv a \pmod{p^n}$ 知 $(-c)^2 = c^2 \equiv a \pmod{p^n}$, 故知 $x \equiv \pm c \pmod{p^n}$ 為 $x^2 \equiv a \pmod{p^n}$ 所有的解. □

我們再來看個例子.

Example 5.2.6. 解 $x^2 \equiv 14 \pmod{125}$. 由於 $x^2 \equiv 14 \equiv 4 \pmod{5}$ 有解 ($x = 2$ 為一解), 由 Proposition 5.2.4 知 $x^2 \equiv 14 \pmod{125}$ 必有解. 我們利用 Proposition 5.2.4 證明中所用的方法來找出一個解. 首先找出 $x^2 \equiv 14 \pmod{25}$ 之一個解. 利用 2 為 $x^2 \equiv 14 \pmod{5}$ 之一解, 考慮 $(2 + 5t)^2 = 4 + 20t + 25t^2$. 因此 $(2 + 5t)^2 - 14 \equiv -10 + 20t \pmod{25}$. 也就是說需解出 $t \in \mathbb{Z}$ 使得 $20t \equiv 10 \pmod{25}$, 即解 $4t \equiv 2 \pmod{5}$. 可得 $t = 3$ 為一解, 故帶入 $2 + 5t$ 得 $x = 17$ 為 $x^2 \equiv 14 \pmod{25}$ 之一解. 現再利用 17 求 $x^2 \equiv 14 \pmod{125}$ 之一解. 考慮 $(17 + 25t)^2 = 289 + 850t + 625t^2$. 因此 $(17 + 25t)^2 - 14 \equiv 275 + 850t \equiv 25 + 100t \pmod{125}$. 也就是說需解出 $t \in \mathbb{Z}$ 使得 $100t \equiv -25 \pmod{125}$, 即解 $4t \equiv -1 \pmod{5}$. 可得 $t = 1$ 為一解, 故帶入 $17 + 25t$ 得 $x = 42$ 為 $x^2 \equiv 14 \pmod{125}$ 之一解. 找到一解後, 最後利用 Proposition 5.2.2 知 $x \equiv \pm 42 \pmod{125}$ 為 $x^2 \equiv 14 \pmod{125}$ 所有的解.

我們已完全了解 $x^2 \equiv a \pmod{2^n}$ 的解的情況. 而當 p 是奇質數時, 對任意 $n \in \mathbb{N}$, $x^2 \equiv a \pmod{p^n}$ (其中 $p \nmid a$) 的解的情況完全取決於 $x^2 \equiv a \pmod{p}$ 的解的情況. 所以以後我們僅專注於 $x^2 \equiv a \pmod{p}$ 其中 p 為奇質數且 $p \nmid a$ 的情形.

5.3. The Legendre Symbol

我們已經把解一般的二次 congruence equation 一步一步的化簡到解 $x^2 \equiv a \pmod{p}$, 其中 p 為奇質數且 $p \nmid a$ 的情形. 這裡我們將探討何時 $x^2 \equiv a \pmod{p}$ 有解. 至於若有解如何找解, 我們留待下一章學習更多方法後再處理.

由於我們只關注 $x^2 \equiv a \pmod{p}$ 何時有解, 何時無解, 我們介紹一個符號稱 (Legendre symbol) 來表示其有解或無解.

Definition 5.3.1. 給定奇質數 p 以及 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 若 $x^2 \equiv a \pmod{p}$ 有解, 我們稱 a 是一個 *quadratic residue* modulo p 並以 $\left(\frac{a}{p}\right) = 1$ 表示之. 反之, 若 $x^2 \equiv a \pmod{p}$ 無解, 我們稱 a 是一個 *quadratic nonresidue* modulo p 並以 $\left(\frac{a}{p}\right) = -1$ 表示之.

首先要注意的是 Legendre symbol 不要和分數搞混. 在本講義中的分數如三分之二的平方我們會用 $(\frac{2}{3})^2$ 或 $(2/3)^2$ 這兩種方法表示, 括號比較小. 而 Legendre symbol $\left(\frac{2}{3}\right)$ 的括號比較大. 另外依定義 Legendre symbol 的分母一定是一個奇質數且分子一定和分母互質 (有的書規定不同, 這裡為了不讓同學搞混我們嚴格如此規定). 例如在本講義中 $\left(\frac{5}{6}\right)$ 或 $\left(\frac{6}{3}\right)$ 這樣的符號是沒意義的 .

接下來我們來看 Legedre symbol 直接依定義所得之性質.

Lemma 5.3.2. 假設 p 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$.

(1) $\left(\frac{a^2}{p}\right) = 1$.

(2) 若 $b \in \mathbb{Z}$ 滿足 $b \equiv a \pmod{p}$, 則 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. (1) 要判斷 a^2 是否為 quadratic residue modulo p, 也就是要判斷 $x^2 \equiv a^2 \pmod{p}$ 是否有解. 然而很容易知道 $x = a$ 是 $x^2 \equiv a^2 \pmod{p}$ 的解, 故知 $\left(\frac{a^2}{p}\right) = 1$.

(2) 要判斷 b 是否為 quadratic residue modulo p, 也就是要判斷 $x^2 \equiv b \pmod{p}$ 是否有解. 然而依假設 $b \equiv a \pmod{p}$ 故要解 $x^2 \equiv b \pmod{p}$ 就等同於解 $x^2 \equiv a \pmod{p}$. 故知 $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$. □

其實 $x^2 \equiv a \pmod{p}$ 要不然有解要不然就無解. 所以若僅將 Legendre symbol 看成只是一個符號表示有解無解就太小看它了. 若要定符號, 我們也可以將有解定為 1 無解定為 0, 或其他相異的兩個數, 為何要將有解定為 1 無解定為 -1 呢? 說實話若僅想用兩個數字來表示有解或無解的情況, 那真的是怎麼定值都可以, 然而如此一來這樣的符號頂多僅讓我們方便表達有解或無解的情況, 沒有什麼太大的意義. Legendre symbol 之所以要將有解定為 1 無解定為 -1, 主要是我們可以將它們看成整數的 1 和 -1 來做乘法運算. 其原因就是下面這一個定理.

Theorem 5.3.3 (Euler's Criterion)**.** 假設 p 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$.

(1) 若 $x^2 \equiv a \pmod{p}$ 有解, 則 $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(2) 若 $x^2 \equiv a \pmod{p}$ 無解, 則 $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Proof. (1) 若 $x^2 \equiv a \pmod{p}$ 有解且 $x = c$ 為其一解, 即 $c^2 \equiv a \pmod{p}$. 此時

$$a^{\frac{p-1}{2}} \equiv (c^2)^{\frac{p-1}{2}} \equiv c^{p-1} \pmod{p}.$$

由於 a 和 p 互質, 所以 $x^2 \equiv a \pmod{p}$ 之解 c 亦與 p 互質. 因此利用 Fermat's Little Theorem (3.3.4) 知 $c^{p-1} \equiv 1 \pmod{p}$, 故得證 $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(2) 考慮 $S = \{1, 2, \ldots, p-1\}$ 這一個 reduced residue system modulo p. 對任意 $i \in S$, 由於 i 和 p 互質, 故由 Theorem 4.3.3 知 $ix \equiv a \pmod{p}$ 在 modulo p 之下有唯一解. 由於 a 和 p 互質, 故知其解必也與 p 互質. 換句話說, 給定 $i \in S$ 必存在唯一的 $j \in S$ 滿足 $ij \equiv a \pmod{p}$. 要注意此時 $j \neq i$, 否則會得到 $i^2 \equiv a \pmod{p}$, 也就是說 $x = i$ 是 $x^2 \equiv a \pmod{p}$ 的一個解, 此與 $x^2 \equiv a \pmod{p}$ 無解的假設相矛盾. 另一方面也要注意因為 $jx \equiv a \pmod{p}$ 在 modulo p 之下其解唯一且已知 $x = i$ 為其一解, 所以不可能找到另一個 $i' \in S$ 使得 $i'j \equiv a \pmod{p}$. 因此對於 S 中的元素, 我們可以將之兩兩配對, 也就是對任意 $i \in S$ 將 i 和滿足 $ij \equiv a \pmod{p}$ 唯一的 $j \in S$ 相配對. 如此一來我們共有 $(p-1)/2$ 對. 由於每一對相乘在 modulo p 之下和 a congruent, 故可得

$$(p-1)! = 1 \cdot 2 \cdots p-1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

不過 Wilson's Theorem (3.4.3) 告訴我們 $(p-1)! \equiv -1 \pmod{p}$, 故得證 $a^{(p-1)/2} \equiv -1 \pmod{p}$. □

如果大家不健忘的話, 當初在證明 Wilson's Theorem 我們是將 $S = \{1, \ldots, p-1\}$ 中之元素依 $ij \equiv 1 \pmod{p}$ 來配對. 所以 Wilson's Theorem 和 Euler's Criterion 的證明有異曲同工之妙.

當 $p \nmid a$ 時 $a^{(p-1)/2}$ 在 modulo p 之下之值不是 1 就是 -1. 這是因為若令 $b = a^{(p-1)/2}$, 則 $b^2 = a^{p-1} \equiv 1 \pmod{p}$, 也就是說 $x = b$ 為 $x^2 \equiv 1 \pmod{p}$ 之一根. 因此由 Lemma 3.4.2 知 $b \equiv \pm 1 \pmod{p}$. 因此, 給定 $a \in \mathbb{Z}$ 滿足 $p \nmid a$, 我們可以由 $a^{(p-1)/2}$ modulo p 為 1 或 -1 來判斷 $x^2 \equiv a \pmod{p}$ 是否有解. 例如, 若 $a^{(p-1)/2} \equiv 1 \pmod{p}$ 而又 $\left(\frac{a}{p}\right) = -1$, 則因 $x^2 \equiv a \pmod{p}$ 無解由 Theorem 5.3.3 知 $a^{(p-1)/2} \equiv -1 \pmod{p}$. 這會造成 $1 \equiv -1 \pmod{p}$ 即 $p|2$ 的矛盾. 因此我們知, 若 $a^{(p-1)/2} \equiv 1 \pmod{p}$, 則 $\left(\frac{a}{p}\right) = 1$. 同理, 若 $a^{(p-1)/2} \equiv -1 \pmod{p}$, 則 $\left(\frac{a}{p}\right) = -1$. 這就是 Legendre symbol 取 1 和 -1 為值的理由. 我們有以下之結論.

Corollary 5.3.4. 假設 p 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 則

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

所以今後我們要知道 $x^2 \equiv a \pmod{p}$ 有解或無解, 只要去算 $a^{(p-1)/2}$ 除以 p 的餘數是 1 或 $p-1$. 若餘數是 1 則有解, 若餘數是 $p-1$ 則無解. 不過這個方法在實際狀況下仍很費事, 因為要計算 $a^{(p-1)/2}$ 一般來說當 p 很大時仍很很麻煩. 不過這個 criterion 在證明一般抽象的定理時就很管用了. 我們有以下有關 Legendre symbol 的重要性質.

Proposition 5.3.5. 假設 p 是一個奇質數且 $a, b \in \mathbb{Z}$ 滿足 $p \nmid a$ 且 $p \nmid b$. 則

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. 由 Corollary 5.3.4 知

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

由於 $\left(\frac{ab}{p}\right)$ 和 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ 之值要不是 1 就是 -1, 所以他們在 modulo p 之下同餘表示必相等(否則又會得 $p|2$ 之矛盾). 故得 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Proposition 5.3.5 可以推出很令人吃驚的結果. 例如假設 $x^2 \equiv a \pmod{a}$ 和 $x^2 \equiv b \pmod{p}$ 皆有解且設 $x = c$ 和 $x = c'$ 分別為其一解. 那麼我們很容易推得 $x^2 \equiv ab \pmod{p}$ 必有解. 因為 $x = cc'$ 就是其中之一解. 不過若 $x^2 \equiv a \pmod{a}$ 和 $x^2 \equiv b \pmod{p}$ 其中有一個無解或是皆無解, 那們我們就很難利用解方程式的方法來處理 $x^2 \equiv ab \pmod{p}$ 是否有解了. 不過若利用 Proposition 5.3.5, 我們很快的便知若 $x^2 \equiv a \pmod{p}$ 有解但 $x^2 \equiv b \pmod{p}$ 無解 (即 $\left(\frac{a}{p}\right) = 1$, $\left(\frac{b}{p}\right) = -1$), 則 $x^2 \equiv ab \pmod{p}$ 便無解 (因為此時 $\left(\frac{ab}{p}\right) = 1 \times (-1) = -1$). 更令人訝異的是若 $x^2 \equiv a \pmod{p}$ 和 $x^2 \equiv b \pmod{p}$ 皆無解, 我們可以知 $x^2 \equiv ab \pmod{p}$ 必有解 (因為此時 $\left(\frac{ab}{p}\right) = (-1) \times (-1) = 1$). 這個結果是很難用有解無解這樣的角度來判斷的.

Proposition 5.3.5 另一個好處是對任意整數 a 我們可以分解成 $a = (-1)^m 2^{n_0} q_1^{n_1} \cdots q_r^{n_r}$, 其中 q_i 為奇質數 (且 $p \neq q_i$ 因 $p \nmid a$), $m \in \{0, 1\}$, $n_i \geq 0$. 因此可得

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^m \left(\frac{2}{p}\right)^{n_0} \left(\frac{q_1}{p}\right)^{n_1} \cdots \left(\frac{q_r}{p}\right)^{n_r}.$$

也就是說給定一奇質數 p, 我們只要知道 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ (q 為任意與 p 相異的奇質數) 之值, 那麼對任意與 p 互質的整數 a, 就可以算出 $\left(\frac{a}{p}\right)$ 之值了.

我們從原來要了解一般二次的 congruence equation 解的情形, 一路化簡到現在只要了解 $x^2 \equiv -1 \pmod{p}$, $x^2 \equiv 2 \pmod{p}$ 和 $x^2 \equiv q \pmod{p}$ (其中 q 是與 p 相異的奇質數), 這三種簡單形式的情形. 這就是解決數學問題常遇到的由繁化簡的過程, 值得大家細細體會其中的演化. 另一件有趣的是 Legendre symbol 和 Euler's Criterion 幫助我們將一個原本解二次 congruence equation 的問題換成另外一個和解方程式完全無關的方法來處理. 接下來

我們就是要利用這樣的方式來處理 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$, 而不再直接探討 $x^2 \equiv -1, 2, q \pmod{p}$ 有解或是無解.

5.4. Quadratic Reciprocity Law

我們僅剩下要討論 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ 之值. 在這節中 p 和 q 永遠表示兩相異奇質數, 我們就不另加說明了.

5.4.1. 求 $\left(\frac{-1}{p}\right)$**.** 我們首先探討 $\left(\frac{-1}{p}\right)$ 的取值情形. 或許大家會疑惑當 a 是一個負整數時, 一定可以找到一正整數 b 使得 $a \equiv b \pmod{p}$, 因此利用 Lemma 5.3.2(2) 我們有 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, 所以只要探討正整數的情況就好了為何還要考慮負的情況呢? 沒錯, 一般來說我們只要知道正整數的情形就足夠了, 不過考慮負整數也有其方便性. 例如我們要求 $\left(\frac{97}{101}\right)$. 因為 $97 \equiv -4 = (-1) \times 2^2 \pmod{101}$, 利用 Lemma 5.3.2 以及 Proposition 5.3.5 馬上可得 $\left(\frac{97}{101}\right) = \left(\frac{-1}{101}\right)$. 另一方面在 modulo p 之下是否有元素像複數中的 i 一樣滿足 $i^2 = -1$ 原本也就是一個有趣的問題. 所以了解 $\left(\frac{-1}{p}\right)$ 之值事實上是必要的.

Euler's Criterion 雖然在算一般的 $\left(\frac{a}{p}\right)$ 不是很好用, 不過在算 $\left(\frac{-1}{p}\right)$ 就很好用了.

Theorem 5.4.1. 假設 p 是奇質數, 則

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{當 } p \equiv 1 \pmod{4}; \\ -1, & \text{當 } p \equiv -1 \pmod{4}. \end{cases}$$

Proof. 利用 Corollary 5.3.4 我們知

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

若 $p \equiv 1 \pmod{4}$, 表示存在 $k \in \mathbb{N}$ 使得 $p = 4k+1$, 故得 $(-1)^{(p-1)/2} = (-1)^{2k} = 1$. 因此得證 $\left(\frac{-1}{p}\right) = 1$. 若 $p \equiv -1 \pmod{4}$, 表示存在 $k \in \mathbb{N}$ 使得 $p = 4k-1$, 故得 $(-1)^{(p-1)/2} = (-1)^{2k-1} = -1$. 因此得證 $\left(\frac{-1}{p}\right) = -1$. □

要注意由於 p 是奇質數, 因此 p 在 modulo 4 之下要不然和 1 同餘要不然就和 -1 同餘, 所以 Theorem 5.4.1 給了 $\left(\frac{-1}{p}\right)$ 完整的答案. 今後我們要知道 $x^2 \equiv -1 \pmod{p}$ 是否有解時, 只要看 p 在 modulo 4 之情形就可以知道答案. 例如剛才我們想知道 $x^2 \equiv 97 \pmod{101}$ 是否有解, 由 $\left(\frac{97}{101}\right) = \left(\frac{-1}{101}\right)$ 以及 $101 \equiv 1 \pmod{4}$ 馬上知道 $x^2 \equiv 97 \pmod{101}$ 是有解的.

5.4.2. 求 $\left(\frac{2}{p}\right)$. 接下來我們要探討 $\left(\frac{2}{p}\right)$ 的取值情形. 會將 2 和一般的奇質數分開討論的原因是因為 2 是唯一的偶質數, 其表現在很多狀況是和奇質數不同的, 事實上我們在前面已經看到許多在 2 的情況和一般奇質數有很大不同的情形例如 $x^2 \equiv a \pmod{2^n}$ 和 $x^2 \equiv a \pmod{p^n}$ 這兩種 congruence equation 其解的形態就完全不同.

我們還是要用 Euler's criterion 的精神來求 $\left(\frac{2}{p}\right)$ 而不是直接探討 $x^2 \equiv 2 \pmod{p}$ 何時有解. 然而 Euler's criterion 並不能直接套用來求 $\left(\frac{2}{p}\right)$, 主要原因是我們這裡的 p 是一般的奇質數而不是特定的奇質數, 所以根本無法估計 $2^{(p-1)/2}$ 在 modulo p 之下為 1 或 -1. 我們必須推導出另外的方法可以幫助我們求 $2^{(p-1)/2}$ 在 modulo p 之情形.

Lemma 5.4.2 (Gauss's Lemma)**.** 假設 p 是奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 考慮集合 $S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$. 若 S 中共有 n 個元素其除以 p 的餘數大於 $(p-1)/2$, 則

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Proof. 我們將 S 中的元素除以 p 的餘數分成 $r_1, \ldots, r_n$ 及 $s_1, \ldots, s_m$ 兩部份, 其中 r_i 是大於 $(p-1)/2$ 的部份, 而 s_j 表小於等於 $(p-1)/2$ 的部份. 由於 S 中的元素皆與 p 互質, 所以對所有的 $i \in \{1, \ldots, n\}$ 和 $j \in \{1, \ldots, m\}$ 依 r_i, s_j 的定義我們知存在 $1 \le n_i \le (p-1)/2$ 使得 $n_i a$ 除以 p 的餘數為 r_i 且 $(p+1)/2 \le r_i \le p-1$, 另一方面存在 $1 \le m_j \le (p-1)/2$ 使得 $m_j a$ 除以 p 的餘數為 s_j 且 $1 \le s_j \le (p-1)/2$. 要注意此時 $n+m = (p-1)/2$, 現考慮 $T = \{p-r_1, \ldots, p-r_n, s_1, \ldots, s_m\}$, 我們要證明 $T = \{1, 2, \ldots, (p-1)/2\}$.

要證明 $T = \{1, 2, \ldots, (p-1)/2\}$. 我們先證明 $T \subseteq \{1, 2, \ldots, (p-1)/2\}$. 然而對任意的 $i \in \{1, \ldots, n\}$ 我們有 $p - r_i \le p - (p+1)/2 = (p-1)/2$ 且 $p - r_i \ge p - (p-1) = 1$, 故知 $p - r_i \in \{1, 2, \ldots, (p-1)/2\}$. 另一方面對任意 $j \in \{1, \ldots, m\}$ 已知 $1 \le s_j \le (p-1)/2$ 故得證 $T \subseteq \{1, 2, \ldots, (p-1)/2\}$.

接下來我們證明 $p - r_i$, $i \in \{1, \ldots, n\}$ 和 s_j, $j \in \{1, \ldots, m\}$ 這 $n+m$ (即 $(p-1)/2$) 個元素皆相異, 便可得證 $T = \{1, 2, \ldots, (p-1)/2\}$. 所以我們要證明 (1): $1 \le i \ne i' \le n$ 時, $p - r_i \ne p - r_{i'}$; (2): $1 \le j \ne j' \le m$ 時, $s_j \ne s_{j'}$ 以及 (3): 對任意 $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$, $p - r_i \ne s_j$.

當 $1 \le i \ne i' \le n$ 時, 若 $p - r_i = p - r_{i'}$ 表示 $r_i = r_{i'}$, 依定義即 $n_i a$ 和 $n_{i'} a$ 除以 p 的餘數相同, 也就是說 $n_i a \equiv n_{i'} a \pmod{p}$. 然而已假設 a 和 p 互質故由 Corollary 3.2.4 知 $n_i \equiv n_{i'} \pmod{p}$. 但此與 $1 \le n_i \ne n_{i'} \le (p-1)/2$ 的假設矛盾, 故得證 $p - r_i \ne p - r_{i'}$, 即 (1) 是對的. 同理可證得 (2) 是對的. 至於 (3), 若 $p - r_i = s_j$, 表示 $r_i + s_j = p$, 可得 $n_i a + m_j a \equiv 0 \pmod{p}$. 故再由 Corollary 3.2.4 得 $n_i + m_j \equiv 0 \pmod{p}$. 然而 $1 \le n_i, m_j \le (p-1)/2$, 得 $2 \le n_i + m_j \le p-1$, 不可能滿足 $p | n_i + m_j$, 故得證 $p - r_i \ne s_j$.

既然 $T = \{1, 2, \ldots, (p-1)/2\}$, 我們得

$$\frac{p-1}{2}! = (p - r_1) \cdots (p - r_n) \cdot s_1 \cdots s_m \equiv (-1)^n r_1 \cdots r_n \cdot s_1 \cdots s_m \pmod{p}.$$

另一方面 $S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中元素除以 p 的餘數所成的集合為 $\{r_1, \ldots, r_n, s_1, \ldots, s_m\}$, 故得

$$r_1 \cdots r_n \cdot s_1 \cdots s_m \equiv a \cdot 2a \cdots \frac{p-1}{2}a = \frac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \pmod{p}.$$

和上式整理得

$$\frac{p-1}{2}! \equiv (-1)^n \frac{p-1}{2}! \cdot a^{\frac{p-1}{2}} \pmod{p}.$$

因為 $\frac{p-1}{2}!$ 和 p 互質, 故由 Corollary 3.2.4 知

$$1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod{p},$$

即

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

□

若 $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中共有 n 個元素除以 p 的餘數大於 $(p-1)/2$, 則由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

故由 $\left(\frac{a}{p}\right)$ 的取值為 ± 1, 得

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Gauss's Lemma 將繁複 $a^{(p-1)/2}$ 的計算換成計算 $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中有多少個除以 p 的餘數大於 $(p-1)/2$, 確實將問題簡化了. 我們可以利用它來計算 $\left(\frac{2}{p}\right)$.

Theorem 5.4.3. 假設 p 是奇質數, 則

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{當 } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{當 } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. 考慮 $S = \{2, 2 \times 2, \ldots, \frac{p-1}{2} \times 2\}$, 我們得 $S = \{2, 4, \ldots, p-1\}$. 也就是說 S 中的元數除以 p 所得餘數所成的集合恰為 S, 即小於 p 的正偶數所成之集合. 由於 p 是奇數, 我們將之分成 $p \equiv \pm 1, \pm 3 \pmod{8}$ 四種情形來討論. 看看 S 中有多少元素大於 $(p-1)/2$.

當 $p = 8k+1$ (即 $p \equiv 1 \pmod{8}$) 時, $(p-1)/2 = 4k$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1 = 8k$ 且大於 $4k$ 的偶數之個數. 知其共有 $(8k-4k)/2 = 2k$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k} = 1.$$

當 $p = 8k-1$ (即 $p \equiv -1 \pmod{8}$) 時, $(p-1)/2 = 4k-1$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1 = 8k-2$ 且大於 $4k-1$ 的偶數之個數. 知其共有 $(8k-2-(4k-2))/2 = 2k$.

故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k} = 1.$$

當 $p = 8k+3$ (即 $p \equiv 3 \pmod 8$) 時, $(p-1)/2 = 4k+1$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1 = 8k+2$ 且大於 $4k+1$ 的偶數之個數. 知其共有 $(8k+2-4k)/2 = 2k+1$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k+1} = -1.$$

當 $p = 8k-3$ (即 $p \equiv -3 \pmod 8$) 時, $(p-1)/2 = 4k-2$. 因此 S 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1 = 8k-4$ 且大於 $4k-2$ 的偶數之個數. 知其共有 $(8k-4-(4k-2))/2 = 2k-1$. 故由 Corollary 5.3.4 以及 Lemma 5.4.2 知

$$\left(\frac{2}{p}\right) = (-1)^{2k-1} = -1.$$

□

有了 Theorem 5.4.3, 給定一奇質數 p, 我們將很容易知道 $x^2 \equiv 2 \pmod p$ 是否有解. 例如因為 $101 \equiv 5 \equiv -3 \pmod 8$, 故知 $x^2 \equiv 2 \pmod{101}$ 無解. 而 $23 \equiv -1 \pmod 8$ 故知 $x^2 \equiv 2 \pmod{23}$ 有解. 事實上 $5^2 \equiv 2 \pmod{23}$, 故知 $x \equiv \pm 5 \pmod{23}$ 為 $x^2 \equiv 2 \pmod{23}$ 之解.

5.4.3. 求 $\left(\frac{q}{p}\right)$**.** 最後我們來探討 p, q 為相異奇質數的情形. 若給定了 p 和 q 我們當然就可以利用 Gauss's Lemma 求 $\left(\frac{q}{p}\right)$, 不過現在要討論的是一般的 p 和 q, 我們必須考慮別的方法.

在 Gauss's Lemma 中我們需要算出 $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中有多少元素其除以 p 的餘數大於 $(p-1)/2$. 若其個數為 n, 則 $\left(\frac{a}{p}\right) = (-1)^n$. 由於 $(-1)^n$ 的取值完全取決於 n 是奇數或偶數, 所以我們並不需精確地算出 n 為多少, 只需確認其為奇數或偶數即可. 以下我們將介紹一個判別 n 為奇或偶的方法, 不過由於我們要考慮的 $\left(\frac{q}{p}\right)$ 其中 q 為奇質數, 所以底下的方法中我們僅考慮 a 為奇數的情況.

為了方便我們先介紹一個符號. 給定一實數 r, 我們令 $[r]$ 表示小於等於 r 的整數中最大的整數. 例如若 π 表圓周率, 則 $[\pi] = 3$. 又例如 $[-5.2] = -6$. 要注意當 m, n 是正整數時 $[m/n]$ 即為 m 除以 n 的商.

Lemma 5.4.4. 給定一奇質數 p 及一奇數 a 滿足 $p \nmid a$. 若令 n 表示集合 $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ 中除以 p 餘數大於 $(p-1)/2$ 的元素個數, 則

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \pmod 2.$$

Proof. 假設 ka 除以 p 的餘數為 r, 則依定義我們有 $ka = p[ka/p] + r$. 故若依 Lemma 5.4.2 的證明我們將 $\{a, 2a, \cdots, \frac{p-1}{2}a\}$ 中的元素除以 p 的餘數分成 $r_1, \ldots, r_n$ 及 $s_1, \ldots, s_m$ 兩部份, 其中 r_i 是大於 $(p-1)/2$ 的部份, 而 s_j 表小於等於 $(p-1)/2$ 的部份, 則

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} p\left[\frac{ka}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j.$$

由於我們僅在乎奇或偶, 所以可考慮上式在 modulo 2 的情況, 故利用 a 和 p 皆為奇數 (即 $a \equiv p \equiv 1 \pmod 2$) 我們得

$$\sum_{k=1}^{(p-1)/2} k \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \pmod 2. \tag{5.1}$$

另一方面在 Lemma 5.4.2 的證明中我們證得

$$\{p - r_1, \ldots, p - r_n, s_1, \ldots, s_m\} = \{1, 2, \ldots, (p-1)/2\}.$$

故得

$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{n}(p - r_i) + \sum_{j=1}^{m} s_j = np - \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j.$$

再利用 $p \equiv 1 \pmod 2$ 得

$$\sum_{k=1}^{(p-1)/2} k \equiv n - \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \pmod 2. \tag{5.2}$$

合併式子 (5.1) 和 (5.2) 得證

$$n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] + 2\sum_{i=1}^{n} r_i \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \pmod 2.$$

□

再次強調在 Lemma 5.4.4 的證明中我們用到 a 是奇數 (即 $a \equiv 1 \pmod 2$) 的假設, 所以此結果僅適用於 a 為奇數的情況, 千萬別用此法來算 $\left(\frac{2}{p}\right)$.

利用 Corollary 5.3.4 以及 Lemma 5.4.2, Lemma 5.4.4, 我們知給定一奇質數 p, 要計算一個奇數 a 其 $\left(\frac{a}{p}\right)$ 之值, 我們只要計算 $\sum_{k=1}^{(p-1)/2}[ka/p]$ 之值即可. 若其值為 N, 則得 $\left(\frac{a}{p}\right) = (-1)^N$. 例如要求 $\left(\frac{5}{11}\right)$, 我們只要計算 $[5/11]+[10/11]+[15/11]+[20/11]+[25/11]$. 算出其值為 4, 故知 $\left(\frac{5}{11}\right) = (-1)^4 = 1$.

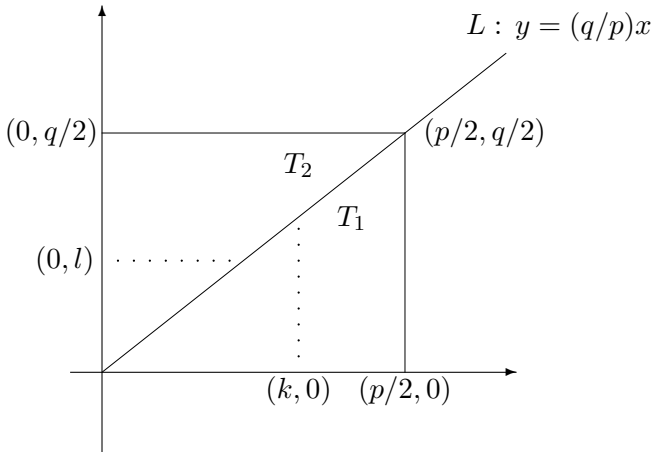
接著我們要利用 Lemma 5.4.4 來計算 $\left(\frac{q}{p}\right)$. 很容易理解算 $\left(\frac{q}{p}\right)$ 不止和 p 有關也和 q 有關, 所以我們要探討 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 的關係. 由於 p, q 皆為奇質數, 我們都可以利用 Lemma 5.4.4 來計算 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$. 因此我們要探討 $\sum_{k=1}^{(p-1)/2}[kq/p]$ 和 $\sum_{l=1}^{(q-1)/2}[lp/q]$ 之間的關係.

在探討此問題前, 我們再從另一個角度來看 $[r]$ 這個整數. 當 r 是正的實數時, $[r]$ 之值就是所有滿足 $0 \le n \le r$ 的正整數 n 的個數. 在座標 xy-平面上, 我們稱 x-軸及 y-軸座標皆為正整數的點為"正格子點". 依此看法, 當 k 是正整數時, $[kq/p]$ 之值就是直線 $x = k$ 在 $0 \le y \le kq/p$ 之間的正格子點個數. 而當 l 是正整數時, $[lp/q]$ 之值就是直線 $y = l$ 在 $0 \le x \le lp/q$ 之間的正格子點個數. 利用這種觀點, 我們有以下之結果.

Lemma 5.4.5. 假設 p 和 q 為相異奇質數. 則

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{l=1}^{(q-1)/2} \left[\frac{lp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}.$$

Proof. 在 xy-平面上, 考慮以 $(0,0)$, $(p/2,0)$, $(p/2,q/2)$ 以及 $(0,q/2)$ 四點為頂點的長方形區域 T, 並以直線 $L : y = (q/p)x$ 將此區域分成 T_1 和 T_2 兩部份. 其中 T_1 表直線 L 下方的部份, 而 T_2 表直線 L 上方的部份, 如下圖.



在 T 中的任意正格子點 (m,n), 依定義需滿足 $m, n \in \mathbb{N}$ 且 $0 \le m \le p/2$ 及 $0 \le n \le q/2$. 因此由 p, q 為奇數知在 T 中的正格子點個數為 $\dfrac{p-1}{2}\dfrac{q-1}{2}$.

另一方面在 T_1 中的正格子點 (k,s), 依定義需滿足 $k, s \in \mathbb{N}$ 且 $0 \le k \le p/2$ 及 $0 \le s \le kq/p$. 也就是說 $k \in \mathbb{N}$ 需滿足 $1 \le k \le (p-1)/2$, 且給定 k, 則 $0 \le s \le kq/p$. 換句話說要計算在 T_1 中的格子點, 等於在計算給定 $k \in \mathbb{N}$ 且 $1 \le k \le (p-1)/2$ 時會有多少 $s \in \mathbb{N}$ 滿足 $0 \le s \le kq/p$, 再將所有 k 所算得之結果加起來. 然而對任意的正整數 k 符合 $0 \le s \le kq/p$ 的正整數 s 的個數為 $[kq/p]$. 所以在 T_1 中的正格子點數為 $\sum_{k=1}^{(p-1)/2}[kq/p]$. 同理在 T_2 中的正格子點數為 $\sum_{l=1}^{(q-1)/2}[lp/q]$.

在 T_1 和 T_2 的交界, 即滿足 $y = (q/p)x$ 且 $0 \le x \le p/2$ 的線段上會不會有正格子點呢? 若 (m,n) 為其上之一正格子點, 則我們有 $pn = qm$ 且 $1 \le m \le (p-1)/2$. 然而由 $pn = qm$ 可得 $p|qm$, 再因 p, q 為相異質數故由 Proposition 1.2.7(1) 知 $p|m$, 此和 $1 \le m \le (p-1)/2$ 相矛盾. 故知在 T_1 和 T_2 交界的線段上無正格子點. 因此在 T_1 和 T_2 上的正格子點數之

和恰為在 T 上的正格子點數, 故得證

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\frac{q-1}{2}.$$

□

當 p,q 為相異奇質數, 若 $M=\sum_{k=1}^{(p-1)/2}[kq/p]$ 且 $N=\sum_{l=1}^{(q-1)/2}[lp/q]$ 由 Lemma 5.4.4 知 $\left(\frac{q}{p}\right)=(-1)^M$ 且 $\left(\frac{p}{q}\right)=(-1)^N$. 而 Lemma 5.4.5 告訴我們 $M+N=(p-1)(q-1)/4$, 故得

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{M+N}=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

因此我們有以下之結果.

Theorem 5.4.6 (Quadratic Reciprocity Law)**.** 假設 p 和 q 為相異奇質數. 則

$$\left(\frac{q}{p}\right)=\begin{cases}-\left(\frac{p}{q}\right), & \text{若 } p\equiv q\equiv -1 \pmod 4;\\ \left(\frac{p}{q}\right), & \text{其他情形.}\end{cases}$$

Proof. 由於 p,q 皆為奇數, 我們依 $p\equiv\pm1 \pmod 4$ 以及 $q\equiv\pm1 \pmod 4$ 四種情形來討論.

假設 $p=4k-1$ 且 $q=4k'-1$ 其中 $k,k'\in\mathbb{N}$ (即 $p\equiv q\equiv -1 \pmod 4$). 則 $(p-1)/2=2k-1$ 且 $(q-1)/2=2k'-1$, 故得

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(2k-1)(2k'-1)}=-1.$$

也就是說 $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$.

剩下的情況為 p 和 q 中至少有一個在 modulo 4 之後餘 1. 不失一般性就假設 $p\equiv 1 \pmod 4$. 此時 $p=4k+1$, 其中 $k\in\mathbb{N}$, 故得 $(p-1)/2=2k$. 而 $(q-1)/2$ 必為整數故知

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(2k)\frac{q-1}{2}}=1^{\frac{q-1}{2}}=1.$$

也就是說 $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$. □

要注意 Theorem 5.4.6 要在 p,q 為相異奇質數時才適用, 否則若 q 不是奇質數, $\left(\frac{p}{q}\right)$ 這個符號是沒有定義的. 雖然 Theorem 5.4.6 並沒有明確告訴我們 $\left(\frac{q}{p}\right)$ 之值為何, 但是可利用 $\left(\frac{p}{q}\right)$ 之值來求得 $\left(\frac{q}{p}\right)$. 一般來說將 $\left(\frac{q}{p}\right)$ 的問題反轉成 $\left(\frac{p}{q}\right)$ 的問題就像輾轉相除法一樣, 可以快速的將問題簡化. 這是因為一般來說利用 Lemma 5.3.2(2), 要求 $\left(\frac{q}{p}\right)$ 時, 可假設 $q<p$, 所以一反轉成 $\left(\frac{p}{q}\right)$ 時我們已將一個 modulo 比較大的 p 的問題簡化成一個 modulo 比較小的 q 的問題. 例如求 $\left(\frac{7}{101}\right)$, 由於 $101\equiv 1 \pmod 4$, 故得

$\left(\frac{7}{101}\right) = \left(\frac{101}{7}\right)$. 所以馬上將 modulo 101 的問題轉成 modulo 7 的問題, 自然變得簡單. 事實上 $\left(\frac{101}{7}\right) = \left(\frac{3}{7}\right)$, 可馬上驗證知 $\left(\frac{3}{7}\right) = -1$ (或再用一次 Theorem 5.4.6 得 $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$). 所以得知 $\left(\frac{7}{101}\right) = -1$. 總而言之, 對於一般的相異奇質數 p, q, 我們沒有辦法由 p 和 q 馬上得知 $\left(\frac{q}{p}\right)$ 之值. 但是利用 Theorem 5.4.6, 我們可以很快速的將問題化簡而求出其值. 最後我們來看一個例子整合這一節中學到的方法.

Example 5.4.7. 考慮二次 congruence equation $x^2 \equiv 539 \pmod{631}$ 是否有解. 要注意若要用 Legendre symbol 處理, 首先要檢查 631 是否為質數. 我們可以利用篩法 (Proposition 1.4.6) 檢查小於 $\sqrt{631}$ 的質數是否可整除 631. 由於小餘 25 的質數皆不能整除 631, 所以 Proposition 1.4.6 告訴我們 631 是質數. 因此我們就是要計算 $\left(\frac{539}{631}\right)$ 之值. 由於 539 和 631 頗近, 我們利用 $539 \equiv -92 \pmod{631}$ 以及 Lemma 5.3.2(2) 知 $\left(\frac{539}{631}\right) = \left(\frac{-92}{631}\right)$ 接著將 92 作質因數分解得 $92 = 2^2 \times 23$. 故利用 Proposition 5.3.5 知

$$\left(\frac{539}{631}\right) = \left(\frac{-92}{631}\right) = \left(\frac{-1}{631}\right)\left(\frac{4}{631}\right)\left(\frac{23}{631}\right).$$

由於 $631 \equiv 3 \equiv -1 \pmod{4}$, 故由 Theorem 5.4.1 知 $\left(\frac{-1}{631}\right) = -1$. 而 $4 = 2^2$, 故由 Lemma 5.3.2(1) 知 $\left(\frac{4}{631}\right) = 1$, 因此得 $\left(\frac{539}{631}\right) = -\left(\frac{23}{631}\right)$. 由於 $631 \equiv 23 \equiv 3 \pmod{4}$, 故由 Theorem 5.4.6 知 $\left(\frac{23}{631}\right) = -\left(\frac{631}{23}\right)$. 又由 $631 \equiv 10 \pmod{23}$ 因此知

$$\left(\frac{539}{631}\right) = -\left(\frac{23}{631}\right) = \left(\frac{631}{23}\right) = \left(\frac{10}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{5}{23}\right).$$

因為 $23 \equiv 7 \equiv -1 \pmod{8}$, 故由 Theorem 5.4.3 知 $\left(\frac{2}{23}\right) = 1$. 又因 $5 \equiv 1 \pmod{4}$, 故由 Theorem 5.4.6 知 $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right)$. 因此得 $\left(\frac{539}{631}\right) = \left(\frac{2}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right)$. 再由 $23 \equiv 3 \pmod{5}$ 以及 $5 \equiv 1 \pmod{4}$ 知 $\left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$. 所以知 $\left(\frac{539}{631}\right) = \left(\frac{2}{3}\right) = -1$. 也就是說 $x^2 \equiv 539 \pmod{631}$ 無解.

當然了當初若看出 $539 = 7^2 \times 11$, 則馬上得 $\left(\frac{539}{631}\right) = \left(\frac{7^2}{631}\right)\left(\frac{11}{631}\right) = \left(\frac{11}{631}\right)$. 再因 $631 \equiv 11 \equiv 3 \pmod{4}$ 以及 $631 \equiv 4 \pmod{11}$ 知

$$\left(\frac{539}{631}\right) = \left(\frac{11}{631}\right) = -\left(\frac{631}{11}\right) = -\left(\frac{4}{11}\right) = -1.$$

所以不管用哪種看法只要善用 Legendre symbol 且正確地使用 quadratic reciprocity law (記得只有奇質數才能置於 Legendre symbol 的下方), 便能快速且正確的求出 Legendre symbol 之值.

Chapter 6

Primitive Roots

給定 $m \in \mathbb{N}$, 若存在 $a \in \mathbb{Z}$ 使得 $\{a, a^2, \ldots, a^{\phi(m)}\}$ 成為一個 reduced residue system modulo m, 則稱 a 是 modulo m 之下的 primitive root. Primitive roots 的概念可以幫助我們解高次的 congruence equation. 在本章中我們將探討 Primitive Root Theorem, 即了解怎樣的正整數 m 會使得在 modulo m 之下有 primitive root. 並依此來解高次的 congruence equation.

6.1. Order 與 Primitive Roots

給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$, 我們已知如何判別 $x^2 \equiv a \pmod{m}$ 有解或無解, 而 primitive root 的概念可以幫助我們找到解.

考慮 $x^2 \equiv 5 \pmod{11}$. 利用 quadratic reciprocity law 我們知 $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$, 故知 $x^2 \equiv 5 \pmod{11}$ 有解. 然而解為何呢? 我們可以利用 2 在 modulo 11 之下特有的性質幫助我們找解. 下表為 2^n 在 modulo 11 的情形.

n	1	2	3	4	5	6	7	8	9	10
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1

我們發現第二行 (即 a^n 那一行) 中這 10 ($= \phi(11)$) 個數在 modulo 11 之下皆相異, 而且因 2 和 11 互質所以自然 2^n 和 11 互質, 因此由 reduced residue system 的定義知 $\{2, 2^2, \ldots, 2^{10}\}$ 是一個 reduced residue system modulo 11. 這代表的意義是每個和 11 互質的數 a, 都可以找到 $1 \le n \le 10$ 使得 $a \equiv 2^n \pmod{11}$. 另一方面我們僅將 n 列到 10 的原因是因為 $2^{10} \equiv 1 \pmod{11}$, 如果 $m = 10k + i$ 其中 $0 \le i \le 9$, 則 $2^m \equiv 2^i \pmod{11}$. 也就是每 10 次方一循環, 所以列出 10 次就夠了. 又由於已知當 $1 \le i \ne j \le 10$ 時, $2^i \not\equiv 2^j \pmod{11}$, 我們知 $2^i \equiv 2^j \pmod{11}$ 若且唯若 $i \equiv j \pmod{10}$. 結合這些結果可以幫助我們解 $x^2 \equiv 5 \pmod{11}$. 原因如下: 假設 $x = c$ 是一解, 由於 5 和 11 互質, 故知 c 和 11 互質. 因此知存在 $t \in \mathbb{N}$ 使得 $c \equiv 2^t \pmod{11}$. 然而 $5 \equiv 2^4 \pmod{11}$, 故由 $2^{2t} \equiv c^2 \equiv 5 \equiv 2^4 \pmod{11}$ 得 $2t \equiv 4 \pmod{10}$. 我們很巧妙的將解二次的 $x^2 \equiv 5 \pmod{11}$ 轉化成解一次的 $2t \equiv 4 \pmod{10}$ (注意 modulo 不同的數). 故利用 Proposition 4.2.1 解得 $t \equiv 2 \pmod{5}$, 也就是

說 $t = 2, 7, \ldots$ 為 $2t \equiv 4 \pmod{10}$ 之解. 將之代回 $c = 2^t$, 得 $c \equiv 4, 7 \pmod{11}$. 故知 $x \equiv \pm 4 \pmod{11}$ 為 $x^2 \equiv 5 \pmod{11}$ 之解.

可依此法解二次 congruence equation 歸功於在 modulo 11 之下 $\{2, 2^2, \ldots, 2^{11}\}$ 是 reduced residue system. 要注意並不是 2 永遠有此特性. 例如 $2^3 \equiv 1 \pmod{7}$, 所以 $\{2, 2^2, \ldots, 2^6\}$ 在 modulo 7 之下並不是 reduced residue system. 我們將有此特性的元素給個特定的名子.

Definition 6.1.1. 給定 $m \in \mathbb{N}$, 若 $a \in \mathbb{Z}$ 且與 m 互質滿足 $\{a, a^2, \ldots, a^{\phi(m)}\}$ 是一個 reduced residue system modulo m, 則稱 a 為 modulo m 之下的一個 *primitive root*.

要注意並不是對所有的 m 皆有 primitive root. 例如在 modulo 15 之下, 所有和 15 互質的數 a 皆有 $a^4 \equiv 1 \pmod{15}$, 所以又因 $a^{\phi(15)} = a^8 \equiv 1 \pmod{15}$ 知 $\{a, a^2, a^3, a^4, \ldots, a^8\}$ 不可能形成 reduced residue system modulo 15. 也就是說在 modulo 15 之下並無 primitive root. 我們最主要的目的就是要探討哪些 $m \in \mathbb{N}$ 在 modulo m 之下會有 primitive root.

首先我們必須了解怎樣的 a 在 modulo m 之下會是 primitive root. 由於 $S = \{a, a^2, \ldots, a^{\phi(m)}\}$ 是 reduced residue system modulo m, 所以若 $1 \le i \ne j \le \phi(m)$, 則 $a^i \not\equiv a^j \pmod{m}$. 否則 S 在 modulo m 之下會有少於 $\phi(m)$ 個同餘類, 無法形成 reduced residue system modulo m. 然而 a 和 m 互質, Euler's Theorem (3.3.2) 告訴我們 $a^{\phi(m)} \equiv 1 \pmod{m}$, 所以 a 在 modulo m 之下是 primitive root 的先決條件是若 $1 \le i \le \phi(m) - 1$, 則 $a^i \not\equiv 1 \pmod{m}$ (否則會造成 $1 \le i < \phi(m)$ 且 $a^i \equiv a^{\phi(m)} \pmod{m}$ 的矛盾). 也就是說滿足 $a^n \equiv 1 \pmod{m}$ 的最小正整數 n 為 $n = \phi(m)$. 因此給定 $a \in \mathbb{Z}$ 且 $\gcd(a, m) = 1$, 最小的正整數 n 滿足 $a^n \equiv 1 \pmod{m}$ 為何, 是判斷 a 在 modulo m 之下是否為 primitive root 的重要依據. 我們自然有以下之定義.

Definition 6.1.2. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 若 $n \in \mathbb{N}$ 是最小的正整數滿足 $a^n \equiv 1 \pmod{m}$, 則稱 n 為 a 在 modulo m 之下的 *order*, 並以 $\mathrm{ord}_m(a) = n$ 表之.

要注意由於 $\gcd(a, m) = 1$, Euler's Theorem 告訴我們 $a^{\phi(m)} \equiv 1 \pmod{m}$, 所以 $\mathrm{ord}_m(a)$ 必存在且依定義知 $\mathrm{ord}_m(a) \le \phi(m)$. 首先我們來看依定義馬上可得之性質.

Lemma 6.1.3. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$.

(1) 若 $a \equiv b \pmod{m}$ 則 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

(2) $\mathrm{ord}_m(a) = 1$ 若且唯若 $a \equiv 1 \pmod{m}$.

Proof. (1) 若 $a \equiv b \pmod{m}$, 知對任意 $i \in \mathbb{N}$ 皆有 $a^i \equiv b^i \pmod{m}$, 故若 n 是最小的正整數使得 $a^n \equiv 1 \pmod{m}$, 則 n 也會是最小的正整數使得 $b^n \equiv 1 \pmod{m}$. 因此知 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

(2) 若 $\mathrm{ord}_m(a) = 1$, 表示 $a^1 \equiv 1 \pmod{m}$, 故得 $a \equiv 1 \pmod{m}$. 反之, 若 $a \equiv 1 \pmod{m}$, 當然 $n = 1$ 是最小的正整數使得 $a^n \equiv 1 \pmod{m}$, 故知 $\mathrm{ord}_m(a) = 1$. □

其實 order 的定義和最大公因數的定義類似, 我們要說 $\mathrm{ord}_m(a) = n$ 等於要說兩件事:

(1) $a^n \equiv 1 \pmod{m}$.

(2) 若 $1 \le i \le n-1$, 則 $a^i \not\equiv 1 \pmod{m}$.

要記住這兩件事缺一不可才能保證 $\mathrm{ord}_m(a) = n$. 接下來我們就來看依此兩點可推得 $\mathrm{ord}_m(a)$ 的性質.

Proposition 6.1.4. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 假設 $\mathrm{ord}_m(a) = n$. 則 $a^k \equiv 1 \pmod{m}$ 若且唯若 $n|k$.

Proof. 假設 $a^k \equiv 1 \pmod{m}$. 利用 Division Algorithm (Theorem 1.2.1) 知存在 $h, r \in \mathbb{Z}$ 滿足 $k = nh + r$, 其中 $0 \le r \le n-1$. 由 $a^n \equiv 1 \pmod{m}$ 知 $a^k = a^{nh+r} = (a^n)^h a^r \equiv a^r \pmod{m}$. 現假設 $r \neq 0$ (即 $1 \le r \le n-1$), 則由 $a^k \equiv 1 \pmod{m}$ 之假設知 $a^r \equiv 1 \pmod{m}$. 此和 n 是最小的正整數滿足 $a^n \equiv 1 \pmod{m}$ 相違背, 故知 $r = 0$, 即 $n|k$.

反之若 $n|k$, 即存在 $h \in \mathbb{Z}$ 滿足 $k = nh$, 故得 $a^k = a^{nh} = (a^n)^h \equiv 1 \pmod{m}$. □

若 a 和 m 互質, Euler's Theorem 告訴我們 $a^{\phi(m)} \equiv 1 \pmod{1}$, 故由 Proposition 6.1.4 知 $\mathrm{ord}_m(a)|\phi(m)$, 這比我們前面依定義知 $\mathrm{ord}_m(a) \le \phi(m)$ 好多了. 同樣的, 利用 Proposition 6.1.4, 我們可以有更好的方式來判定 $\mathrm{ord}_m(a)$ 之值.

Corollary 6.1.5. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 則 $\mathrm{ord}_m(a) = n$ 若且唯若 n 滿足以下兩條件:

(1) $a^n \equiv 1 \pmod{m}$.

(2) 若 $a^k \equiv 1 \pmod{m}$, 則 $n|k$.

Proof. 若 $\mathrm{ord}_m(a) = n$, 則自然有 $a^n \equiv 1 \pmod{m}$, 再利用 Proposition 6.1.4 知, 若 $a^k \equiv 1 \pmod{m}$, 則 $n|k$.

反之若 n 滿足 (1), (2) 兩項, 我們要證明 $\mathrm{ord}_m(a) = n$. 由於 (1) 已知 $a^n \equiv 1 \pmod{m}$, 故僅剩要證明若 $1 \le i \le n-1$, 則 $a^i \not\equiv 1 \pmod{m}$. 我們用反證法, 假設 $a^i \equiv 1 \pmod{m}$, 則由 (2) 知 $n|i$. 此和 $1 \le i \le n-1$ 相矛盾, 故知 $a^i \not\equiv 1 \pmod{m}$. 也就是說 $\mathrm{ord}_m(a) = n$. □

Corollary 6.1.5 的 (2) 將 $\mathrm{ord}_m(a) = n$ 原本表最小的正整數滿足 $a^n \equiv 1 \pmod{m}$ 的性質轉換成看似更強的性質 (就如同當初原本最大公因數是最大的公因數可轉換成為所有的公因數的倍數這樣的性質) 在以後有關 order 的理論推導中有很大的幫助.

計算 order 的另一個重要的原因是我們可以知道 a^i 在 modulo m 之下的週期.

Proposition 6.1.6. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 假設 $\mathrm{ord}_m(a) = n$ 且 $i, j \in \mathbb{N}$. 則 $a^i \equiv a^j \pmod{m}$ 若且唯若 $i \equiv j \pmod{n}$.

Proof. 假設 $a^i \equiv a^j \pmod{m}$, 不失一般性我們也假設 $i \ge j$, 此時 $a^i - a^j = a^j(a^{i-j} - 1)$. 利用 $m|a^i - a^j$ 以及 m 和 a^j 互質 (因 m 和 a 互質), Proposition 1.2.7 告訴我們 $m|a^{i-j} - 1$, 即 $a^{i-j} \equiv 1 \pmod{m}$. 故利用 $\mathrm{ord}_m(a) = n$ 以及 Proposition 6.1.4 知 $m|i-j$, 亦即 $i \equiv j \pmod{n}$.

反之, 若 $i \equiv j \pmod{n}$, 不失一般性我們假設 $i \geq j$, 則有 $n|i-j$. 故再利用 Proposition 6.1.4 知 $a^{i-j} \equiv 1 \pmod{m}$. 兩邊乘上 a^j 因此有 $a^i = a^j a^{i-j} \equiv a^j \pmod{m}$. □

若 $\mathrm{ord}_m(a) = n$, Proposition 6.1.6 不只告訴我們 $a, a^2, \ldots, a^i, \ldots$ 在 modulo m 之下的週期為 n (即每隔 n 個 i, a^i 會形成一循環) 而且告訴我們, $a, a^2, \ldots, a^n$ 在 modulo m 之下皆相異. 否則若存在 $1 \leq j < i \leq n$ 使得 $a^i \equiv a^j \pmod{m}$, 可得 $n|i-j$ 而與 $0 < i-j < n-1$ 相矛盾. 依此我們可以確定可以用 $\mathrm{ord}_m(a)$ 之值來判定 a 在 modulo m 之下是否為 primitive root.

Corollary 6.1.7. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 則 $\mathrm{ord}_m(a) = \phi(m)$ 若且唯若 a 在 *modulo* m 之下是一個 *primitive root.*

Proof. 假設 a 是 modulo m 之下的一個 primitive root. 由於 $a, a^2, \ldots, a^{\phi(m)}$ 在 modulo m 之下皆不同餘, 故知若 $1 \leq i \leq \phi(m)$, 則 $a^i \not\equiv a^{\phi(m)} \pmod{m}$. 又由於 Euler's Theorem 知 $a^{\phi(m)} \equiv 1 \pmod{m}$, 故知 $\mathrm{ord}_m(a) = \phi(m)$.

反之, 假設 $\mathrm{ord}_m(a) = \phi(m)$, 由 Proposition 6.1.6 知若 $a^i \equiv a^j \pmod{m}$, 則 $\phi(m)|i-j$. 因此 $a, a^2, \ldots, a^{\phi(m)}$ 在 modulo m 之下皆不同餘. 又由於 a 和 m 互質, 知 a^i 皆與 m 互質, 故 $\{a, a^2, \ldots, a^{\phi(m)}\}$ 是一個 reduced residue system modulo m, 也就是說 a 在 modulo m 之下是一個 primitive root. □

若已知 a 在 modulo m 的 order, 則對任意 $i \in \mathbb{N}$, 利用 Corollary 6.1.5 我們都可算出 a^i 在 modulo m 之下的 order.

Proposition 6.1.8. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a, m) = 1$. 若 $\mathrm{ord}_m(a) = n$, 則對於任意的正整數 i,

$$\mathrm{ord}_m(a^i) = \frac{n}{\gcd(i, n)}.$$

Proof. 為了方便, 我們令 $d = \gcd(i, n)$. 欲證明 $\mathrm{ord}_m(a^i) = n/d$, 首先得證明 $(a^i)^{n/d} \equiv 1 \pmod{m}$. 事實上因為 d 是 i 的因數, i/d 是個整數. 再加上由假設 $\mathrm{ord}_m(a) = n$, 故 $a^n \equiv 1 \pmod{m}$. 所以可得

$$(a^i)^{n/d} = (a^n)^{i/d} \equiv 1 \pmod{m}.$$

接下來我們須證明, 若 $(a^i)^k \equiv 1 \pmod{m}$ 則 $(n/d) \,|\, k$ (參見 Corollary 6.1.5(2)). 若 $(a^i)^k \equiv 1 \pmod{m}$, 即 $a^{ki} \equiv 1 \pmod{m}$. 故由 Proposition 6.1.4, 我們可得 $n \,|\, ki$. 但因 d 是 n 和 i 的最大公因數. 我們有 n/d 和 i/d 皆為整數且互質. 故由 $n \,|\, ki$ 可得 $(n/d) \,|\, k(i/d)$. 再由 n/d 和 i/d 互質, 得 $(n/d) \,|\, k$. □

由 Proposition 6.1.8, 我們知 $\mathrm{ord}_m(a^i)$ 整除 $\mathrm{ord}_m(a)$ 而且 $\mathrm{ord}_m(a^i) = \mathrm{ord}_m(a)$ 若且唯若 $\gcd(i, \mathrm{ord}_m(a)) = 1$. 因此在 modulo m 之下 primitive root 若存在, 則我們可推知在 modulo m 之下會有多少個 primitive roots.

Corollary 6.1.9. 給定 $m \in \mathbb{N}$ 以及 $a \in \mathbb{Z}$ 滿足 $\gcd(a,m) = 1$. 若 $\mathrm{ord}_m(a) = n$, 則 $\{a, a^2, \ldots, a^n\}$ 中共有 $\phi(n)$ 個元素其在 *modulo* m 之下的 *order* 為 n. 特別地, 若在 *modulo* m 之下 *primitive root* 是存在的, 則在 *modulo* m 之下共有 $\phi(\phi(m))$ 個 *primitive roots.*

Proof. 已知 $\mathrm{ord}_m(a) = n$, 由 Proposition 6.1.8 知 $\mathrm{ord}_m(a^i) = n$ 若且唯若 $\gcd(n,i) = 1$. 又由於 $a, a^2, \ldots, a^n$ 在 modulo m 之下皆相異, 故 $\{a, a^2, \ldots, a^n\}$ 中在 modulo m 之下 order 為 n 的元素個數等於和 n 互質且小於 n 的正整數的個數, 依定義知此數為 $\phi(n)$.

現假設在 modulo m 之下有 primitive root 且 a 為一個 primitive root. 故知 $\mathrm{ord}_m(a) = \phi(m)$ 且所有和 m 互質的整數在 modulo m 之下皆和 $S = \{a, a^2, \ldots, a^{\phi(m)}\}$ 中某個元素同餘. 所以在 modulo m 之下所有的 primitive root 皆可在 S 中找到. 然而由前知 S 中共有 $\phi(\phi(m))$ 個元素其在 modulo m 之下的 order 為 $\phi(m)$, 且 Corollary 6.1.7 告訴我們在 modulo m 之下只有這些元素為 primitive root. 故知在 modulo m 之下共有 $\phi(\phi(m))$ 個 primitive roots. □

6.2. 沒有 Primitive Root 的情況

我們將探討有哪些 m 在 modulo m 之下沒有 primitive root.

我們仍然從唯一的偶質數 2 出發. 在 modulo 2 之下 $\phi(2) = 1$, 而任何的奇數在 modulo 2 之下皆餘 1, 故所有的奇數皆為 primitive root. 在 modulo 4 時, $\{1,3\}$ 是一個 reduced residue system modulo 4, 而 $3^1 \not\equiv 1 \pmod 4$ 且 $3^2 \equiv 1 \pmod 4$ 故得 $\mathrm{ord}_4(3) = 2 = \phi(4)$, 故知 3 在 modulo 4 之下是 primitive root. 事實上若 $a \in \mathbb{Z}$ 滿足 $a \equiv 3 \pmod 4$ 則 a 在 modulo 4 之下為 primitive root.

接著我們來看 8 情形, 由於 $\{1,3,5,7\}$ 是一個 reduced residue system modulo 8, 我們來看看它們在 modulo 8 之下之 order 為何. 很明顯的 $\mathrm{ord}_8(1) = 1$ 且因為 $7 \equiv -1 \pmod 8$, 故知 $\mathrm{ord}_8(7) = 2$. 另外 $3^1 \equiv 3 \pmod 8$ 且 $3^2 \equiv 1 \pmod 8$, 故知 $\mathrm{ord}_8(3) = 2$. 同理得 $\mathrm{ord}_8(5) = 2$. 由於所有和 8 互質的數在 modulo 8 之下必和 $1,3,5,7$ 中某一數同餘, 因此由 Lemma 6.1.3(1) 知沒有一個和 8 互質的數其在 modulo 8 之下的 order 為 $\phi(8) = 4$. 故知在 modulo 8 之下沒有 primitive root.

或許大家看到 modulo 8 之下沒有 primitive root 很自然會認為那麼在 modulo 16 之下也沒有 primitive root. 事實上這件事並不能直接用 order 的定義得到. 也就是說若已知 $\mathrm{ord}_8(a) = n$ 並不能直接用 order 的性質推出 $\mathrm{ord}_{16}(a)$ 之值. 頂多我們知道若 $\mathrm{ord}_{16}(a) = n'$, 則由 $a^{n'} \equiv 1 \pmod{16}$ 可知 $a^{n'} \equiv 1 \pmod 8$, 故利用 Proposition 6.1.4 得 $n | n'$. 但我們並不能由此以及 $n < \phi(8)$ 推出 $n' < \phi(16)$. 所以要推出在 modulo 16 或甚至 modulo 2^n, $n > 3$ 時沒有 primitive root, 是需要多下功夫的. 在前面我們已算出對任意奇數 a, 皆滿足 $a^2 \equiv 1 \pmod{2^3}$. 我們要用歸納法推出以下結果.

Lemma 6.2.1. 假設 a 為一奇數, 則對任意 $n \in \mathbb{N}$ 皆有 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

Proof. 我們已知當 $n=1$ 時這是對的. 假設當 $n=k$ 時皆有 $a^{2^k}\equiv 1 \pmod{2^{k+2}}$, 我們要證明當 $n=k+1$ 時亦成立. 依假設我們知存在 $b\in\mathbb{Z}$ 使得 $a^{2^k}=1+2^{k+2}b$. 故

$$a^{2^{k+1}}=(a^{2^k})^2=(1+2^{k+2}b)^2=1+2(2^{k+2}b)+(2^{k+2}b)^2.$$

由於 $2(k+2)=k+(k+4)>k+3$, 我們得 $a^{2^{k+1}}\equiv 1 \pmod{2^{k+3}}$. 也就是說當 $n=k+1$ 時 $a^{2^n}\equiv 1 \pmod{2^{n+2}}$ 亦成立, 故由數學歸納法得證本定理. □

依 order 的定義我們馬上由 Lemma 6.2.1 知當 a 為奇數且 $n\in\mathbb{N}$ 時,

$$\mathrm{ord}_{2^{n+2}}(a)\le 2^n<2^{n+1}=\phi(2^{n+2}),$$

故得證以下重要的結果.

Proposition 6.2.2. 當 $n\in\mathbb{N}$ 且 $n\ge 3$ 時, 在 *modulo* 2^n 之下沒有 *primitive root.*

接下來我們要探討另一種沒有 primitive root 的情況, 首先我們來看另一個有關 order 簡單的性質.

Lemma 6.2.3. 給定互質的兩正整數 m,n 以及 $a\in\mathbb{Z}$ 滿足 $\gcd(a,mn)=1$. 則

$$\mathrm{ord}_{mn}(a)\le\frac{\phi(mn)}{\gcd(\phi(m),\phi(n))}.$$

Proof. 令 $d=\gcd(\phi(m),\phi(n))$. 由於 $\gcd(a,mn)=1$, 我們知 $\gcd(a,m)=\gcd(a,n)=1$. 因此由 Euler's Theorem 我們有 $a^{\phi(m)}\equiv 1 \pmod m$ 以及 $a^{\phi(n)}\equiv 1 \pmod n$. 因此由 $\phi(mn)=\phi(m)\phi(n)$ (因 $\gcd(m,n)=1$) 以及 $\phi(n)/d\in\mathbb{N}$ 可得

$$a^{\frac{\phi(mn)}{d}}=(a^{\phi(m)})^{\frac{\phi(n)}{d}}\equiv 1 \pmod m.$$

同理可得 $a^{\phi(mn)/d}\equiv 1 \pmod n$. 也就是說 $m|a^{\phi(mn)/d}-1$ 且 $n|a^{\phi(mn)/d}-1$, 故再因 $\gcd(m,n)=1$ 利用 Proposition 1.2.7(2) 可得 $mn|a^{\phi(mn)/d}-1$, 即 $a^{\phi(mn)/d}\equiv 1 \pmod{mn}$. 故依 order 之定義得 $\mathrm{ord}_{mn}(a)\le\phi(mn)/d$. □

特別地, 假設 m 是一個大於 2 的整數. 若 m 沒有奇的質因數, 即 $m=2^k$ 其中 $k\ge 2$. 此時 $\phi(m)=\phi(2^k)=2^{k-1}$, 故得 $2|\phi(m)$. 若 m 有奇的質因數, 即存在一奇質數 p 使得 $m=p^lm'$, 其中 $l\in\mathbb{N}$ 且 $p\nmid m'$. 此時 $\phi(m)=\phi(p^l)\phi(m')=(p-1)p^{l-1}\phi(m')$, 同樣可得 $2|\phi(m)$. 因此可知當 $m,n>2$ 時 $\gcd(\phi(m),\phi(n))\ge 2$. 利用此一結果, 我們馬上可得另一個重要結論.

Proposition 6.2.4. 當 $m>2$ 且 $n>2$ 為兩互質的整數時, 在 *modulo* mn 之下沒有 *primitive root.*

Proof. 因 m,n 皆大於 2 我們知 $2|\phi(m)$ 且 $2|\phi(n)$ 故得 $\gcd(\phi(m),\phi(n))\ge 2$. 另一方面 m 和 n 是互質的, 故對任一與 mn 互質的整數 a, 由 Lemma 6.2.3 知

$$\mathrm{ord}_{mn}(a)\le\frac{\phi(mn)}{\gcd(\phi(m),\phi(n))}\le\frac{\phi(mn)}{2}<\phi(mn).$$

故知在 modulo mn 之下無 primitive root. □

當 $m > 1$ 且沒有奇的質因數時, 我們知道當 $m = 2, 4$ 時在 modulo m 之下有 primitive root, 而在其他狀況 (即 $m = 2^n$ 且 $n \geq 3$) Proposition 6.2.2 告訴我們在 modulo m 之下沒有 primitive root. 當 m 有奇的質因數時, Proposition 6.2.4 告訴我們若 m 有兩個或兩個以上奇的質因數時, 在 modulo m 之下沒有 primitive root. 而當 m 只有一個奇的質因數時, Proposition 6.2.4 也告訴我們若 $4|m$, 在 modulo m 之下沒有 primitive root. 所以我們僅剩下 m 僅有一個奇的質因數且 $4 \nmid m$ 的情形未討論, 即 $m = p^n$ 或 $m = 2p^n$, 其中 p 為奇質數的情形.

6.3. The Primitive Root Theorem

我們僅剩下 $m = p^n$ 或 $m = 2p^n$, 其中 p 為奇質數的情形尚未探討. 事實上在這剩下的情況中, primitive root 皆存在. 在這節中我們將先得到當 p 是一個奇質數時, 在 modulo p 之下可找到 primitive root. 再利用 modulo p 所得的 primitive root 得到在 modulo p^2 之下的 primitive root. 最後利用 modulo p^2 所得的 primitive root 得到 modulo p^n 以及 modulo $2p^n$ 的 primitive root. 在本節中 p 永遠表示為奇質數, 我們就不再多說明.

6.3.1. Modulo p 的 Primitive Root. 我們要說明當 p 是一個奇質數時在 modulo p 之下可以找到 primitive root. 我們曾經提及要證明存在性, 一般來說有兩種方法: 第一種就是提供一個可以找到東西的方法; 另一種就是利用邏輯推演的方式來推導出東西一定存在 (例如用反證法證明若找不到會導致矛盾). 第一種方法的好處是它提供了找到東西的方法所以不只告訴你東西存在且告訴你如何找到. 不過這在一般抽象理論的推導中不是容易的, 例如前一章提過找二次 congruence equation 的解並不容易, 但我們可發展一套理論來確認何時有解. 同樣地, 在證明 primitive root 存在的問題上, 即使已知存在到目前為止仍沒有一套完善的方法可以直接找到 primitive root, 所以我們仍是用邏輯推演的方式來證明存在性.

在 modulo p 時, 有一件事是很特殊的即 Theorem 4.1.3 告訴我們一個 n 次的整係數多項式在 modulo p 之下最多有 n 個解. 然而若 $p \nmid a$ 且 $\mathrm{ord}_p(a) = n$, 已知 $a, a^2, \ldots, a^n$ 在 modulo p 之下皆相異, 且由於 $a^n \equiv 1 \pmod{p}$, 故 $(a^i)^n \equiv 1 \pmod{p}$. 由此可知 $a, a^2, \ldots, a^n$ 這 n 個在 modulo p 之下皆不同餘的數皆為 $x^n \equiv 1 \pmod{p}$ 的一個解, 但由於此式在 modulo p 之下至多有 n 個解, 所以它們就是 $x^n \equiv 1 \pmod{p}$ 所有的解. 另一方面, 若 $p \nmid b$ 且 $\mathrm{ord}_p(b) = n$, 則由於 b 是 $x^n \equiv 1 \pmod{p}$ 之一解, 故由前知存在 $i \in \{1, \ldots, n\}$ 使得 $b \equiv a^i \pmod{p}$. 換言之, 所有在 modulo p 之下 order 為 n 的元素, 在 modulo p 之下必和 $\{a, a^2, \ldots, a^n\}$ 中某個元素同餘, 故利用 Corollary 6.1.9 知在 modulo p 之下僅有 $\phi(n)$ 個元素其 order 為 n. 我們將此結果總結如下.

Lemma 6.3.1. 假設 p 為質數且在 *modulo* p 之下有一元素其 *order* 為 n, 則在 *modulo* p 之下共有 $\phi(n)$ 個元素其 *order* 為 n.

再次強調, 此結果在質數時才對. 例如在 modulo 15 時, 共有 $4, 11$ 和 14 三個元素在 modulo 15 之下的 order 為 2, 而不是 $\phi(2) = 1$ 個.

我們要說在 modulo p 之下有 primitive root 主要的方法便是將 modulo p 之下的元素依其 order 分類. 最後說明 order 為 $\phi(p) = p-1$ 那一類元素所成的集合不是 $\emptyset$ (空集合). 下面就是依這樣分類所得之結果.

Lemma 6.3.2. 假設 p 是質數且令 $S = \{1, 2, \ldots, p-1\}$. 現對於 $d \in \mathbb{N}$ 滿足 $d|p-1$, 我們考慮 $S_d = \{i \in S \mid \mathrm{ord}_p(i) = d\}$.

(1) 若 $d \neq d'$, 則 $S_d \cap S_{d'} = \emptyset$.

(2) $\bigcup_{d|p-1, d>0} S_d = S$.

(3) 若 $S_d \neq \emptyset$, 則 S_d 共有 $\phi(d)$ 個元素.

Proof. (1) 若 $a \in S_d \cap S_{d'}$, 即表示 $\mathrm{ord}_p(a) = d$ 且 $\mathrm{ord}_p(a) = d'$. 但依 order 的定義每一個和 p 互質的數在 modulo p 之下其 order 是唯一的, 此與 $d \neq d'$ 之假設相矛盾, 故知 $S_d \cap S_{d'} = \emptyset$.

(2) $\bigcup_{d|p-1, d>0} S_d$ 這個符號的意思是將所有 S_d 其中 $d \in \mathbb{N}$ 且 $d|p-1$ 聯集起來. 由於對所有 $d|p-1$ 皆有 $S_d \subseteq S$, 所以 $\bigcup_{d|p-1, d>0} S_d \subseteq S$. 另一方面若 $i \in S$, 由於 $p \nmid i$, 故由 Theorem 3.3.4 知 $i^{p-1} \equiv 1 \pmod{p}$. 因此由 Proposition 6.1.4 知 $\mathrm{ord}_p(i) | p-1$. 換句話說, 若 $\mathrm{ord}_p(i) = d$, 則 $d|p-1$, 故知存在 $d|p-1$ 使得 $i \in S_d$. 得證 $S \subseteq \bigcup_{d|p-1, d>0} S_d$, 因此知 $\bigcup_{d|p-1, d>0} S_d = S$.

(3) 若 $S_d \neq \emptyset$, 表示存在 $a \in S_d$. 此時 $p \nmid a$ 且 $\mathrm{ord}_p(a) = d$, 故利用 Lemma 6.3.1 知在 modulo p 之下共有 $\phi(d)$ 個元素其 order 為 d. 由於 S 是 reduced residue system modulo p, 這 $\phi(d)$ 個元素在 modulo p 之下必和 S 中 $\phi(d)$ 個元素同餘. 因此 S 中這 $\phi(d)$ 個元素剛好組成 S_d, 故知 S_d 共有 $\phi(d)$ 個元素. □

Lemma 6.3.2(1,2) 告訴我們 $S = \{1, 2, \ldots, p-1\}$ 中的每一個元素必會落在某個且恰有一個 S_d 中, 其中 $d \in \mathbb{N}$ 且 $d|p-1$. 因此若計算每個 S_d 中的元素個數再加總起來其值應為 S 中的元素個數 $p-1$. 依此我們可以得到以下重要的結果.

Theorem 6.3.3. 假設 p 是一個質數且 $d \in \mathbb{N}$ 滿足 $d|p-1$. 則在 *modulo* p 之下共有 $\phi(d)$ 個元素其 *order* 為 d. 特別地, 在 *modulo* p 之下 *primitive root* 必存在.

Proof. 我們沿用 Lemma 6.3.2 中所用的符號, 並令 $n(d)$ 表示 $S_d = \{i \in S \mid \mathrm{ord}_p(i) = d\}$ 中元素的個數, 即 $n(d)$ 為在 modulo p 之下 order 為 d 的元素個數.

由 Lemma 6.3.2(1,2) 我們知 $\sum_{d|p-1, d>0} n(d) = p-1$ 而且 Lemma 6.3.2(3) 告訴我們 $n(d) = 0$ 或 $n(d) = \phi(d)$. 另一方面利用 Corollary 2.3.6 我們知 $\sum_{d|p-1, d>0} \phi(d) = p-1$, 而 $\phi(d) > 0$, 故比較 $\sum_{d|p-1, d>0} n(d) = \sum_{d|p-1, d>0} \phi(d)$, 可得對所有的 $d \in \mathbb{N}$ 滿足 $d|p-1$ 皆有 $n(d) = \phi(d)$.

特別地 $n(p-1)=\phi(p-1)$ 表示在 modulo p 之下有 $\phi(p-1)\neq 0$ 個元素其 order 為 $p-1$, 也就是說這些元素皆為 primitive root. 故知在 modulo p 之下 primitive root 是存在的. □

我們證明了在 modulo p 之下 primitive root 是存在的. 這個證明方式很明顯的並沒有告訴我們如何找到 primitive root. 事實上我們所用的證明方式有點像反證法, 也就是說如果沒有 primitive root, 那麼在計算上面那些元素個數時會發生數目兜不攏的情形而造成矛盾.

6.3.2. Modulo p^2 的 primitive root. 很容易去猜測若在 modulo p^2 之下有 primitive root, 那麼這個 primitive root 應來自於 modulo p 之下的 primitive root. 因此我們將利用 modulo p 的 primitive root 來找到 modulo p^2 的 primitive root. 這裡的存在性的證明就比較具體, 也就是說如果能找到 modulo p 的 primitive root, 那們我們的證明能給出具體的方法來找到 modulo p^2 的 primitive root.

首先我們來看如何判別一個 modulo p 的 primitive root 在 modulo p^2 之下是否為 primitive root.

Lemma 6.3.4. 假設 $a\in\mathbb{Z}$ 是一個 *primitive root modulo* p. 則 $\mathrm{ord}_{p^2}(a)=p-1$ 或 $\mathrm{ord}_{p^2}(a)=p(p-1)$. 特別地, $a^{p-1}\not\equiv 1 \pmod{p^2}$ 若且唯若 a 在 *modulo* p^2 之下是一個 *primitive root.*

Proof. 依假設 a 在 modulo p 之下是 primitive root 表示 $\mathrm{ord}_p(a)=p-1$. 現假設 $\mathrm{ord}_{p^2}(a)=n$, 則 $a^n\equiv 1 \pmod{p^2}$, 因此知 $a^n\equiv 1 \pmod{p}$. 故依 $\mathrm{ord}_p(a)=p-1$ 及 Proposition 6.1.4 知 $p-1|n$. 又因為 a 與 p 互質, 故 a 與 p^2 互質, 故由 Euler's Theorem 知 $a^{\phi(p^2)}\equiv 1 \pmod{p^2}$, 因此在 modulo p^2 的情況再利用 Proposition 6.1.4 知 $n|\phi(p^2)$. 由於 $\phi(p^2)=p(p-1)$, 我們得 $p-1|n$ 且 $n|p(p-1)$. 也就是 $n=\lambda(p-1)$ 且又 $\lambda(p-1)|p(p-1)$, 故知 $\lambda|p$. 因此由 p 是質數知 $\lambda=1$ 或 $\lambda=p$. 故得證 $\mathrm{ord}_{p^2}(a)=p-1$ 或 $\mathrm{ord}_{p^2}(a)=p(p-1)$.

現若 $a^{p-1}\not\equiv 1 \pmod{p^2}$, 知 a 在 modulo p^2 之下其 order 一定不是 $p-1$, 故得 $\mathrm{ord}_{p^2}(a)=p(p-1)=\phi(p^2)$. 由 Corollary 6.1.7 得證 a 在 modulo p^2 之下是一個 primitive root. 反之若 a 在 modulo p^2 之下是 primitive root, 即 $\mathrm{ord}_{p^2}(a)=p(p-1)$, 故由 order 的定義知 $a^{p-1}\not\equiv 1 \pmod{p^2}$. □

知道如何判別 modulo p 的 primitive root 在 modulo p^2 亦是 primitive root 後, 接下來我們就要找到哪些 modulo p 的 primitive root 在 modulo p^2 之下仍為 primitive root. 現假設 a 在 modulo p 之下是 primitive root, 那麼那些在 modulo p 之下和 a 同餘的數在 modulo p 之下也都是 primitive root, 但這些數在 modulo p^2 之下可能不同餘, 我們就將它們一一列出. 也就是說, $a, a+p, \ldots, a+(p-1)p$, 共有這 p 個數是在 modulo p 之下同餘但在 modulo p^2 之下不同餘.

Proposition 6.3.5. 假設 p 是一個質數且 $a\in\mathbb{Z}$ 為一個在 *modulo* p 之下的 *primitive root.* 令 $S=\{a, a+p, a+2p+\cdots, a+(p-1)p\}$, 則在 S 中僅有一個元素在 *modulo* p 之下不是 *primitive root,* 其餘 $p-1$ 個元素在 *modulo* p 之下是 *primitive root.*

Proof. 已知 a 在 modulo p 之下是 primitive root 且 S 中的元素在 modulo p 之下皆與 a 同餘, 故知 S 中的元素在 modulo p 之下皆為 primitive root. 所以我們可以利用 Lemma 6.3.4 檢查 S 中哪些元素 $a+tp$ 會使得 $(a+tp)^{p-1} \equiv 1 \pmod{p^2}$.

由於 $a^{p-1} \equiv 1 \pmod{p}$, 故存在 $\lambda \in \mathbb{Z}$ 使得 $a^{p-1} = 1 + \lambda p$. 因此

$$(a+tp)^{p-1} = a^{p-1} + (p-1)a^{p-2}(tp) + \frac{(p-1)(p-2)}{2}a^{p-3}(tp)^2 + \cdots$$

由於 $C_2^{p-1}a^{p-3}(tp)^2$ 這一項以及其之後每一項 $C_k^{p-1}a^{p-1-k}(tp)^k$, $k \geq 3$ 在 modulo p^2 之下皆為 0, 所以我們得

$$(a+tp)^{p-1} \equiv a^{p-1} - a^{p-2}tp \equiv 1 + (\lambda - a^{p-2}t)p \pmod{p^2}.$$

因此要找到 t 使得 $(a+tp)^{p-1} \equiv 1 \pmod{p^2}$ 若且唯若 $p|\lambda - a^{p-2}t$. 也就是說我們要找到 $t \in \{0, 1, 2, \ldots, p-1\}$ 使得 $a^{p-2}t \equiv \lambda \pmod{p}$. 然而 $a^{p-1} \equiv 1 \pmod{p}$, 故上式兩邊乘上 a 得 $t \equiv a\lambda \pmod{p}$. 也就是說當 $0 \leq t \leq p-1$, 僅有 $t \equiv a\lambda \pmod{p}$ 時, 會使得 $(a+tp)^{p-1} \equiv 1 \pmod{p^2}$, 此時 $a+tp$ 在 modulo p^2 之下不是 primitive root. 其餘 S 中的元素 $a+rp$ 由於皆會使得 $(a+rp)^{p-1} \not\equiv 1 \pmod{p^2}$, 故由 Lemma 6.3.4 知皆為 modulo p^2 之下的 primitive root. □

從 Theorem 6.3.3 以及 Proposition 6.3.5 我們知道由於 modulo p 的 primitive root 存在, 所以 modulo p^2 的 primitive root 也存在. 事實上若 a 是 modulo p 的 primitive root, 我們僅要檢驗是否 $a^{p-1} \equiv 1 \pmod{p^2}$. 要是 $a^{p-1} \not\equiv 1 \pmod{p^2}$, 那麼由 Lemma 6.3.4, 我們知 a 在 modulo p^2 之下是 primitive root. 要是 $a^{p-1} \equiv 1 \pmod{p^2}$, 那麼 a 在 modulo p^2 之下不是 primitive root, 故由 Proposition 6.3.5 知 $a+p$ 在 modulo p^2 之下必為 primitive root.

6.3.3. Modulo p^n 的 Primitive Root. 由於 modulo p 的 primitive root 存在, 利用 Corollary 6.1.9 知在 modulo p 之下共有 $\phi(\phi(p)) = \phi(p-1)$ 個 primitive roots. Proposition 6.3.5 告訴我們每一個 modulo p 的 primitive root 在 modulo p^2 之下可得 $p-1$ 個 primitive roots, 所以在 modulo p^2 之下我們共找到了 $(p-1)\phi(p-1)$ 個 primitive roots. 然而由於 modulo p^2 的 primitive root 存在, Corollary 6.1.9 告訴我們在 modulo p^2 之下共有 $\phi(\phi(p^2)) = \phi(p(p-1))$ 個 primitive roots. 由於 p 和 $p-1$ 互質, 我們有 $\phi(\phi(p^2)) = \phi(p)\phi(p-1) = (p-1)\phi(p-1)$. 此值恰與前面由 modulo p 的 primitive root 所得 modulo p^2 的 primitive roots 的個數相吻合. 也就是說每一個 modulo p^2 的 primitive root 確來自於某個 modulo p 的 primitive root. 我們可以如此一直估算下去, 若 modulo p^3 的 primitive root 存在, 則由 Corollary 6.1.9 知在 modulo p^3 之下共有

$$\phi(\phi(p^3)) = \phi(p^2(p-1)) = \phi(p^2)\phi(p-1) = p(p-1)\phi(p-1)$$

個 primitive roots. 而又已知在 modulo p^2 之下共有 $(p-1)\phi(p-1)$ 個 primitive roots. 每一個 modulo p^2 的 primitive root, 在 modulo p^3 之下共可產生 p 個不同餘類, 所以這 $(p-1)\phi(p-1)$ 個 modulo p^2 的 primitive roots 在 modulo p^3 之下共產生了 $p(p-1)\phi(p-1)$ 個不同餘類. 這個數字恰與前面所提若 modulo p^3 的 primitive root 存在則在 modulo p^3 之

下共有 $p(p-1)\phi(p-1)$ 個 primitive roots 相吻合. 也就是說每一個 modulo p^2 的 primitive root, 在 modulo p^3 之下產生的 p 個不同餘類"應該"在 modulo p^3 仍為 primitive root.

接下來我們就是要用數學歸納法來驗證此事, 我們要證明當 $n \geq 3$ 時任何數只要在 modulo p^2 是 primitive root, 則在 modulo p^n 必也是 primitive root. 首先我們來看如何判別一個 modulo p^n 的 primitive root 在 modulo p^{n+1} 之下是否為 primitive root.

Lemma 6.3.6. 假設 $a \in \mathbb{Z}$ 是一個 *primitive root modulo* p^n. 則 $\mathrm{ord}_{p^{n+1}}(a) = p^{n-1}(p-1)$ 或 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1)$. 特別地, $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$ 若且唯若 a 在 *modulo* p^{n+1} 之下是一個 *primitive root.*

Proof. 依假設 a 在 modulo p^n 之下是 primitive root 表示 $\mathrm{ord}_{p^n}(a) = \phi(p^n) = p^{n-1}(p-1)$. 現假設 $\mathrm{ord}_{p^{n+1}}(a) = k$, 則 $a^k \equiv 1 \pmod{p^{n+1}}$, 因此知 $a^k \equiv 1 \pmod{p^n}$. 故依 $\mathrm{ord}_{p^n}(a) = p^{n-1}(p-1)$ 及 Proposition 6.1.4 知 $p^{n-1}(p-1)|k$. 又因為 a 與 p 互質, 故 a 與 p^{n+1} 互質, 故由 Euler's Theorem 知 $a^{\phi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}$, 因此在 modulo p^{n+1} 的情況再利用 Proposition 6.1.4 知 $k|\phi(p^{n+1})$. 由於 $\phi(p^{n+1}) = p^n(p-1)$, 我們得 $p^{n-1}(p-1)|k$ 且 $k|p^n(p-1)$. 也就是 $k = \lambda p^{n-1}(p-1)$ 且又 $\lambda p^{n-1}(p-1)|p^n(p-1)$, 故知 $\lambda|p$. 因此由 p 是質數知 $\lambda = 1$ 或 $\lambda = p$. 故得證 $\mathrm{ord}_{p^{n+1}}(a) = p^{n-1}(p-1)$ 或 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1)$.

現若 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$, 知 a 在 modulo p^{n+1} 之下其 order 一定不是 $p^{n-1}(p-1)$, 故得 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1) = \phi(p^{n+1})$. 由 Corollary 6.1.7 得證 a 在 modulo p^{n+1} 之下是一個 primitive root. 反之若 a 在 modulo p^{n+1} 之下是 primitive root, 即 $\mathrm{ord}_{p^{n+1}}(a) = p^n(p-1)$, 故由 order 的定義知 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$. □

現若我們找到 a 在 modulo p^2 之下是 primitive root, 要檢查 a 在 modulo p^3 之下是否為 primitive root, 依 Lemma 6.3.6, 我們要檢查 $a^{p(p-1)}$ 在 modulo p^3 之下是否與 1 同餘. 然而已知 $a^{p-1} \equiv 1 \pmod{p}$ (Fermat's Little Theorem) 我們可令 $a^{p-1} = 1 + \lambda p$. 此時由於 a 在 modulo p^2 之下是 primitive root 故由 Lemma 6.3.4 知 $a^{p-1} \not\equiv 1 \pmod{p^2}$, 即 $p \nmid \lambda$. 依此可得

$$a^{p(p-1)} = (a^{p-1})^p = (1+\lambda p)^p = 1 + p(\lambda p) + \frac{p(p-1)}{2}(\lambda p)^2 + \cdots .$$

這裡由於 p 是奇數所以 $p|p(p-1)/2$ (注意這就是為何此結果在 $p = 2$ 時不成立的原因), 再加上之後每一項 $C_k^p(\lambda p)^k$, $k \geq 3$ 在 modulo p^3 之下皆為 0, 所以我們得

$$a^{p(p-1)} \equiv 1 + \lambda p^2 \pmod{p^3}.$$

故由 $p \nmid \lambda$ 得證 $a^{p(p-1)} \not\equiv 1 \pmod{p^3}$, 所以依 Lemma 6.3.6 知 a 在 modulo p^3 之下亦為 primitive root. 如此一直下去, 我們可證得當 $n \geq 3$ 時, a 在 modulo p^n 之下皆為 primitive root.

Proposition 6.3.7. 假設 a 在 *modulo* p^2 之下是一個 *primitive root.* 則對任意 $n \geq 3$, a 在 *modulo* p^n 之下也是 *primitive root.*

Proof. 前面我們已證得 a 在 modulo p^3 之下是 primitive root. 現在依歸納法, 我們假設 a 在 modulo p^n $(n \geq 3)$ 之下是 primitive root, 要證明 a 在 modulo p^{n+1} 之下仍為 primitive root.

由於 a 與 p 互質, 依 Euler's Theorem 知 $a^{\phi(p^{n-1})} = a^{p^{n-2}(p-1)} \equiv 1 \pmod{p^{n-1}}$. 現假設 $a^{p^{n-2}(p-1)} = 1 + \lambda p^{n-1}$. 由於 a 在 modulo p^n 之下是 primitive root, 依 Lemma 6.3.6 知 $a^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$, 故知 $p \nmid \lambda$. 現考慮

$$a^{p^{n-1}(p-1)} = (a^{p^{n-2}(p-1)})^p = (1 + \lambda p^{n-1})^p = 1 + p(\lambda p^{n-1}) + \frac{p(p-1)}{2}(\lambda p^{n-1})^2 + \cdots .$$

在 $p(\lambda p^{n-1})$ 之後每一項 $C_k^p(\lambda p^{n-1})^k$, $k \geq 2$ 中由於 $k(n-1) \geq 2(n-1) = n + (n-2) \geq n+1$ (因為 $n \geq 3$), 所以當 $k \geq 2$ 時在 modulo p^{n+1} 之下 $C_k^p(\lambda p^{n-1})^k$ 皆為 0, 所以我們得

$$a^{p^{n-1}(p-1)} \equiv 1 + \lambda p^n \pmod{p^{n+1}}.$$

故由 $p \nmid \lambda$ 得證 $a^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$, 所以依 Lemma 6.3.6 知 a 在 modulo p^{n+1} 之下亦為 primitive root. □

從 Theorem 6.3.3 以及 Proposition 6.3.5 我們知道 modulo p^2 的 primitive root 存在, 所以再由 Proposition 6.3.7 得知當 $n \geq 3$ 時 modulo p^n 的 primitive root 也存在. 再次強調由於從 modulo p^2 的 primitive root 推得 modulo p^3 的 primitive root 之過程需用到 p 是奇數所以當 $n \geq 3$ 時 modulo p^n 的 primitive root 存在需在 p 是奇質數才成立. 事實上之前我們已知在 modulo $2^3 = 8$ 時 primitive root 是不存在的.

6.3.4. Modulo $2p^n$ 的 Primitive Root. 我們已知在 modulo p^n 之下皆有 primitive root. 現在我們將由 modulo p^n 的 primitive root 找出 modulo $2p^n$ 的 primitive. 首先我們來看當 m 是奇數時 modulo m 的 order 和 modulo $2m$ 的 order 間之關係.

Lemma 6.3.8. 給定一奇數 m, 且 $a \in \mathbb{Z}$ 是一個和 m 互質的奇數. 若 $\mathrm{ord}_m(a) = n$, 則 $\mathrm{ord}_{2m}(a) = n$.

Proof. 由於 a 是奇數且與 m 互質, 故知 $\gcd(a, 2m) = 1$. 因此 a 在 modulo $2m$ 之下的 order 是有定義的, 就假設 $\mathrm{ord}_{2m}(a) = k$. 由 $a^k \equiv 1 \pmod{2m}$ 可得 $a^k \equiv 1 \pmod{m}$. 故由 $\mathrm{ord}_m(a) = n$ 以及 Proposition 6.1.4 知 $n|k$. 另一方面由於 $a^n \equiv 1 \pmod{m}$ 且 a 為奇數知 $a^n \equiv 1 \pmod{2}$, 故知 $m|a^n - 1$ 且 $2|a^n - 1$. 又由於 m 是奇數知 $\gcd(2, m) = 1$, 故由 Proposition 1.2.7(2) 知 $2m|a^n - 1$, 也就是說 $a^n \equiv 1 \pmod{2m}$. 因假設 $\mathrm{ord}_{2m}(a) = k$, 故再利用 Proposition 6.1.4 得 $k|n$. 因此得證 $k = n$ 也就是說 $\mathrm{ord}_{2m}(a) = n$. □

假設 a 為 modulo p^n 的 primitive root, 即 $\mathrm{ord}_{p^n}(a) = \phi(p^n)$. 若 a 又是奇數則由 Lemma 6.3.8 知 $\mathrm{ord}_{2p^n}(a) = \phi(p^n)$. 但由於 p 是奇質數與 2 互質, 故知 $\phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$. 也就是說 $\mathrm{ord}_{2p^n}(a) = \phi(2p^n)$. 故由 Corollary 6.1.7 知 a 在 modulo $2p^n$ 之下亦為 primitive root. 利用此結果我們可找到 modulo $2p^n$ 的 primitive root.

Proposition 6.3.9. 給定 p 是一個奇質數, 則一定可找到一奇數 a 使其在 *modulo* p^2 之下是一個 *primitive root.* 特別地, 此時對任意 $n \in \mathbb{N}$, a 在 *modulo* $2p^n$ 之下亦為 *primitive root.*

Proof. 當 $p = 3$ 時, 由於 $\mathrm{ord}_3(5) = \mathrm{ord}_3(2) = 2$ 故知 5 在 modulo 3 之下是一個 primitive root. 又由於 $5^{3-1} = 25 \not\equiv 1 \pmod 9$, 故由 Lemma 6.3.4 知 5 在 modulo 3^2 之下是一個 primitive root.

當 $p \geq 5$ 是一個奇質數時, Theorem 6.3.3 告訴我們在 modulo p 之下的 primitive root 存在. 現假設 α 是一個 modulo p 之下的 primitive root. 利用 Proposition 6.3.5 知 $\{\alpha, \alpha+p, \ldots, \alpha+(p-1)p\}$ 中僅有一個在 modulo p^2 之下不是 primitive root. 由於 $p \geq 5$, 得 $p-1 \geq 4$, 故知 $\{\alpha, \alpha+p, \alpha+2p, \alpha+3p\}$ 中至多有一個在 modulo p^2 之下不是 primitive root. 因此若 α 是奇數, 則得 $\alpha, \alpha+2p$ 這兩個奇數中必有一個在 modulo p^2 之下是 primitive root. 若 α 是偶數, 則得 $\alpha+p, \alpha+3p$ 這兩個奇數中必有一個在 modulo p^2 之下是 primitive root. 我們得證必存在一奇數在 modulo p^2 之下是 primitive root.

現假設 a 是一奇數且在 modulo p^2 之下是 primitive root. 由 Proposition 6.3.7 知 a 在 modulo p^n 之下亦為 primitive root. 故由 Lemma 6.3.8 知 $\mathrm{ord}_{2p^n}(a) = \mathrm{ord}_{p^n}(a) = \phi(p^n) = \phi(2p^n)$, 故得證 a 在 modulo $2p^n$ 之下亦為 primitive root. □

事實上要找到一奇數使其在 modulo p^2 之下是 primitive root 並不需如 Proposition 6.3.9 的證明中那麼複雜. 若 a 是偶數且在 modulo p^2 之下是 primitive root, 那麼 $a+p^2$ 必為奇數且由於 $a+p^2 \equiv a \pmod{p^2}$ 所以 $a+p^2$ 當然也是在 modulo p^2 之下的 primitive root. 不過由於考慮 $a+p^2$ 數值較大, 我們若要找較小的 primitive root, 證明中最大只要考慮到 $a+3p$, 這個數當 p 很大時當然比 $a+p^2$ 要小得多.

我們總結這兩節 Proposition 6.2.2, Proposition 6.2.4, Theorem 6.3.3, Proposition 6.3.5, Proposition 6.3.7 以及 Proposition 6.3.9 之結果得到以下所謂的 primitive root Theorem.

Theorem 6.3.10 (Primitive Root Theorem)**.** 只有當 $m = 2, 4, p^n, 2p^n$ 時, 其中 p 為奇質數且 $n \in \mathbb{N}$, 在 *modulo* m 之下會有 *primitive root.*

6.4. 高次的 Congruence Equation

所謂高次的 congruence equation 指的是次數大於 2 的 congruence equation. 我們這裡要處理的當然不是一般的 congruence equation. 我們想利用 primitive root 來幫我們解如 $x^n \equiv a \pmod m$ 其中 $\gcd(a, m) = 1$ 這樣的 congruence equation.

首先我們將 m 寫成質因數的乘積, 即 $m = 2^{n_0} p_1^{n_1} \cdots p_r^{n_r}$, 其中這些 p_i 為相異奇質數而 $n_0 \geq 0$. 利用 Corollary 4.4.3, 我們知道 $x^n \equiv a \pmod m$ 有解若且唯若 $x^n \equiv a \pmod{2^{n_0}}$ 以及所有的 $i \in \{1 \ldots, r\}$, $x^n \equiv a \pmod{p_i^{n_i}}$ 皆有解. 所以我們只要探討 $x^n \equiv a \pmod{2^{n_0}}$ 及 $x^n \equiv a \pmod{p_i^{n_i}}$ 解的情況. 當 $n_0 \geq 3$ 時, 由於在 modulo 2^{n_0} 沒有 primitive root, 討論解的情形較複雜, 這裡我們不多做討論. 我們僅討論當 $n_0 \leq 2$ 的情形, 也就是說此處我們探討解 $x^n \equiv a \pmod m$ 的方法僅適用於 $8 \nmid m$ 的情況. 在此情況之下我們只要解 $x^n \equiv a$

$(\mathrm{mod}\ 2^{n_0})$, 其中 $n_0 \leq 2$, 以及解 $x^n \equiv a\ (\mathrm{mod}\ p_i^{n_i})$. 這兩種情況 (即 modulo 2^{n_0} 和 modulo $p_i^{n_i}$), 由於 primitive root 皆存在, 我們利用下面的方法就可判別其解是否存在.

Theorem 6.4.1. 給定 $m \in \mathbb{N}$, 假設在 *modulo* m 之下 *primitive root* 存在. 考慮 $x^n \equiv a\ (\mathrm{mod}\ m)$, 其中 $n \in \mathbb{N}$ 且 $\gcd(a, m) = 1$. 令 $d = \gcd(n, \phi(m))$. 則 $x^n \equiv a\ (\mathrm{mod}\ m)$ 有解若且唯若

$$a^{\phi(m)/d} \equiv 1 \pmod{m}.$$

Proof. 首先假設 $x^n \equiv a\ (\mathrm{mod}\ m)$ 有解, 即存在 $c \in \mathbb{Z}$ 滿足 $c^n \equiv a\ (\mathrm{mod}\ m)$. 因為 $\gcd(a, m) = 1$, 所以 $\gcd(c, m) = 1$, 故由 Euler's Theorem (3.3.2) 知 $c^{\phi(m)} \equiv 1\ (\mathrm{mod}\ m)$. 此時由於 $d|\phi(m)$ 且 $d|n$, 故得

$$a^{\phi(m)/d} \equiv (c^n)^{\phi(m)/d} = (c^{\phi(m)})^{n/d} \equiv 1 \pmod{m}.$$

(注意此部分的證明是不需 modulo m 的 primitive root 存在之假設.)

反之, 假設 γ 為 modulo m 之下的一個 primitive root. 依定義 $\{\gamma, \gamma^2, \ldots, \gamma^{\phi(m)}\}$ 是一個 reduced residue system modulo m, 也就是說任何和 m 互質的數 b, 皆存在 $i \in \mathbb{N}$ 使得 $\gamma^i \equiv b\ (\mathrm{mod}\ m)$. 因此存在 $r \in \mathbb{N}$ 使得 $a \equiv \gamma^r\ (\mathrm{mod}\ m)$. 另一方面若 c 是 $x^n \equiv a\ (\mathrm{mod}\ m)$ 的一個解, 則由於 $\gcd(c, m) = 1$, 一定也存在 $t \in \mathbb{N}$ 使得 $c \equiv \gamma^t\ (\mathrm{mod}\ m)$. 因此要解 $x^n \equiv a\ (\mathrm{mod}\ m)$ 就等同於要找到 $t \in \mathbb{N}$ 使得

$$(\gamma^t)^n = \gamma^{nt} \equiv \gamma^r \pmod{m}.$$

由於 γ 是 modulo m 的 primitive root, 我們有 $\mathrm{ord}_m(\gamma) = \phi(m)$, 故利用 Proposition 6.1.6, 知 $\gamma^{nt} \equiv \gamma^r\ (\mathrm{mod}\ m)$ 若且唯若 $nt \equiv r\ (\mathrm{mod}\ \phi(m))$, 也就是說我們要找到 $t \in \mathbb{N}$ 滿足

$$nt \equiv r \pmod{\phi(m)}.$$

另一方面依假設 $a^{\phi(m)/d} \equiv 1\ (\mathrm{mod}\ m)$, 即 $\gamma^{r\phi(m)/d} \equiv 1\ (\mathrm{mod}\ m)$, 故由 Proposition 6.1.4 知 $\phi(m)|r\phi(m)/d$. 這表示 $\phi(m)r/d$ 必須是 $\phi(m)$ 的倍數, 亦即 $r/d \in \mathbb{Z}$, 也就是說 $d|r$. 然而 Proposition 4.3.1 告訴我們給定 n, r, 一次的 congruence equation, $nt \equiv r\ (\mathrm{mod}\ \phi(m))$ 有解若且唯若 $d = \gcd(n, \phi(m))|r$. 所以我們由 $a^{\phi(m)/d} \equiv 1\ (\mathrm{mod}\ m)$ 之假設知 $nt \equiv r\ (\mathrm{mod}\ \phi(m))$ 必有解. 若 t_0 為其一解, 令 $c = \gamma^{t_0}$, 則得

$$c^n = \gamma^{nt_0} \equiv \gamma^r \equiv a \pmod{m}.$$

故知 c 為 $x^n \equiv a\ (\mathrm{mod}\ m)$ 的一個解. □

當 $m = p$ 為一質數 (此時 modulo p 當然有 primitive root) 且 $n = 2$ 時, Theorem 6.4.1 就是 Euler's criterion (Theorem 5.3.3). 所以 Theorem 6.4.1 可以說是 Theorem 5.3.3 的推廣.

接下來我們要知道 $x^n \equiv a\ (\mathrm{mod}\ m)$ 要是有解, 那麼在 modulo m 之下會有多少解. 和往常一樣, 我們所用的方法是直接探討兩個解之間的關係, 如此一來不只可以精確地算出解的個數, 而且可以很快的利用一個已知解將其他的解求出.

Proposition 6.4.2. 給定 $m \in \mathbb{N}$, 假設在 *modulo* m 之下 *primitive root* 存在. 考慮 $x^n \equiv a \pmod{m}$, 其中 $n \in \mathbb{N}$ 且 $\gcd(a, m) = 1$. 令 $d = \gcd(n, \phi(m))$. 若 $x^n \equiv a \pmod{m}$ 有解, 則在 *modulo* m 之下共有 d 個解.

事實上, 若 $x \equiv c \pmod{m}$ 是 $x^n \equiv a \pmod{m}$ 的一個解且 γ 是 *modulo* m 之下的一個 *primitive root,* 則在 *modulo* m 之下 $x \equiv c\gamma^{t\phi(m)/d} \pmod{m}$, 其中 $t \in \{0, 1, \ldots, d-1\}$ 是 $x^n \equiv a \pmod{m}$ 所有的解.

Proof. 由於 a 和 m 互質, $x^n \equiv a \pmod{m}$ 的解皆與 m 互質. 又由於 γ 是 modulo m 之下的一個 primitive root, 所以對於 $x^n \equiv a \pmod{m}$ 的任兩個解, 我們可假設其分別為 γ^r 和 γ^s, 其中 $r, s \in \mathbb{N}$. 也就是說

$$\gamma^{rn} = (\gamma^r)^n \equiv a \equiv (\gamma^s)^n \equiv \gamma^{sn} \pmod{m}.$$

因此利用 $\mathrm{ord}_m(\gamma) = \phi(m)$ 以及 Proposition 6.1.6 得 $rn \equiv sn \pmod{\phi(m)}$. 因此由於 $d = \gcd(n, \phi(m))$ 依 Proposition 3.2.3 知 $r \equiv s \pmod{\phi(m)/d}$. 也就是說存在 $\lambda \in \mathbb{Z}$ 使得 $s = r + \lambda\phi(m)/d$. 反之, 若 γ^r 是 $x^n \equiv a \pmod{m}$ 的一個解且 $s = r + \lambda\phi(m)/d$, 則

$$(\gamma^s)^n = (\gamma^r\gamma^{\lambda\phi(m)/d})^n = \gamma^{rn}\gamma^{\lambda\phi(m)n/d} \equiv a\,(\gamma^{\phi(m)})^{\lambda n/d} \equiv a \pmod{m}.$$

因此 γ^s 也是 $x^n \equiv a \pmod{m}$ 的一個解.

我們證得了若 $x \equiv c \equiv \gamma^r \pmod{m}$, 是 $x^n \equiv a \pmod{m}$ 的一個解, 則 $x \equiv c\gamma^{\lambda\phi(m)/d} \pmod{m}$, 其中 $\lambda \in \mathbb{Z}$, 是 $x^n \equiv a \pmod{m}$ 所有的解. 不過這些解在 modulo m 之下有許多是相同的, 我們必須將有哪些相異解找出. 然而 c 和 m 互質, 故由 Corollary 3.2.4知 $c\gamma^{\lambda\phi(m)/d} \equiv c\gamma^{\lambda'\phi(m)/d} \pmod{m}$ 若且唯若 $\gamma^{\lambda\phi(m)/d} \equiv \gamma^{\lambda\phi(m)/d} \pmod{m}$. 再利用 $\mathrm{ord}_m(\gamma) = \phi(m)$ 以及 Proposition 6.1.6 知 $\gamma^{\lambda\phi(m)/d} \equiv \gamma^{\lambda'\phi(m)/d} \pmod{m}$ 若且唯若 $\lambda\phi(m)/d \equiv \lambda'\phi(m)/d \pmod{\phi(m)}$ 也就是說 $\phi(m)|(\lambda - \lambda')\phi(m)/d$ 亦即 $d|\lambda - \lambda'$. 因此當 $0 \le t \le d-1$ 時, $c\gamma^{t\phi(m)/d}$ 在 modulo m 之下皆相異. 另一方面對任意 $\lambda \in \mathbb{Z}$ 皆存在 $h, t \in \mathbb{Z}$ 使得 $\lambda = hd + t$, 其中 $0 \le t \le d-1$. 所以 $c\gamma^{\lambda\phi(m)/d}$ 在 modulo m 之下都會與某個 $c\gamma^{t\phi(m)/d}$ 同餘, 其中 $t \in \{0, 1, \ldots, d-1\}$. 因此我們得證 $x^n \equiv a \pmod{m}$ 若有 $x \equiv c \pmod{m}$ 這一個解 則在 modulo m 之下 $x^n \equiv a \pmod{m}$ 共有 $x \equiv c, c\gamma^{\phi(m)/d}, c\gamma^{2\phi(m)/d}, \ldots, c\gamma^{(d-1)\phi(m)/d}$ 這 d 個解. □

接下來我們利用一個實際的例子解釋 Proposition 6.4.1 和 Proposition 6.4.2 所得之結果.

Example 6.4.3. 我們來探討 $x^{12} \equiv 10 \pmod{27}$ 和 $x^{12} \equiv 11 \pmod{27}$ 解的情形.

由於 $27 = 3^3$ 所以在 modulo 27 之下 primitive root 是存在的. 又 $\phi(27) = 18$ 且 $\gcd(12, \phi(27)) = \gcd(12, 18) = 6$ 利用 Proposition 6.4.1 我們可分別由 $10^{\phi(27)/6} = 10^3$ 和 11^3 在 modulo 27 是否為 1 來判定 $x^{12} \equiv 10 \pmod{27}$ 和 $x^{12} \equiv 11 \pmod{27}$ 是否有解. 事實上 $10^3 \equiv 1 \pmod{27}$ 且 $11^3 \equiv 8 \not\equiv 1 \pmod{27}$, 所以 $x^{12} \equiv 10 \pmod{27}$ 有解而 $x^{12} \equiv 11 \pmod{27}$ 無解.

要找出 $x^{12} \equiv 10 \pmod{27}$ 的解, 首先需先找到 modulo 27 的一個 primitive root. 由於 2 是 modulo 3 的 primitive root 且 $2^2 \equiv 4 \not\equiv 1 \pmod{9}$, 所以由 Lemma 6.3.4 知 2 在 modulo 9 是 primitive root. 因而由 Proposition 6.3.7 知 2 在 modulo 27 之下依然是 primitive root. 既然 2 是 modulo 27 的一個 primitive root 經計算我們知 $2^6 \equiv 10 \pmod{27}$ 且可以將 $x^{12} \equiv 10 \pmod{27}$ 的一解寫成 $x \equiv 2^t \pmod{27}$ 的形式. 也就是說我們要解

$$(2^t)^{12} \equiv 2^6 \pmod{27}.$$

因此由 $\mathrm{ord}_{27}(2) = \phi(27) = 18$ 以及 Proposition 6.1.6 知此等價於解

$$12t \equiv 6 \pmod{18}.$$

故由 $\gcd(18, 12) = 6$ 得 $2t \equiv 1 \pmod{3}$, 即 $t \equiv 2 \pmod{3}$. 解出 $x \equiv 2^2 \equiv 4 \pmod{27}$ 為 $x^{12} \equiv 10 \pmod{27}$ 的一個解. 再由 $\phi(27)/6 = 3$ 以及 Proposition 6.4.2 知 $x \equiv 4, 4\times 2^3, 4\times 2^6, 4\times 2^9, 4\times 2^{12}, 4\times 2^{15} \pmod{27}$, 即 $x \equiv 4, 5, 13, 23, 22, 14 \pmod{27}$ 為 $x^{12} \equiv 10 \pmod{27}$ 所有的解. 事實上我們也可以由 $12t \equiv 6 \pmod{18}$ 找到 $t \equiv 2, 5, 8, 11, 14, 17 \pmod{18}$ 為其所有的解, 而得 $x \equiv 2^2, 2^5, 2^8, 2^{11}, 2^{14}, 2^{17} \pmod{27}$ 為 $x^{12} \equiv 10 \pmod{27}$ 所有的解.

Chapter 7

略談 Diophantine Equations

我們利用探討 Diophantine equations 的問題來作為本講義之總結. 一般而言若 $f(x_1,\ldots,x_n)$ 是一個多變數的整係數多項式, 求 $f(x_1,\ldots,x_n)=0$ 的所有整數解就是 Diophantine equation 的問題. 由於是求整數解有無限多種可能, 所以解 Diophantine equations 的問題比起解有限問題的 congruence equations 是困難許多. 事實上我們目前學的理論僅能論及一些簡單的 Diophantine equations. 在這裡我們僅希望利用前幾章所學的結果讓大家了解如何用它們來解決問題, 而不想深入的談論 Diophantine equations.

7.1. 兩個處理 Diophantine Equations 的方法

我們簡單的介紹兩種處理 Diophantine equations 的方法. 這兩種方法都是用來處理 Diophantine equations 無解的情況.

第一種方法是用 congruence 的方法處理. 也就是說如果一個 Diophantine equation $f(x_1,\ldots,x_n)=0$ 有整數解, 則對任意的 $m\in\mathbb{N}$ 在 modulo m 之下 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 當然有解. 因此若能找到一個 m 使得 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 無解, 那麼原 Diophantine equation $f(x_1,\ldots,x_n)=0$ 就無解.

Proposition 7.1.1. 假設 $f(x_1,\ldots,x_n)$ 是一個整係數多項式. 若存在 $m\in\mathbb{N}$ 使得 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 無解, 則 $f(x_1,\ldots,x_n)=0$ 無整數解.

Proof. 利用反證法假設 $x_1=c_1,\ldots,x_n=c_n$ 是 $f(x_1,\ldots,x_n)=0$ 的一組整數解. 由於 $f(c_1,\ldots,c_n)=0$, 自然有 $f(c_1,\ldots,c_n)\equiv 0 \pmod m$, 也就是說 $x_1=c_1,\ldots,x_n=c_n$ 是 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 的一組解. 此和 $f(x_1,\ldots,x_n)\equiv 0 \pmod m$ 無解的假設相矛盾故知 $f(x_1,\ldots,x_n)=0$ 無整數解. □

要注意 Proposition 7.1.1 說的是若能找到一個 $m \in \mathbb{N}$ 使得 $f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ 無解, 則 $f(x_1, \ldots, x_n) = 0$ 無整數解. 並不是說若能找到 $m \in \mathbb{N}$ 使得 $f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ 有解, 則 $f(x_1, \ldots, x_n) = 0$ 有整數解. 千萬別搞錯了, 我們來看個例子.

Example 7.1.2. 考慮 Diophantine equation $11x^2 - 7y^2 = 2$. 在 modulo 11 之下, 我們要解 $-7y^2 \equiv 2 \pmod{11}$. 由於 $-7 \times 3 \equiv 1 \pmod{11}$, $-7y^2 \equiv 2 \pmod{11}$ 兩邊乘上 3 可得 $y^2 \equiv 6 \pmod{11}$. 考慮 Legendre symbol $\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. 由於 $11 \equiv 3 \pmod{4}$ 故由 Theorem 5.4.3 知 $\left(\frac{2}{11}\right) = -1$ 且由 Theorem 5.4.6 知 $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$. 因此得 $\left(\frac{6}{11}\right) = -1$, 也就是說 $y^2 \equiv 6 \pmod{11}$ 無解. 換言之, $11x^2 - 7y^2 - 2 \equiv 0 \pmod{11}$ 無解, 因而由 Proposition 7.1.1 知 $11x^2 - 7y^2 = 2$ 無整數解.

注意若將 $11x^2 - 7y^2 = 2$ 考慮在 modulo 7 的情形, 也就是解 $11x^2 \equiv 2 \pmod{7}$. 由於 $11 \times 2 \equiv 1 \pmod{7}$, $11x^2 \equiv 2 \pmod{7}$ 兩邊乘上 2 得 $x^2 \equiv 4 \pmod{7}$. 很明顯的此式有 $x \equiv 2 \pmod{7}$ 為其解, 但由前已知 $11x^2 - 7y^2 = 2$ 並無整數解. 所以由此例可知, 並不能因找到 $m \in \mathbb{N}$ 使得 $f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ 有解, 便斷言 $f(x_1, \ldots, x_n) = 0$ 有解.

或許大家會好奇, 若對於任意的正整數 m, $f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ 皆有解, 是否就能得 $f(x_1, \ldots, x_n) = 0$ 有整數解呢? 由下面的例子我們可以知道, 這仍是不一定對的.

Example 7.1.3. 令 $f(x) = (x^2-17)(x^2-19)(x^2-323)$ 考慮 Diophantine equation $f(x) = 0$. 很明顯的這個 Diophantine equation 並無整數解. 但是我們將說明, 對任意 $m \in \mathbb{N}$, $f(x) \equiv 0 \pmod{m}$ 皆有解.

由 Corollary 4.4.3 我們知道要證明對任意 $m \in \mathbb{N}$, $f(x) \equiv 0 \pmod{m}$ 皆有解, 等同於要證明對任意質數 p 以及 $n \in \mathbb{N}$, $f(x) \equiv 0 \pmod{p^n}$ 皆有解.

當 $p = 2, n = 1$ 時, $f(x) \equiv (x^2 - 1)^3 \pmod{2}$, 故 $f(x) \equiv 0 \pmod{2}$ 有解. 而當 $p = 2, n = 2$ 時, $f(x) \equiv (x^2 - 1)(x^2 - 3)^2 \pmod{4}$, 所以 $f(x) \equiv 0 \pmod{4}$ 亦有解. 當 $p = 2, n \geq 3$ 時, 由於 $17 \equiv 1 \pmod{8}$, Proposition 5.2.1 告訴我們 $x^2 \equiv 17 \pmod{2^n}$ 必有解, 所以 $f(x) = (x^2 - 17)(x^2 - 19)(x^2 - 323) \equiv 0 \pmod{2^n}$ 當然有解.

當 $p = 17$ 時由於 $17 \equiv 1 \pmod{8}$, 故由 Theorem 5.4.3 知 $x^2 \equiv 19 \equiv 2 \pmod{17}$ 有解. 因此由 Proposition 5.2.4 知對任意 $n \in \mathbb{N}$, $x^2 \equiv 19 \pmod{17^n}$ 皆有解. 因此知 $f(x) \equiv 0 \pmod{17^n}$ 有解. 而當 $p = 19$ 時, 由於 $17 \equiv 1 \pmod{8}$ 故得 $\left(\frac{17}{19}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = 1$, 也就是說 $x^2 \equiv 17 \pmod{19}$ 有解. 再由 Proposition 5.2.4 知對任意 $n \in \mathbb{N}$, $x^2 \equiv 17 \pmod{19^n}$ 皆有解. 因此知 $f(x) \equiv 0 \pmod{19^n}$ 有解.

當 p 是奇質數且 $p \neq 17, 19$ 時, 若 $x^2 \equiv 17 \pmod{p}$ 有解, 則 Proposition 5.2.4 告訴我們對任意 $n \in \mathbb{N}$, $x^2 \equiv 17 \pmod{p^n}$ 亦有解. 所以此時 $f(x) \equiv 0 \pmod{p^n}$ 有解. 同理若 $x^2 \equiv 19 \pmod{p}$ 有解, 可得對任意 $n \in \mathbb{N}$, $f(x) \equiv 0 \pmod{p^n}$ 亦有解. 而若 $x^2 \equiv 17 \pmod{p}$ 和 $x^2 \equiv 19 \pmod{p}$ 皆無解, 即 $\left(\frac{17}{p}\right) = \left(\frac{19}{p}\right) = -1$, 則由 $\left(\frac{232}{p}\right) = \left(\frac{17}{p}\right)\left(\frac{19}{p}\right) = 1$

知 $x^2 \equiv 232 \pmod{p}$ 有解, 因此得對任意 $n \in \mathbb{N}$, $x^2 \equiv 232 \pmod{p^n}$ 皆有解. 我們仍得 $f(x) \equiv 0 \pmod{p^n}$ 有解.

綜合以上結果我們知, 對任意質數 p 以及 $n \in \mathbb{N}$, $f(x) \equiv 0 \pmod{p^n}$ 皆有解. 所以對任意 $m \in \mathbb{N}$, $f(x) \equiv 0 \pmod{m}$ 皆有解. 但是事實上 $f(x) = 0$ 並沒有整數解.

再次強調一次, 我們介紹的 congruence 方法僅能拿來證明 Diophantine equation 無解. 所以若有一個 Diophantine equation 你認為它並無整數解, 那你可以考慮用 congruence 的方法去證明它無解. 也就是說試著找到一個 $m \in \mathbb{N}$ 使其在 modulo m 之下無解, 那麼就證得此 Diophantine equation 無整數解. 若你認為一個 Diophantine equation 有解, 那麼 congruence 的方法頂多可以提供你其解的可能形式, 並無法告訴你原 Diophantine equation 有解.

另一種常用的方法稱為 *descent* 的方法. 它也是拿來證明一個 Diophantine equation 沒有正整數解. 其背後的原理是用到正整數的 well-ordering principle. 方法仍然是用反證法: 假設 Diophantine equation $f(x_1, \ldots, x_n) = 0$ 有正整數解且 $x_1 = c_1, \ldots, x_i = c_i, \ldots, x_n = c_n$ 為其一組解. 若我們能利用 $x_1 = c_1, \ldots, x_i = c_i, \ldots, x_n = c_n$ 這一組正整數解找到另一組正整數解 $x_1 = c_1', \ldots, x_i = c_i', \ldots, x_n = c_n'$, 其中對某個特定 $i \in \{1, \ldots, n\}$ 會有 $c_i' < c_i$, 則接下來可利用 $x_1 = c_1', \ldots, x_i = c_i', \ldots, x_n = c_n'$ 這一組正整數解找到另一組正整數解 $x_1 = c_1'', \ldots, x_i = c_i'', \ldots, x_n = c_n''$ 滿足 $c_i'' < c_i'$. 如此一直下去我們可得一個嚴格遞減的無窮正整數數列 $c_i > c_i' > c_i'' > \cdots$ 此和正整數的 well-ordering principle 相違背, 故得證 $f(x_1, \ldots, x_n) = 0$ 沒有整數解.

以後我們會利用 descent 的方法證明某個有名的 Diophantine equation 無正整數解. 底下我們先舉一個簡單的例子讓大家了解 descent 的方法.

Example 7.1.4. 大家都知道 $\sqrt{2}$ 是無理數, 所以我們可知 $x^2 - 2y^2 = 0$ 這個 diophantine equation 無正整數解. 我們利用 descent 的方法來解釋 $x^2 - 2y^2 = 0$ 無正整數解.

假設 $x = c_1, y = d_1$ 是 $x^2 - 2y^2 = 0$ 的一組正整數解. 則由於 $c_1^2 = 2d_1^2$, 我們知 c_1 必為正偶數, 也就是說存在 $c_2 \in \mathbb{N}$ 使得 $c_1 = 2c_2$. 因此得 $4c_2^2 = 2d_1^2$, 即 $2c_2^2 = d_1^2$. 由此又得 d_1 是正偶數, 故存在 $d_2 \in \mathbb{N}$ 使得 $d_1 = 2d_2$. 因此得 $2c_2^2 = 4d_2^2$, 即 $c_2^2 = 2d_2^2$. 也就是說 $x = c_2, y = d_2$ 為 $x^2 - 2y^2 = 0$ 的一組正整數解. 我們利用 $x = c_1, y = d_1$ 這一組正整數解得到 $x = c_2, y = d_2$ 這一組正整數解且滿足 $c_1 > c_2$, 故利用 descent 的方法知 $x^2 - 2y^2 = 0$ 無正整數解.

這裡有一個邏輯上的問題需注意. 所謂 descent 的方法是指一個 Diophantine equation 若能證明「任給一組」正整數解都能產生另一組"較小"的正整數解, 則該 Diophantine equation 無正整數解. 僅由「特定的一組」正整數解可以得到另一組"較小"的正整數解並無法推得矛盾的結論. 例如 $x = 8, y = 6, z = 10$ 是 $x^2 + y^2 = z^2$ 的一組正整數解, 將 x, y, z 皆除以 2 得 $x = 4, y = 3, z = 5$ 也是 $x^2 + y^2 = z^2$ 的一組正整數解, 但此組解並不能再依此推得更小的一組解, 所以無法推得矛盾的結論. 事實上 $x^2 + y^2 = z^2$ 當然是有正整數解, 這並沒有和 descent 的方法相違背.

7.2. Pythagorean Triple 和 Fermat's Last Theorem

我們都知道直角三角形的兩股平方和等於斜邊的平方. 若一個直角三角形其三邊長皆為正整數則此三個正整數就稱為是一組 Pythagorean triple. 換言之, 滿足 Diophantine equation $x^2+y^2=z^2$ 的一組正整數解就是 Pythagorean triple. 我們將找到所有 Pythagorean triples 的形式且利用其來探討和 Fermat's Last Theorem 有關的問題.

7.2.1. Pythagorean Triples. 我們希望能找到所有的 Pythagorean triples. 不過若沒有限制條件要找到所有的解實在有點困難, 更何況有些 Pythagorean triple 其實是從某些 Pythagorean triple 輕易得到的. 因此我們希望找的 Pythagorean triples 雖然有限制條件但希望都能由這些 Pythagorean triples 得到所有可能的 Pythagorean triples. 該多加哪些限制能達到這個目的呢? 例如我們可以僅考慮 $x^2+y^2=z^2$ 的正整數解. 這是因為一來若 $x=0$ 或 $y=0$ 那麼 $x^2=z^2$ 或 $y^2=z^2$ 這樣的 Diophantine equation 根本沒有意思; 再來其他的負整數解都可以輕鬆地由正整數解得到, 所以僅考慮正整數解就足以表達所有的解.

類似的思考方向, 我們也可很輕易的從 $x^2+y^2=z^2$ 的一組正整數解得到無窮多組正整數解. 例如 $x=3,y=4,z=5$ 是一組正整數解, 因此可得對任意 $\lambda\in\mathbb{N}$, $x=3\lambda,y=4\lambda,z=5\lambda$ 也是一組正整數解. 所以我們知有無窮多組 Pythagorean triples. 不過這樣所得的 Pythagorean triple 對我們來說是沒多大興趣的. 我們比較有興趣的是一組 Pythagorean triple "原始"是來自哪個 Pythagorean triple. 也就是我們有興趣於那些最大公因數為 1 的 Pythagorean triple. 事實上任一組 Pythagorean triple 都是來自於某一組最大公因數為 1 的 Pythagorean triple. 這是因為若 $x=a,y=b,z=c$ 是一組 Pythagorean triple 且 $\gcd(a,b,c)=d$, 則存在 $a',b'c'\in\mathbb{N}$ 使得 $a=da',b=db',c=dc'$ 且 $\gcd(a',b',c')=1$. 另一方面由於 $a^2+b^2=c^2$ 可得 $a'^2+b'^2=c'^2$, 所以 $x=a',y=b',z=c'$ 就是一組最大公因數為 1 的 Pythagorean triple. 因此我們只要專注於最大公因數為 1 的 Pythagorean triple 即可.

最後我們發現若 $x=a,y=b,z=c$ 是一組最大公因數為 1 的 Pythagorean triple, 當然 $x=b,y=a,z=c$ 也是一組最大公因數為 1 的 Pythagorean triple, 也就是說藉由交換 x,y 的順序所得的解也沒多大意思. 所以我們想找一個方法僅考慮一組 x,y 的順序即可. 例如我們可僅考慮 $x>y$ 的情形. 不過這樣的限制對我們找解沒有多大的幫助. 我們可以考慮另一種限制. 首先注意最大公因數的限制使得我們的 Pythagorean triple 其 x,y 的值不能同為偶數, 否則由 $z^2=x^2+y^2$ 知 z 必為偶數, 造成 x,y,z 的最大公因數會大於等於 2. 另一方面 x,y 的值也不能同為奇數. 這是因為若 x,y 皆為奇數, 則 $x^2\equiv y^2\equiv 1 \pmod 4$. 因此會造成 $x^2+y^2\equiv 2 \pmod 4$, 然而 x^2+y^2 是偶數, 故由 $z^2=x^2+y^2$ 得 z 為偶數. 也就是說 $z^2\equiv 0 \pmod 4$. 這會造成

$$0\equiv z^2\equiv x^2+y^2\equiv 2 \pmod 4$$

的矛盾. 因此若我們要求的 Pythagorean triple 其最大公因數是 1, 則 x 和 y 必一奇一偶. 所以我們可以考慮限制我們的 Pythagorean triple 其 x 值為奇數而 y 值為偶數. 我們給有這些限制的 Pythagorean triples 一個特別的名字.

Definition 7.2.1. 假設 $a,b,c\in\mathbb{N}$ 滿足 $a^2+b^2=c^2$ 且 $\gcd(a,b,c)=1$ 又 a 為奇數而 b 為偶數, 則稱 a,b,c 為一個 *primitive Pythagorean triple.*

我們希望能找到所有的 primitive Pythagorean triples. 事實上 primitive Pythagorean triples 會有無窮多個, 所以這裡指的找到並不是將所有的 primitive Pythagorean triples 都列出, 我們是要找到一個方法將所有的 primitive Pythagorean triples 表示出來.

Theorem 7.2.2. 給定任一組 *primitive Pythagorean triple* x,y,z 皆存在一組 $m,n\in\mathbb{N}$ 其中 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數使得

$$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2.$$

反之對任意一組 $m,n\in\mathbb{N}$ 滿足 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數, 若令 $x=m^2-n^2$, $y=2mn$ 且 $z=m^2+n^2$, 則 x,y,z 為一組 *primitive Pythagorean triple.*

Proof. 假設 x,y,z 是一組 primitive Pythagorean triple. 由於 $x^2+y^2=z^2$, 我們得 $y^2=(z+x)(z-x)$. 依定義 y 是偶數而 x,z 是奇數, 所以 $y/2$,$(z+x)/2$ 和 $(z-x)/2$ 皆為正整數且 $(y/2)^2=((z+x)/2)((z-x)/2)$. 注意此時 $(z+x)/2$ 和 $(z-x)/2$ 互質. 要不然會有一質數 p 為 $(z+x)/2$ 和 $(z-x)/2$ 的公因數, 因而得 p 為 $(z+x)/2+(z-x)/2=z$ 和 $(z+x)/2-(z-x)/2=x$ 的公因數. 如此會造成 $p|y^2=z^2-x^2$, 即 $p|y$, 因而與 $\gcd(x,y,z)=1$ 相矛盾.

既然 $(z+x)/2$ 和 $(z-x)/2$ 互質, 故由 $(y/2)^2=((z+x)/2)((z-x)/2)$ 可得 $(z+x)/2$ 和 $(z-x)/2$ 皆為某個整數之平方, 亦即存在 $m,n\in\mathbb{N}$ 使得 $m^2=(z+x)/2$ 及 $n^2=(z-x)/2$. 此時我們得

$$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2.$$

至於 m 和 n, 由於 $x>0$, 即 $m^2-n^2>0$, 故知 $m>n$. 又因為 $(z+x)/2$ 和 $(z-x)/2$ 互質, 即 $\gcd(m^2,n^2)=1$, 我們得 $\gcd(m,n)=1$. 最後依定義 $x=m^2-n^2$ 是奇數, 故知 m 和 n 中有一個是奇數一個是偶數.

反之對任意一組 $m,n\in\mathbb{N}$ 滿足 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數, 若令 $x=m^2-n^2$, $y=2mn$ 且 $z=m^2+n^2$, 則自然知 $x,y,z\in\mathbb{N}$ 且 $x^2+y^2=z^2$, 也就是說 x,y,z 是一組 Pythagorean triple. 因此我們僅剩下要說明它們是 primitive, 即 $\gcd(x,y,z)=1$, x 為奇數且 y 為偶數. 依定義 $y=2mn$ 所以 y 當然是偶數, 而 m,n 中一個是奇數一個是偶數所以 $x=m^2-n^2$ 當然是奇數. 至於 $\gcd(x,y,z)=1$ 是因為如果 $\gcd(x,y,z)>1$, 則 $\gcd(x,y,z)$ 必為奇數 (因為已知 x 是奇數) 所以存在一奇質數 p 為 x,y,z 的公因數. 因為 p 整除 $z+x=2m^2$ 且 p 整除 $z-x=2n^2$ 又因為 p 為奇質數, 我們得 $p|m$ 且 $p|n$. 此與 m,n 互質的假設相矛盾, 故知 $\gcd(x,y,z)=1$. □

Theorem 7.2.2 告訴我們每一個 primitive Pythagorean triple 都可由一組一奇一偶且互質的正整數 m,n 得到, 而且每給一組這樣的正整數就可得一組 primitive Pythagorean triple. 雖然我們可以輕易的找到無窮多組這樣的 m,n 但這並不表示可以產生無窮多組

primitive Pythagorean triples, 除非我們知道不同的一組 m,n 可產生不同的 Pythagorean triple. 事實上若 m,n 和 m',n' 是兩組一奇一偶且互質的正整數其中 $m>n$ 且 $m'>n'$, 假設 m,n 和 m',n' 產生一樣的 primitive Pythagorean triple. 亦即 $m^2-n^2=m'^2-n'^2$ 且 $m^2+n^2=m'^2+n'^2$. 將兩式相加可得 $2m^2=2m'^2$, 故由 m,m' 皆為正整數得 $m=m'$. 同理得 $n=n'$. 因此我們有以下之結果.

Corollary 7.2.3. 存在無窮多組 *primitive Pythagorean triple.* 事實上對任意的一組 *primitive Pythagorean triple* 皆存在唯一的一組 $m,n\in\mathbb{N}$ 其中 $m>n$, $\gcd(m,n)=1$ 且 m,n 中有一個是奇數一個是偶數使得 $x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2$.

7.2.2. Fermat's Last Theorem. 我們已找到所有 $x^2+y^2=z^2$ 的正整數解, 很自然的會問 $x^3+y^3=z^3$ 的正整數解, 甚至問對任意大於等於 3 的正整數 n, $x^n+y^n=z^n$ 的正整數解. Fermat 認為當 $n\geq 3$ 時 $x^n+y^n=z^n$ 並無正整數解. 他僅簡短的說有一個很聰明的方法證明此事但並沒有提出證明, 所以我們稱此結果為 Fermat's Last Theorem.

事實上當時應稱 Fermat's Last Theorem 為一個 conjecture (猜想) 因為並沒有人給出完整的證明. 三百多年來許許多多的數學家想要證出此定理, 但一直到 1995 年才被完整的證明. 不過所用的方法牽涉到許多複雜艱深的數學理論, 當然不會是 Fermat 當初所指的方法. 由此我們可以知道 Diophantine equation 雖然僅是討論整數解的問題, 不過有的 Diophantine equation 確實牽涉到很深的數學問題.

其實解 Fermat's Last Theorem 不必考慮所有大於等於 3 的正整數. 若 n 有奇的質因數 p, 此時 $n=pm$, 故若 $x=a,y=b,z=c$ 是 $x^n+y^n=z^n$ 的一組正整數解, 則因 $a^{pm}+b^{pm}=c^{pm}$ 知 $x=a^m,y=b^m,z=c^m$ 是 $x^p+y^p=z^p$ 的一組正整數解. 換言之若能證得 $x^p+y^p=z^p$ 無正整數解, 則對任意 $n=pm$, $x^n+y^n=z^n$ 也無正整數解. 同理若 n 無奇的質因數, 即 $n=2^r$, 此時因 $r\geq 2$ 知 $4|n$, 所以若能證得 $x^4+y^4=z^4$ 無正整數解, 則對任意 $n=2^r>2$, $x^n+y^n=z^n$ 無正整數解. 因此要證明 Fermat's Last Theorem, 我們只要證明對任意奇質數 p, $x^p+y^p=z^p$ 無正整數解, 以及 $x^4+y^4=z^4$ 無正整數解即可. 目前我們無法處理奇質數的情形, 接下來我們將利用 descent 的方法證明 $x^4+y^4=z^4$ 無正整數解.

我們先處理一個比 $x^4+y^4=z^4$ 更一般的 Diophantine equation.

Proposition 7.2.4. $x^4+y^4=z^2$ 無正整數解.

Proof. 我們利用 descent 的方法證明 $x^4+y^4=z^2$ 無正整數解. 假設 $x=a_1,y=b_1,z=c_1$ 是 $x^4+y^4=z^2$ 的一組正整數解, 我們將利用它們得到另一組正整數解 $x=a_2,y=b_2,z=c_2$ 且 $c_1>c_2$. 如此一直下去會和正整數的 well-ordering principle 相違背, 故知原式無正整數解.

現假設 $x=a_1,y=b_1,z=c_1$ 是 $x^4+y^4=z^2$ 的一組正整數解. 如果 $\gcd(a_1,b_1)=d>1$, 由於 $d|a_1$ 且 $d|b_1$ 知 $d^4|a_1^4+b_1^4=c_1^2$, 故得 $d^2|c_1$. 因此 $x=a_1/d,y=b_1/d,z=c_1/d^2$ 是 $x^4+y^4=z^2$ 的一組正整數解且 $c_1/d^2<c_1$.

若 $x=a_1, y=b_1, z=c_1$ 是 $x^4+y^4=z^2$ 的一組正整數解且 $\gcd(a_1,b_1)=1$. 此時由於 $\gcd(a_1^2,b_1^2,c_1)=1$ (因 $\gcd(a_1^2,b_1^2)=1$) 且 $x=a_1^2, y=b_1^2, z=c_1$ 滿足 $x^2+y^2=z^2$. 利用前面討論 primitive Pythagorean triple 的結果, 不失一般性我們假設 a_1^2 是奇數而 b_1^2 是偶數, 亦即 $x=a_1^2, y=b_1^2, z=c_1$ 是一組 primitive Pythagorean triple. 故利用 Theorem 7.2.2 知存在 $m,n\in\mathbb{N}$ 滿足 $m>n$ 且 $\gcd(m,n)=1$ 使得

$$a_1^2=m^2-n^2,\quad b_1^2=2mn,\quad c_1=m^2+n^2.$$

又由於 $\gcd(a_1,m,n)=1$ (因 $\gcd(m,n)=1$), 且 $x=a_1, y=n, z=m$ 滿足 $x^2+y^2=z^2$, 故由 a_1 是奇數之假設以及前面討論 primitive Pythagorean triple 之性質知 n 必為偶數 (且 m 為奇數), 也就是說 $x=a_1, y=n, z=m$ 又是一組 primitive Pythagorean triple. 因此再用一次 Theorem 7.2.2 知存在 $u,v\in\mathbb{N}$ 滿足 $u>v$ 且 $\gcd(u,v)=1$ 使得

$$a_1=u^2-v^2,\quad n=2uv,\quad m=u^2+v^2.$$

這裡要注意, 由於 b_1 和 n 皆為偶數, 我們可假設 $b_1=2b_1'$ 且 $n=2n'$. 此時由 $b_1^2=2mn$ 知 $b_1'^2=mn'$. 又由於 $\gcd(m,n')=1$ 我們知 m 和 n' 皆為某個整數之平方, 亦即存在 $c_2,e\in\mathbb{N}$ 使得 $m=c_2^2$ 且 $n'=e^2$. 又由於 $2e'^2=2n'=n=2uv$ 以及 $\gcd(u,v)=1$, 我們得 u 和 v 皆為某個整數之平方, 亦即存在 $a_2,b_2\in\mathbb{N}$ 使得 $u=a_2^2$ 且 $v=b_2^2$. 因此由 $m=u^2+v^2$ 即 $c_2^2=(a_2^2)^2+(b_2^2)^2$ 知 $x=a_2, y=b_2, z=c_2$ 是 $x^4+y^4=z^2$ 的一組正整數解. 此時因 $c_1=m^2+n^2>m^2>c_2^4$, 知 $x=a_2, y=b_2, z=c_2$ 確實是另一組 $x^4+y^4=z^2$ 的正整數解且滿足 $c_2<c_1$. 故利用 descent 的方法得證本定理. □

Proposition 7.2.4 告訴我們 $x^4+y^4=z^2$ 無正整數解, 我們可以輕鬆的利用這個結果證明 $x^4+y^4=z^4$ 無正整數解. 這是因為若 $x=a, y=b, z=c$ 是 $x^4+y^4=z^4$ 的一組正整數解, 則 $x=a, y=b, z=c^2$ 就會是 $x^4+y^4=z^2$ 的一組正整數解. 此和 Proposition 7.2.4 相矛盾, 故有以下之結論.

Corollary 7.2.5. $x^4+y^4=z^4$ 無正整數解.

7.3. 平方和問題

在此最後一節中我們要探討整數論另一個有趣的問題, 就是將正整數寫成一些整數的平方和問題. 我們將完整的回答哪些正整數可以寫成兩個整數的平方和, 而且證明所有的正整數都可以寫成四個整數的平方和.

7.3.1. Sum of Two Squares. 當一個正整數不是某個整數的平方時, 我們有興趣知道它是否可寫成兩個整數的平方和. 若 n 本身是某個整數的平方, 即存在 $m\in\mathbb{N}$ 使得 $n=m^2$, 當然我們可以將 n 寫成 $n=m^2+0^2$. 所以我們可以將可寫成兩個整數的平方和的數視為平方數的推廣.

首先我們來看一個有趣的等式:

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2. \tag{7.1}$$

這個等式可以直接將等號兩邊展開來求證, 也可以用大家熟悉的複數運算來說明. 假設 $z_1 = a + b\mathbf{i}, z_2 = d + c\mathbf{i} \in \mathbb{C}$ (這裡 $\mathbb{C}$ 表示複數所成之集合, 而 $\mathbf{i} \in \mathbb{C}$ 滿足 $\mathbf{i}^2 = -1$). 我們知 z_1, z_1 的共軛複數分別為 $\overline{z_1} = a - b\mathbf{i}, \overline{z_2} = d - c\mathbf{i}$ 且 $|z_1|^2 = z_1\overline{z_1} = a^2 + b^2$ 及 $|z_2|^2 = z_2\overline{z_2} = c^2 + d^2$. 因此

$$(a^2+b^2)(c^2+d^2) = z_1\overline{z_1}z_2\overline{z_2} = z_1z_2\overline{z_1z_2} = |(ad-bc)+(ac+bd)\mathbf{i}|^2 = (ac+bd)^2+(ad-bc)^2.$$

利用式子 (7.1) 我們馬上有以下之結果.

Lemma 7.3.1. *若 $m, n \in \mathbb{N}$ 皆可以寫成兩個整數的平方和, 則 mn 亦可以寫成兩個整數的平方和.*

Proof. *若 $m = a^2 + b^2$ 且 $n = c^2 + d^2$, 其中 $a, b, c, d \in \mathbb{Z}$, 則利用式子 (7.1) 知 $mn = (ac+bd)^2 + (ad-bc)^2$. 因 $ac+bd, ad-bc \in \mathbb{Z}$ 故知 mn 亦可以寫成兩個整數的平方和.* □

注意 Lemma 7.3.1 僅告訴我們當 m, n 皆可以寫成兩個整數的平方和時, mn 也可以寫成兩個整數的平方和; 它並沒有告訴我們若 m, n 中有一個不能寫成兩個整數的平方和時, mn 是否可以寫成兩個整數的平方和.

由於每個大於 1 的整數都可以寫成質因數的乘積, 所以由 Lemma 7.3.1 我們很自然的要探討哪些質數可以寫成兩個整數的平方和哪些質數不能. 由於 $2 = 1^2 + 1^2$, 即 2 可以寫成兩個整數的平方和, 因此以下我們僅考慮奇質數的情形. 利用 Lemma 7.3.1 我們可以得到一個判別一個質數是否可以寫成兩個整數的平方和的方法.

Lemma 7.3.2. *假設 p 是一個質數. 若存在 $a, b \in \mathbb{Z}$ 使得 $a^2 + b^2 = \lambda p$, 其中 $\lambda \in \mathbb{N}$ 滿足 $\lambda < p$, 則 p 可以寫成兩個整數的平方和.*

Proof. *考慮集合 $S = \{s \in \mathbb{N} \mid$ 存在 $u, v \in \mathbb{Z}$ 使得 $u^2 + v^2 = sp\}$. 依照 S 的定義, 要證明 p 可以寫成兩個整數的平方和就等同於要證明 $1 \in S$. 要如何知 $1 \in S$ 呢? 依假設知 S 為非空集合 (因 $\lambda \in S$) 且 S 的元素皆為正整數, 所以 $1 \in S$ 若且唯若 S 中最小的元素就是 1 (注意依正整數的 well-ordering principle, 由於 S 不是空集合所以 S 中必存在最小的元素). 令 $m \in S$ 是 S 中最小的元素, 我們要證明 $m = 1$.*

利用反證法, 假設 $m \neq 1$. 故由 $\lambda \in S$ 且 $\lambda < p$ 知 $1 < m < p$. 我們希望在 S 中找到比 m 更小的數而得到矛盾. 由於 $m \in S$, 故存在 $u, v \in \mathbb{Z}$ 使得 $u^2 + v^2 = mp$, 我們分成 m 是偶數及 m 是奇數兩種情況討論.

(I) m 是偶數: 此時由於 $u^2 + v^2 = mp$ 是偶數, 我們知 u, v 必同奇同偶 (否則 $u^2 + v^2$ 不會是偶數), 即 $u + v$ 和 $u - v$ 皆為偶數. 此時 $(u + v)/2$ 和 $(u - v)/2$ 皆為整數且

$$(\frac{u+v}{2})^2 + (\frac{u-v}{2})^2 = \frac{u^2}{2} + \frac{v^2}{2} = \frac{m}{2}p.$$

故知 $m/2 \in S$ 且 $m/2 < m$, 此與 m 是 S 中最小的元素相矛盾.

(II) m 是奇數: 因為當 m 是奇數時

$$\{\frac{-m+1}{2}, \frac{-m+1}{2}+1, \ldots, 0, 1, \ldots, \frac{m-1}{2}-1, \frac{m-1}{2}\}$$

是一個 complete residue system modulo m. 我們可找到 $c, d \in \mathbb{Z}$ 滿足 $c \equiv u \pmod{m}$ 且 $d \equiv v \pmod{m}$, 其中 $-(m-1)/2 \leq c, d \leq (m-1)/2$. 注意這裡 c 和 d 不能同時等於 0, 這是因為如果 $c = d = 0$ 表示 $u \equiv v \equiv 0 \pmod{m}$, 即 $m|u$ 且 $m|v$. 因此 $m^2|u^2 + v^2 = mp$, 即 $m|p$. 如此會和 $1 < m < p$ 相矛盾, 故知 c 和 d 不同時為 0. 因為 $c^2 + d^2 \equiv u^2 + v^2 \pmod{m}$ 以及 $u^2 + v^2 = mp$, 我們得 $c^2 + d^2 \equiv 0 \pmod{m}$. 亦即存在 $k \in \mathbb{Z}$ 使得 $c^2 + d^2 = km$. 注意因 c 和 d 不同時為 0, 故 $k \neq 0$. 另一方面因為 $-(m-1)/2 \leq c, d \leq (m-1)/2$, 所以 $c^2 + d^2 \leq (m-1)^2/4 + (m-1)^2/4 = (m-1)^2/2 < m^2$, 故得 $0 < k < m$. 也就是說 $k \in \mathbb{N}$ 且 $k < m$. 現在我們有兩個等式: $u^2 + v^2 = mp$ 以及 $c^2 + d^2 = km$. 利用式子 (7.1) 得

$$(uc + vd)^2 + (ud - vc)^2 = m^2 kp.$$

又因為 $u \equiv c \pmod{m}$ 且 $v \equiv d \pmod{m}$, 我們得

$$uc + vd \equiv u^2 + v^2 \equiv 0 \pmod{m} \quad \text{and} \quad ud - vc \equiv uv - uv \equiv 0 \pmod{m}.$$

也就是說 $(uc + vd)/m \in \mathbb{Z}$ 且 $(ud - vc)/m \in \mathbb{Z}$. 因此知

$$(\frac{uc + vd}{m})^2 + (\frac{ud - vc}{m})^2 = kp,$$

也就是說 kp 可以寫成兩個整數的平方和, 故又由 $k \in \mathbb{N}$ 知 $k \in S$. 然而我們又知 $k < m$, 此與 m 是 S 中最小的元素相矛盾.

我們證得若 $m \neq 1$ 會造成 m 不是偶數且不是奇數這樣的矛盾. 故由反證法知原假設 $m \neq 1$ 不成立, 也就是說 $m = 1$. 因此得證 p 可以寫成兩個整數的平方和. □

Lemma 7.3.2 的證明方法其實是類似於 descent 的方法都是由一個解得到更小的解而推得矛盾. 或許大家會疑惑為何同樣的推論方法, 一個會得到無解; 另一個卻推得有解. 這是因為在 descent 的方法推論中是沒有任何條件的, 所以若有正整數解則會沒有限制的推得無窮多個更小的正整數解而造成矛盾, 因此會得到無解的結論. 而這裡所用的方法中會得到比 m 更小的正整數是有條件的, 也就是說必須在 $m > 1$ 的情形才可以. 因此同樣推得矛盾, 但此時矛盾會讓我們推得 $m = 1$, 所以有解. 希望這兩者邏輯上的差異, 大家都能了解. 另外 Lemma 7.3.2 證得存在的方法表面上好像只是邏輯推演, 並沒有告訴我們如何找到解. 事實上其解法過程中包含了找到解的方法. 我們來看一個具體的例子.

Example 7.3.3. 考慮 $p = 89$. 由於 $89 \equiv 1 \pmod{4}$, 我們知存在 $a \in \mathbb{Z}$ 使得 $a^2 \equiv -1 \pmod{89}$. 事實上當 $a = 34$ 時, $a^2 = 1156 \equiv -1 \pmod{89}$, 我們有 $(34)^2 + 1 = 13 \times 89$. 因為 $13 < 89$ 故由 Lemma 7.3.2 知 89 可以寫成兩個整數的平方和. 我們要利用 Lemma 7.3.2 的證明方法將 89 寫成兩個整數的平方和.

對應到 Lemma 7.3.2 的證明, 我們知 $13 \in S$. 因 $13 \neq 1$, 我們要利用 13, 在 S 中找到更小的元素. 我們要找到 c, d 滿足 $34 \equiv c \pmod{13}$, $1 \equiv d \pmod{13}$ 以及 $-6 \leq c, d \leq 6$. 很容易得知 $c = -5$ 且 $d = 1$. 接著我們考慮 $c^2 + d^2 = 25 + 1 = 26 = 2 \times 13$. 故由式子 (7.1) 得

$$(34 \times (-5) + 1)^2 + (34 - (-5))^2 = 169^2 + 39^2 = 2 \times 13^2 \times 89.$$

由於 $169 = 13 \times 13$ 且 $39 = 3 \times 13$, 我們得 $13^2 + 3^2 = 2 \times 89$, 也就是說 $2 \in S$. 注意到我們已將 $13 \in S$ 降到 $2 \in S$. 再利用處理偶數情況的方法, 將 2 縮小. 即得

$$(\frac{13+3}{2})^2 + (\frac{13-3}{2})^2 = 8^2 + 5^2 = 89.$$

在 Example 7.3.3 中我們利用 $89 \equiv 1 \pmod 4$ 所以可以找到 $a \in \mathbb{Z}$ 滿足 $a^2 \equiv -1 \pmod{89}$. 再適當的選取 a (即選取 a 夠小) 使得 $a^1 + 1 = \lambda p$, 其中 $0 < \lambda < p$, 以便套用 Lemma 7.3.2. 在一般的情形, 當 p 是一質數滿足 $p \equiv 1 \pmod 4$ 時, 我們都可以如此作. 所以我們有以下之結果.

Proposition 7.3.4. *若 p 是一質數且 $p \equiv 1 \pmod 4$, 則 p 可以寫成兩個整數的平方和.*

Proof. 由於 $p \equiv 1 \pmod 4$, Theorem 5.4.1 告訴我們 $x^2 \equiv -1 \pmod p$ 有解. 亦即存在 $a \in \mathbb{N}$ 使得 $a^2 \equiv -1 \pmod p$. 由於 $\{1, 2, \ldots, p-1\}$ 是一個 reduced residue system modulo p, 所以我們可以選取 $1 \leq a \leq p-1$ 使得 $a^2 \equiv -1 \pmod p$ (事實上可選取 $1 < a < p/2$). 因此存在 $\lambda \in \mathbb{N}$ 使得 $a^2 + 1 = \lambda p$. 又因為 $a \leq p-1$, 我們有 $\lambda p = a^2 + 1 \leq (p-1)^2 + 1 = p^2 - 2(p-1) < p^2$. 也就是說 $\lambda < p$, 故利用 Lemma 7.3.2 得證 p 可以寫成兩個整數的平方和. □

接下來我們看怎樣的質數不能寫成兩個整數的平方和. 當 $p \equiv 1 \pmod 4$ 時, 在 Proposition 7.3.4 我們是利用此時 $x^2 \equiv -1 \pmod p$ 有解證得 p 可以寫成兩個整數的平方和. 我們也可以利用當 $p \equiv 3 \pmod 4$ 時, $x^2 \equiv -1 \pmod p$ 無解證得 p 不可以寫成兩個整數的平方和.

Lemma 7.3.5. *假設 p 是一個質數滿足 $p \equiv 3 \pmod 4$ 且 $n \in \mathbb{N}$ 滿足 $p|n$. 若 $a, b \in \mathbb{Z}$ 使得 $a^2 + b^2 = n$, 則 $p|a$ 且 $p|b$.*

Proof. 我們要用反證法證明此定理. 不失一般性, 我們假設 $p \nmid a$. 此時由 $a^2 + b^2 = n$ 且 $p|n$ 知 $p \nmid b$, 否則由 $a^2 = n - b^2$ 得 $p|a^2$ 會造成與 $p \nmid a$ 的假設相矛盾. 既然 $a^2 + b^2 = n$ 且 $p|n$, 我們得 $a^2 \equiv -b^2 \pmod p$. 注意由於 a, b 皆與 p 互質, 我們可以用 Legendre symbol 處理問題. 利用 Legendre symbol 的性質 (Lemma 5.3.2) 知

$$1 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right).$$

然而由 $p \equiv 3 \pmod 4$ 以及 Theorem 5.4.1 我們知 $\left(\frac{-1}{p}\right) = -1$. 由此矛盾知 $p|a$, 並由 $b^2 = n - a^2$ 得 $p|b$. □

Lemma 7.3.5 證明的想法類似於 Proposition 7.1.1 所提的方法, 即利用探討 $x^2 + y^2 = n$ 這個 Diophantine equation 在 modulo p 的情形來推得此 Diophantine equation 無解. 利用 Lemma 7.3.5 我們馬上得到以下之結果.

Proposition 7.3.6. *若 p 是一質數且 $p \equiv 3 \pmod 4$, 則 p 不能寫成兩個整數的平方和.*

Proof. 我們用反證法. 假設存在 $a,b\in\mathbb{Z}$ 使得 $a^2+b^2=p$. 由於 p 是質數, 我們知 a,b 皆不等於 0. 故知可取 $a,b\in\mathbb{N}$ 滿足 $1\le a\le p-1$ 且 $1\le b\le p-1$. 此時 a,b 皆與 p 互質故與 Lemma 7.3.5 的結果相矛盾. 由此矛盾知 p 不能寫成兩個整數的平方和. □

知道了哪些質數可以寫成兩個整數的平方和, 哪些質數不可以寫成兩個整數的平方和. 接下來我們就來探討哪些正整數可以寫成兩個整數的平方和. 給定一正整數 n. 若 $n=1$ 當然可寫成兩個整數的平方和. 若 $n\ge 2$, 首先我們將 n 作質因數的分解. 我們可以將 2 和除以 4 餘 1 的質因數忽略, 因為它們可以寫成兩個整數的平方和. 而若 n 有除以 4 餘 3 的質因數, 我們又可以將有平方的部份忽略, 因為它們也可以寫成兩個整數的平方和. 由此看出質因數分解後的次數是重要的, 我們特別用以下名詞的定義: 若 $n=p_1^{n_1}\cdots p_r^{n_r}$, 其中這些 p_i 是相異質數. 我們稱 p_i 是 n 的質因數且 n_i 是 p_i 的次數. 例如 $2250=2\times 3^2\times 5^3$, 我們稱 2250 有 2 次 3 的質因數且有 3 次 5 的質因數. 依此定義我們有以下之結果.

Theorem 7.3.7. 假設 $n\in\mathbb{N}$. 則 n 可以寫成兩個整數的平方和若且唯若 n 沒有任何的除以 4 餘 3 的質因數其次數是奇數.

Proof. 假設 n 沒有任何的除以 4 餘 3 的質因數其次數是奇數. 我們僅需考慮 $n\ge 2$ 的情形. 此時可將 n 質因數分解成

$$n=2^{n_0}q_1^{n_1}\cdots q_r^{n_r}\cdot p_1^{2m_1}\cdots p_s^{2m_s},$$

其中 q_i,p_j 皆為相異的奇質數且 $q_i\equiv 1\pmod 4$ 及 $p_j\equiv 3\pmod 4$. 由於我們可將 n 寫成

$$n=2^{n_0}q_1^{n_1}\cdots q_r^{n_r}\cdot(p_1^{m_1}\cdots p_s^{m_s})^2,$$

而 2 可以寫成兩個整數的平方和, $q_1,\ldots,q_r$ 可以寫成兩個整數的平方和 (Proposition 7.3.4) 以及 $(p_1^{m_1}\cdots p_s^{m_s})^2$ 可以寫成兩個整數的平方和 (因為是一個平方數), 故由 Lemma 7.3.1 知 n 可以寫成兩個整數的平方和.

反之, 若 $p\equiv 3\pmod 4$ 是 n 的一個質因數且其次數為 $2k+1$, 即 $n=p^{2k+1}n'$, 其中 $p\nmid n'$. 我們用反證法證明 n 不可以寫成兩個整數的平方和. 假設存在 $a,b\in\mathbb{Z}$ 使得 $a^2+b^2=n$. 則由 Lemma 7.3.5 知 $p|a$ 且 $p|b$. 令 $a=p^rc$ 且 $b=p^sd$, 其中 c,d 皆與 p 互質且 $r,s\in\mathbb{N}$. 不失一般性我們假設 $2r\le 2s$, 我們要證明 $2k+1>2r$. 假設 $2k+1<2r$, 由 $p^{2r}c^2+p^{2s}d^2=p^{2k+1}n'$ 知 $n'=p^{2r-2k-1}c^2+p^{2s-2k-1}d^2$. 又因為 $2s-2k-1\ge 2r-2k-1>0$ 知 $p|n'$. 此與 $p\nmid n'$ 相矛盾, 故知 $2k+1>2r$. 再由 $p^{2r}c^2+p^{2s}d^2=p^{2k+1}n'$ 知

$$c^2+p^{2s-2r}d^2=c^2+(p^{s-r}d)^2=p^{2k+1-2r}n',$$

即 $p^{2k+1-2r}n'$ 可以寫成 c 和 $p^{s-r}d$ 的平方和. 由於 $p\equiv 3\pmod 4$, $p|p^{2k+1-2r}n'$ 且 $p\nmid c$, 此與 Lemma 7.3.5 的結果相矛盾, 故知 n 不可以寫成兩個整數的平方和. □

例如 $2250=2\times 3^2\times 5^3$ 中唯一的除以 4 餘 3 的質因數是 3, 且 3 的次數為 2 是偶數, 所以 2250 可以寫成兩個整數的平方和. 事實上 $2250=45^2+15^2$. 另外 $6174=2\times 3^2\times 7^3$ 中除以 4 餘 3 的質因數是 3 和 7, 其中 7 的次數為 3 是奇數, 所以 6174 無法寫成兩個整數的平方和.

7.3.2. Sum of Four Squares. 我們已知並不是所有的正整數都可以寫成兩個整數的平方和, 所以很自然會問是否所有的正整數都可以寫成三個整數的平方和. 這其實仍不對, 例如 7 就不能寫成三個整數的平方和. 事實上我們可以證得一個正整數不能寫成三個整數的平方和若且唯若此正整數可表成 $4^m(8n+3)$ 這樣的形式. 不過這裡因為三個整數的平方和沒有如 Lemma 7.3.1 的性質, 所以此事實之證明會比處理兩個整數的平方和複雜的多. 由於在此我們著重於讓大家學習如何將已知的方法推廣, 我們將避談三個整數平方和的問題, 而直接談論四個整數的平方和問題.

我們要推廣處理兩個整數的平方和的方法來處理四個整數的平方和問題. 首先我們有一個和式子 (7.1) 相對應的式子.

$$\begin{aligned}(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) &= (ae+bf+cg+dh)^2+(af-be+ch-dg)^2 \\ &\quad +(ag-bh-ce+df)^2+(ah+bg-cf-de)^2.\end{aligned} \tag{7.2}$$

這個等式可以直接將等號兩邊展開來求證. 或許大家會好奇這個等式是如何得到的, 事實上這個等式可以利用複數的推廣即所謂的 quaternion algebra 來說明. 不過由於 quaternion algebra 已偏離我們的主題太遠, 我們就不再多說明了.

利用式子 (7.2) 我們馬上有以下之結果.

Lemma 7.3.8. 若 $m,n\in\mathbb{N}$ 皆可以寫成四個整數的平方和, 則 mn 亦可以寫成四個整數的平方和.

由於每個大於 1 的整數都可以寫成質因數的乘積, 所以由 Lemma 7.3.8 我們很自然的要探討哪些質數可以寫成四個整數的平方和. 由於 2 和除以 4 餘 1 的質數皆可寫成兩個整數的平方和, 所以它們皆可寫成四個整數的平方和 (多餘的兩個補 0), 因此我們僅剩下要討論除以 4 餘 3 的質數. 我們可以推廣 Lemma 7.3.2 的方法得到一個判別一個質數是否可以寫成四個整數的平方和的方法.

Lemma 7.3.9. 假設 p 是一個質數. 若存在 $a,b,c,d\in\mathbb{Z}$ 使得 $a^2+b^2+c^2+d^2=\lambda p$, 其中 $\lambda\in\mathbb{N}$ 滿足 $\lambda<p$, 則 p 可以寫成四個整數的平方和.

Proof. 考慮集合 $S=\{s\in\mathbb{N}\mid$ 存在 $t,u,v,w\in\mathbb{Z}$ 使得 $t^2+u^2+v^2+w^2=sp\}$. 依照 S 的定義, 要證明 p 可以寫成四個整數的平方和就等同於要證明 $1\in S$. 要如何知 $1\in S$ 呢? 依假設知 S 為非空集合 (因 $\lambda\in S$) 且 S 的元素皆為正整數, 所以 $1\in S$ 若且唯若 S 中最小的元素就是 1. 令 $m\in S$ 是 S 中最小的元素, 我們要證明 $m=1$.

利用反證法, 假設 $m\neq 1$. 故由 $\lambda\in S$ 且 $\lambda<p$ 知 $1<m<p$. 我們希望在 S 中找到比 m 更小的數而得到矛盾. 由於 $m\in S$, 故存在 $t,u,v,w\in\mathbb{Z}$ 使得 $t^2+u^2+v^2+w^2=mp$, 我們分成 m 是偶數及 m 是奇數兩種情況討論.

(I) m 是偶數: 此時由於 $t^2+u^2+v^2+w^2=mp$ 是偶數, 我們知 t,u,v,w 必皆為奇數; 皆為偶數偶; 或是其中兩個是奇數兩個是偶數. 在所有的情況之下我們都可以將 t,u,v,w

分成同奇同偶的兩對. 不失一般性, 我們假設 t,u 同奇同偶且 v,w 同奇同偶, 即 $t+u$, $t-u$, $v+w$ 和 $v-w$ 皆為偶數. 此時 $(t+u)/2$, $(t-u)/2$, $(v+w)/2$ 和 $(v-w)/2$ 皆為整數且

$$(\frac{t+u}{2})^2+(\frac{t-u}{2})^2+(\frac{v+w}{2})^2+(\frac{v-w}{2})^2=\frac{m}{2}p.$$

故知 $m/2\in S$ 且 $m/2<m$, 此與 m 是 S 中最小的元素相矛盾.

(II) m 是奇數: 因為當 m 是奇數時

$$\{\frac{-m+1}{2},\frac{-m+1}{2}+1,\ldots,0,1,\ldots,\frac{m-1}{2}-1,\frac{m-1}{2}\}$$

是一個 complete residue system modulo m. 我們可找到 $e,f,g,h\in\mathbb{Z}$ 滿足 $e\equiv t \pmod m$, $f\equiv u \pmod m$, $g\equiv v \pmod m$ 且 $h\equiv w \pmod m$, 其中 $-(m-1)/2\le e,f,g,h\le (m-1)/2$. 注意這裡 e, f, g 和 h 不能同時等於 0, 否則會得 $m|p$ 而和 $1<m<p$ 相矛盾. 因為 $e^2+f^2+g^2+h^2\equiv t^2+u^2+v^2+w^2 \pmod m$ 以及 $t^2+u^2+v^2+w^2=mp$, 我們得 $e^2+f^2+g^2+h^2\equiv 0 \pmod m$. 亦即存在 $k\in\mathbb{Z}$ 使得 $e^2+f^2+g^2+h^2=km$. 注意因 e, f, g 和 h 不同時為 0, 故 $k\neq 0$. 另一方面因為 $-(m-1)/2\le e,f,g,h\le (m-1)/2$, 所以 $e^2+f^2+g^2+h^2\le (m-1)^2=(m-1)^2<m^2$, 故得 $0<k<m$. 也就是說 $k\in\mathbb{N}$ 且 $k<m$. 現在我們有兩個等式: $t^2+u^2+v^2+w^2=mp$ 以及 $e^2+f^2+g^2+h^2=km$. 利用式子 (7.2) 得

$$(te+uf+vg+wh)^2+(tf-ue+vh-wg)^2+(tg-uh-ve+wf)^2+(th+ug-vf-we)^2=m^2kp.$$

又因為 $e\equiv t \pmod m$, $f\equiv u \pmod m$, $g\equiv v \pmod m$ 且 $h\equiv w \pmod m$, 我們得

$$te+uf+vg+wh\equiv tf-ue+vh-wg\equiv tg-uh-ve+wf\equiv th+ug-vf-we\equiv 0 \pmod m.$$

也就是說若令

$$T=\frac{te+uf+vg+wh}{m},\ U=\frac{tf-ue+vh-wg}{m},$$
$$V=\frac{tg-uh-ve+wf}{m} \quad\text{and}\quad W=\frac{th+ug-vf-we}{m},$$

則 $T,U,V,W\in\mathbb{Z}$ 且

$$T^2+U^2+V^2+W^2=kp.$$

也就是說 kp 可以寫成四個整數的平方和, 故又由 $k\in\mathbb{N}$ 知 $k\in S$. 然而我們又知 $k<m$, 此與 m 是 S 中最小的元素相矛盾.

我們證得若 $m\neq 1$ 會造成 m 不是偶數且不是奇數的矛盾. 故由反證法知原假設 $m\neq 1$ 不成立, 也就是說 $m=1$. 故得證 p 可以寫成四個整數的平方和. □

接下來我們將利用 Lemma 7.3.9 來證明所有的正整數皆可寫成四個整數的平方和. 我們僅剩下要說明除以 4 餘 3 的質數可以寫成四個整數的平方和. 由於此時 $x^2\equiv -1 \pmod p$ 無解, 我們要利用此特性找出一個 $\alpha\in\mathbb{N}$ 使得 $x^2\equiv -\alpha \pmod p$ 有解. 由於此時 $\left(\frac{-\alpha}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{\alpha}{p}\right)=-\left(\frac{\alpha}{p}\right)$, 得 $\left(\frac{-\alpha}{p}\right)=1$ 若且唯若 $\left(\frac{\alpha}{p}\right)=-1$. 所以我們必須找到 $\alpha\in\mathbb{N}$ 使得 $x^2\equiv \alpha \pmod p$ 無解. 這是可以辦到的, 因為 $S=\{1,2,\ldots,p-1\}$ 是 modulo p 的 reduced residue system, 若 $p\nmid a$, 則 $x^2\equiv a \pmod p$ 的解必和 S 中的某個元素在 modulo p 之下同餘. 也就是說 $x^2\equiv a \pmod p$ 有解若且唯若存在 $c\in S$ 使得 $c^2\equiv a$

$(\mathrm{mod}\ p)$. 所以我們只要將 S 中的每一個元素平方, 若 a 和平方後的某個數在 modulo p 之下同餘則 $x^2 \equiv a\ (\mathrm{mod}\ p)$ 有解; 反之, 若 a 和平方後每個數在 modulo p 之下皆不同餘則 $x^2 \equiv a\ (\mathrm{mod}\ p)$ 無解. 然而若 $c \in S$ 則 $p-c \in S$ 且 $(p-c)^2 \equiv (-c)^2 \equiv c\ (\mathrm{mod}\ p)$, 又因為 p 是奇質數, 所以 $c \not\equiv p-c\ (\mathrm{mod}\ p)$. 也就是說 S 中的元素平方後在 modulo p 之下僅有 $(p-1)/2$ 個不同餘類. 因此我們知道 S 中共有 $(p-1)/2$ 個元素 a 會使得 $x^2 \equiv a\ (\mathrm{mod}\ p)$ 有解, 且有 $(p-1)/2$ 個元素 a 會使得 $x^2 \equiv a\ (\mathrm{mod}\ p)$ 無解.

Theorem 7.3.10. 若 p 是一質數且 $p \equiv 3\ (\mathrm{mod}\ 4)$, 則 p 可以寫成四個整數的平方和. 特別地, 所有的正整數皆可以寫成四個整數的平方和.

Proof. 假設 p 是一質數且 $p \equiv 3\ (\mathrm{mod}\ 4)$. 我們要找到 $a, b, c, d \in \mathbb{Z}$ 使得 $a^2+b^2+c^2+d^2 = \lambda p$, 其中 $\lambda \in \mathbb{N}$ 且 $\lambda < p$, 再利用 Lemma 7.3.9 證得 p 可以寫成四個整數的平方和.

現考慮 $S = \{1, 2, \ldots, p-1\}$ 這一個 modulo p 的 reduced residue system. 令 $\alpha \in S$ 是 S 中最小的數使得 $x^2 \equiv \alpha\ (\mathrm{mod}\ p)$ 無解, 也就是說 $\left(\frac{\alpha}{p}\right) = -1$. 由於 $\left(\frac{1}{p}\right) = 1$, 我們知 $\alpha > 1$, 因此 $\alpha - 1 \in S$, 且 $x^2 \equiv \alpha - 1\ (\mathrm{mod}\ p)$ 有解 (因 α 是 S 中最小的數使得 $x^2 \equiv \alpha\ (\mathrm{mod}\ p)$ 無解). 另一方面 $p \equiv 3\ (\mathrm{mod}\ 4)$, 所以 $\left(\frac{-1}{p}\right) = -1$, 故得 $\left(\frac{-\alpha}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\alpha}{p}\right) = 1$, 也就是說 $x^2 \equiv -\alpha\ (\mathrm{mod}\ p)$ 有解. 現令 $a \in S$ 是 $x^2 \equiv \alpha - 1$ 之一解, 我們可選 a 使得 $1 \le a \le (p-1)/2$. 這是因為若 $(p+1)/2 \le a \le p-1$, 則考慮 $p-a$, 此時 $(p-a)^2 \equiv (-a)^2 \equiv \alpha - 1\ (\mathrm{mod}\ p)$ 仍為 $x^2 \equiv \alpha - 1\ (\mathrm{mod}\ p)$ 之一解且 $1 \le p-a < (p-1)/2$. 同理我們也可找到 $b \in S$ 是 $x^2 \equiv -\alpha\ (\mathrm{mod}\ p)$ 之一解且 $1 \le b \le (p-1)/2$. 現由於

$$a^2 + b^2 + 1 \equiv \alpha - 1 + (-\alpha) + 1 \equiv 0 \pmod{p},$$

故存在 $\lambda \in \mathbb{N}$ 使得 $a^2 + b^2 + 1 = \lambda p$. 又由於

$$\lambda p = a^2 + b^2 + 1 \le (\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1 < \frac{p^2}{2} + 1 < p^2,$$

所以我們有 $\lambda < p$. 故利用 Lemma 7.3.9 得證 p 可以寫成四個整數的平方和.

現任取 $n \in \mathbb{N}$. 若 $n = 1$, 則 n 當然寫成四個整數的平方和. 若 $n > 1$, 則可將 n 寫成質因數之乘積 $n = p_1^{n_1} \cdots p_r^{n_r}$. 若 $p_i = 2$ 或 $p_i \equiv 1\ (\mathrm{mod}\ 4)$ 則 p_i 可以寫成兩個整數的平方和, 故可以寫成四個整數的平方和. 若 $p_i \equiv 3\ (\mathrm{mod}\ 4)$, 則由前知 p_i 也可以寫成四個整數的平方和. 故利用 Lemma 7.3.8 知 $n = p_1^{n_1} \cdots p_r^{n_r}$ 可以寫成四個整數的平方和. □

我們已介紹了一些基礎數論應有的基本知識, 本講義就此結束.