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 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 $0\le r<m$. 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 $0\le r_1,r_2<m$, 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 $0\le r_1,r_2<m$, 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.

Question 3.1. 給定 $m \in \mathbb{N}$.

(1) 假設 $S \subseteq \mathbb{Z}$ 且 S 的元素個數為 m. 若已知對任意 $a \in \mathbb{Z}$ 皆存在 $s \in S$ 滿足 $a \equiv s \pmod{m}$. 試證明 S 為 *complete residue system modulo m*.

(2) 假設 $S \subseteq \mathbb{Z}$ 試證明 S 為 *complete residue system modulo m* 若且唯若對任意 $a \in \mathbb{Z}$ 皆存在唯一的 $s \in S$ 滿足 $a \equiv s \pmod{m}$.

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.

Question 3.2. 給定 $m \in \mathbb{N}$.

(1) 假設 $S \subseteq \mathbb{Z}$ 且 S 的元素個數為 $\phi(m)$. 若已知對任意滿足 $\gcd(a,m) = 1$ 的整數 a, 皆存在 $s \in S$ 滿足 $a \equiv s \pmod{m}$. 試證明 S 為 *reduced residue system modulo m*.

(2) 假設 $S \subseteq \mathbb{Z}$ 試證明 S 為 *reduced residue system modulo m* 若且唯若 S 中的元素皆與 m 互質且對任意滿足 $\gcd(a,m) = 1$ 的整數 a, 皆存在唯一的 $s \in S$ 滿足 $a \equiv s \pmod{m}$.

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 的這一類相加或相乘. 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 $a \neq 0 \pmod 6$ 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 1.1.8 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 1.2.6(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 1.2.4 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 $\{r_1, \ldots, r_{\phi(m)}\}$ 是一個 *reduced residue system modulo m*, 則 $\{ar_1, \ldots, ar_{\phi(m)}\}$ 也是一個 *reduced residue system modulo m*.

Proof. 複習一下, $\{r_1, \ldots, r_{\phi(m)}\}$ 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 $\{ar_1, \ldots, ar_{\phi(m)}\}$ 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 $S = \{a_1, \ldots, a_{\phi(m)}\}$ 和 $T = \{b_1, \ldots, b_{\phi(m)}\}$ 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 $2 \le i \le p-2$, 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.