單元 2 同餘 (Congruences)

2.1 同餘的概念

在上一單元，我們曾詳細討論過有關整除性的問題。在這一單元，我們將介紹另一能更有效處理整除性的工具，這就是由數學家高斯 (Carl Friedrich Gauss, 1777 – 1855) 所建構的「同餘」 (congruences)了。

定義 2.1.1
設 $a, b \in \mathbb{Z}, m \in \mathbb{N}$. 如果 $m \mid (a - b)$，則稱 $a$ 和 $b$ 對模 $m$ 同餘，其表達方式為：$a \equiv b \; (\text{mod } m)$. 另一方面，如果 $m \not\mid (a - b)$，則稱 $a$ 和 $b$ 對模 $m$ 不同餘，其表達方式為：$a \not\equiv b \; (\text{mod } m)$.

例 2.1.1
由於 $7 \mid (211 - 15)$，所以 $211$ 和 $15$ 對模 $7$ 同餘，記作：$211 \equiv 15 \; (\text{mod } 7)$。

從這個例子中，我們應可注意到，$211$ 被 $7$ 除時的餘數為 $1$，而 $15$ 被 $7$ 除時的餘數也是 $1$。換句話說，它們被 $7$ 除時的餘數是相同的，這就是我們稱它們為「對模 $7$ 同餘」的理由了。

例 2.1.2
由於 $3 \not\mid 24 - 5$，所以 $24$ 和 $5$ 對模 $3$ 不同餘，記作 $24 \not\equiv 5 \; (\text{mod } 3)$。

當 $24$ 被 $3$ 除時的餘數為 $0$，而 $5$ 被 $3$ 除時的餘數為 $2$。因此它們被 $3$ 除時所得的餘數是不一樣的。
習作 2.1.1

試判斷以下語句的真假 (設 $a, k \in \mathbb{Z}, m \in \mathbb{N}$)：

a) $38 \equiv 43 \pmod{5}$
b) $43 \equiv 38 \pmod{6}$
c) $0 \not\equiv 20 \pmod{4}$
d) $22 \equiv 32 \pmod{4}$
e) $22 \equiv 32 \pmod{10}$
f) $1 + 1 \equiv 0 \pmod{2}$
g) $a \not\equiv a + 2m \pmod{m}$
h) $a \equiv a + km \pmod{m}$
2.2 同餘的性質

從整數的關係 (relation) 的角度來看，同餘是一個等價關係 (equivalence relation)，即：

定理 2.2.1

對任意整數 \(a, b, c\)，自然數 \(m\)，

a) \(a \equiv a \pmod{m}\) [自反性 (reflexive property)]；

b) 如果 \(a \equiv b \pmod{m}\)，則 \(b \equiv a \pmod{m}\) [對稱性 (symmetric property)]；

c) 如果 \(a \equiv b \pmod{m}\) 及 \(b \equiv c \pmod{m}\)，則 \(a \equiv c \pmod{m}\) [傳遞性 (transitive property)]；

思考題 2.2.1

你能解釋 / 證明上述定理嗎？

兩個同模的同餘式可能進行加、減、乘的運算，請參閱以下定理：

定理 2.2.2

對任意的整數 \(a, b, c, d\)，自然數 \(m\)，如果 \(a \equiv b \pmod{m}\) 及 \(c \equiv d \pmod{m}\)，則

a) \(a + c \equiv b + d \pmod{m}\)；

b) \(a - c \equiv b - d \pmod{m}\)；

c) \(ac \equiv bd \pmod{m}\)；

d) \(a^k \equiv b^k \pmod{m}\)，其中 \(k \in \mathbb{N}\)。
思考題 2.2.2

試解釋 / 證明定理 2.2.2

例 2.2.1

已知 x 為 1 – 50 間的整數及 x – 1 ≡ 5 (mod 40)，求 x 的值。

解：

∴ x – 1 ≡ 5 (mod 40) 及 1 ≡ 1 (mod 40)

根據定理 2.2.2a，
∴ x – 1 + 1 ≡ 5 + 1 (mod 40)
∴ x ≡ 6 (mod 40)
∴ 1 ≤ x ≤ 50
∴ x = 6 或 46

例 2.2.2

設 x + 7 ≡ 12 (mod 3)，求 x 的值。

解：

∴ x + 7 ≡ 12 (mod 3)及 7 ≡ 7 (mod 3)

根據定理 2.2.2b，
∴ x + 7 – 7 ≡ 12 – 7 (mod 3)
∴ x ≡ 5 (mod 3)
∴ 5 ≡ 2 (mod 3)

根據定理 2.2.1c，
∴ x ≡ 2 (mod 3)
例 2.2.3

設 $\frac{x}{2} \equiv 3 \pmod{5}$，求 $x$ 的值。

解：

根據定理 2.2.2c，

$\therefore \frac{x}{2} \times 2 \equiv 3 \times 2 \pmod{5}$

$\therefore x \equiv 6 \pmod{5}$

$\therefore x \equiv 1 \pmod{5}$

例 2.2.4

求 $10^{20}$ 被 9 除所得的餘數。

解：

$\therefore 10 \equiv 1 \pmod{9}$

根據定理 2.2.2d，

$\therefore 10^{20} \equiv 1^{20} \pmod{9}$

$\therefore 10^{20} \equiv 1 \pmod{9}$

即 $10^{20}$ 被 9 除所得的餘數為 1。

例 2.2.5

證明 $41 \mid 2^{20} - 1$ (但不許直接計算 $2^{20} - 1$ 的值)。

解：

首先，我們留意到 $2^{5} = 32$，而且 32 只欠 9 便可被 41 整數，

因此，$2^{5} \equiv -9 \pmod{41}$

根據定理 2.2.2d，
\[
\begin{align*}
\therefore (2^5)^4 & \equiv (-9)^4 \pmod{41} \\
\therefore 2^{20} & \equiv 81^2 \pmod{41} \quad \text{(1)} \\
\text{由於 } 81 & \equiv -1 \pmod{41} \\
\therefore 81^2 & \equiv (-1)^2 \pmod{41} \\
\therefore 81^2 & \equiv 1 \pmod{41} \quad \text{(2)} \\
\therefore \text{根據(1)和(2)及定理 2.2.1c，} \\
\therefore 2^{20} & \equiv 1 \pmod{41} \\
\text{根據定理 2.2.2b，} \\
\therefore 2^{20} - 1 & \equiv 1 - 1 \pmod{41} \\
\therefore 2^{20} - 1 & \equiv 0 \pmod{41} \\
\text{即 } 41 & \mid 2^{20} - 1.
\end{align*}
\]

思考題 2.2.3

a) 試判斷以下推論是否正確：

已知 \(6x \equiv 4 \pmod{10}\)

所以 \(\frac{6x}{2} \equiv \frac{4}{2} \pmod{10}\)，即 \(3x \equiv 2 \pmod{10}\)

b) 證明費馬數的 \(F_5 = 2^{2^5} + 1\) 是 641 的倍數

網上或電腦資源

有關費馬數的說明可參考以下網頁：

2.3 同餘的簡單應用

2.3.1 整除性

在單元 1 中，我們探討過數字的整除性，其實我們也可以利用同餘研究數的整除性。

例 2.3.1

\[ 277 \equiv 2 \times 100 + 77 \pmod{4} \]
\[ \equiv 77 \pmod{4} \] (因為 100 \equiv 0 (mod4))

故此，4 | 277 當且僅當 4 | 77

從上述例子得知，我們只須檢查 77 是否可被 4 整除，便可判斷 277 是否 4 的倍數。(即 4 的整除性：4 | a 當且僅當 4 | (a_1 \times 10 + a_0))。

例 2.3.2

\[ 2727 \equiv 2 \times 1000 + 7 \times 100 + 2 \times 10 + 7 \pmod{10} \]
\[ \equiv 7 \pmod{10} \] (\because\ 1000 \equiv 100 \equiv 10 \equiv 0 \pmod{10})

這說明了 10 | a 當且僅當 a_0 = 0。

思考題 2.3.1

試以同餘的概念闡釋 11 的整除性判定方法，可參考單元 1 中 1.5.3 節。
例 2.3.3

求 $2^{75}$ 的個位數。

解：

如果 $a$ 的個位數是 $a_0$，則 $a \equiv a_0 \pmod{10}$。

要計算 $2^{75}$ 的個位數，我們只須找出一個介乎 0 至 9 的整數 $a_0$ 使得

$$2^{75} \equiv a_0 \pmod{10}$$

便可知道 $a_0$ 是所需答案了。

觀察 2 的冪的個位數：

$$
2^1 \equiv 2 \pmod{10} \\
2^2 \equiv 4 \pmod{10} \\
2^3 \equiv 8 \pmod{10} \\
2^4 \equiv 6 \pmod{10} \\
2^5 \equiv 2 \pmod{10} \\
2^6 \equiv 4 \pmod{10} \\
2^7 \equiv 8 \pmod{10} \\
2^8 \equiv 6 \pmod{10}
$$

(餘此類推)

很容易發現個位數之間是很有規律的：2、4、8、6、2、4、8、6、…

循環節是：2、4、8、6

∴ $75 = 4 \times 18 + 3$

∴ $2^{75}$ 的個位數是 8。
利用 Maple 或其他電腦代數系統驗算：

\[ 2^{75} = 37778931862957161709568 \]

例 2.3.4
求 \(3^{41}\) 的個位數。
解：

觀察 3 的冪的個位數：

\[
\begin{align*}
3^1 & \equiv 3 \pmod{10} \\
3^2 & \equiv 9 \pmod{10} \\
3^3 & \equiv 7 \pmod{10} \\
3^4 & \equiv 1 \pmod{10} \\
3^5 & \equiv 3 \pmod{10} \\
3^6 & \equiv 9 \pmod{10} \\
3^7 & \equiv 7 \pmod{10} \\
3^8 & \equiv 1 \pmod{10}
\end{align*}
\]

(餘此類推)

可見 3 的冪的個位數有以下的規律：

3、9、7、1、3、9、7、1、...

即循環節是：3、9、7、1

\[
\therefore 41 = 4 \times 10 + 1
\]

\[
\therefore 3^{41} \equiv 3 \pmod{10}
\]

即 \(3^{41}\) 的個位數是 3。

驗算：

\[ 3^{41} = 36472996377170786403 \]

其個位數為 3
習作 2.3.1
試計算下列各題：

a) $7^{14}$ 的十位和個位數

b) $5^{25}$ 的百位、十位和個位數

2.3.2 計算身份證的檢定碼的速算法

「同餘」除了可以用來解釋整除性外，也可以幫助我們計算（香港）身份證的檢定碼(check digit)。首先，讓我們解釋一下身份證上的檢定碼是甚麼的一回事。我們的身份證號碼主要由一個英文字母和六個數字所組成，例如，L 123465，為了防止身份證號碼因抄寫或輸入時而造成的錯誤出現(例如，把 L123465 写為 L123456)，我們便在身份證號碼後面加上一個數字，作為檢查驗證之用。這個數字，就是我們前面所說的檢定碼了，它是利用身份證號碼計算出來的，當身份證號碼因抄寫或輸入而出現錯誤時，這個檢查碼便很有可能會與錯寫的身份證號碼不符，錯誤便會因此而被及早發現了。

身份證上的這個檢定碼是如何從身份證號碼中計算出來的呢？以下就讓我們介紹一下吧！

設身份證號碼為

$$x \ y \ abcdef (g)$$

其中 $x$ 通常為空格，其數值為 58；$y$ 為字母，其數值為 $9 + “字母的排序”$，例 $A = 9 + 1 = 10$、$B = 9 + 2 = 11$、…、$L = 9 + 12 = 21$；$a$、$b$、$c$、$d$、$e$、$f$
則為 0−9 之間的整數；而 g 則為檢定碼，它可以是 0−10 之間的整數
(如果是 10，則用 ‘A’ 表示)，其數值由下式給出：
$$11|(9x + 8y + 7a + 6b + 5c + 4d + 3e + 2f + g)$$；
或
$$9x + 8y + 7a + 6b + 5c + 4d + 3e + 2f + g \equiv 0 \pmod{11}$$。

例如 2.3.5

要計算 □ L123465 (g) 的檢定碼 g，我們得下式
$$11|(9 \times 58 + 8 \times 21 + 7 \times 1 + 6 \times 2 + 5 \times 3 + 4 \times 4 + 3 \times 6 + 2 \times 5 + 1 \times g)$$
即 $$11|(768 + g)$$；
由於 g 是 0 至 10 間的整數，所以，g = 2。
換句話說，上述的身份證號碼是 □ L123457 (2)。

利用同餘的性質，我們可以把上述計算簡化，說不定，心算好的同學可以
不用紙筆或計數機，便可在數秒間計算出任何一個身份證的檢定碼。

以身份證 □ L427147 (?) 為例：

首先，我們應盡量在計算過程中，把數簡化。例如，由於 $58 \equiv 3 \pmod{2}$，
因此，所有出現 58 的地方，都可以用 3 來代替。同理，49、33、51 分
別可被 5、0、−4 取代。簡化的原则可締結為：$ab$ 可被 $b−a$ 取代。

然後，把對應的乘數寫在身份證號碼的上面：

$$9\ 8\ 7\ 6\ 5\ 4\ 3\ 2$$
$$58\ L\ 4\ 2\ 7\ 1\ 4\ 7$$
由於 $L=21$，運用上面剛談過的簡化原則，我們得：

$$
\begin{array}{cccccccc}
9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\
\phantom{0} & 3 & \phantom{0} & 4 & 2 & 7 & 1 & 4 & 7 \\
\end{array}
$$

接下來，我們把這八組數分成四對，為了方便說明，我們把每對組別的數用線連起來：

每一對組別的數，例如：

$$
\begin{array}{cccccccc}
9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\
\phantom{0} & 3 & \phantom{0} & 4 & 2 & 7 & 1 & 4 & 7 \\
\end{array}
$$
我們從下排的數中（即 3 和 7），選取較大的數，減去較小的數，即 7 – 3。然後把結果乘以剛才較大的數的上面的那個數（即 7 上面的 2），得出的結果是：

\[(7 – 3) \times 2 = 8\]

這個數便可代替原先數式中的 9 \times 3 + 2 \times 7。其餘四對組別的數也是這樣計算：

第二組的計算是：

\[(4 – (-1)) \times 3 = 15\]

按上述簡化原則，15 可用 4 取代，即：\((4 – (-1)) \times 3 = 15 \rightarrow 4\)。

第三組的計算是：

\[(4 – 1) \times 7 = 21 \rightarrow -1\]
最後一組的計算是：

\[(7 - 2) \times 5 = 25 \rightarrow 3\]

把這四組的結果加起來，得出：

\[8 + 4 + (-1) + 3 = 14 \rightarrow 3\]

3 須加 8 才會是 11 的倍數，因此，身份證括號內的數是 8。

習作 2.3.2
試利用速算法計算身份證 H744221 的檢定碼。

網上或電腦資源
有關身份證檢定碼的資料，可參考：

http://www.hkcities.com/123/id.html

身份證上面，出生日期下面有一行字母或符號（例如：★★★AZ），你知道它們所代表的意思嗎？有關詳情，可參閱：

2.4 孫子定理 (又稱「中國剩餘定理」)(Chinese Reminder Theorem)

「今有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二。問物幾何？」

《孫子算經》卷下，第 26 題

運用同餘式符號表示：

\[
\begin{align*}
    x &\equiv 2 \pmod{3} \\
    x &\equiv 3 \pmod{5} \\
    x &\equiv 2 \pmod{7}
\end{align*}
\]

要找出題中未知數量，我們可以運用試誤法(trial and error)。例如，已知「三三數之剩二」，即未知數 \(x\) 是 3 的倍數再多 2 的倍數是 3、6、9、12、15、18、21、24、27、…，把它們加 2 便是 5、8、11、14、17、20、23、26、29、…。這數列中哪些數會滿足餘下的兩條同餘式呢？稍經試誤法驗算，我們便會發現 23 是其中一個答數。這個方法雖然簡單，但逐一驗算，始終效率不高。在《孫子算經》裏面，原來已經有一個更有效的解題方法：

「答曰二十三。」

術曰三三數之剩二，置一百四十；五五數之剩三，置六十三；七七數之剩二，置三十；並之得二百三十三，以二百一十減之即得。凡三三數之剩一則置七十；五五數之剩一則置二十一；七七數之剩一則置十五。一百六以上以一百五減之即得」

《孫子算經》卷下，第 26 題
我們試用同餘這工具，解釋一下孫子定理所提供的解題方法：

三條同餘式中的模是 3、5、7，它們都是兩兩互質的，而它們的最小公倍數是 105。明顯地，如果 \( a \) 是三條同餘式(*))的解，則 \( a \equiv 105 \), \( a\equiv 2\times105 \), \( a\equiv 3\times105\ldots \) 等都必定是(*)的解。換句話說，同餘式(*)如果有解的話，它的解會有無窮多個。接著，我們在 5×7 的倍數中，計算出用 3 去除，令餘數為 1 的數。用同餘式表示，我們希望計算出的，是滿足下式的 \( N \) 的值：

\[
M_1N_1 \equiv 1 \pmod{3}, \text{其中 } M_1 = 5 \times 7 \quad (\ast)
\]

即：

\[
35N_1 \equiv 1 \pmod{3} \\
2N_1 \equiv 1 \pmod{3} \quad (\because \ 35 \equiv 2 \pmod{3}) \\
N_1 \equiv 4
\]

同理，我們在 3×7、3×5 的倍數中，和 \( N_2 \) 的值：

\[
M_2N_2 \equiv 1 \pmod{5}, \quad M_3N_3 \equiv 1 \pmod{7}, \text{其中 } M_2 = 3 \times 7, \quad M_3 = 3 \times 5.
\]

經簡單計算得：

\[
N_2 \equiv 1 \pmod{5}, \quad N_3 \equiv 1 \pmod{7}.
\]

這樣，\( 2M_1N_1 + 3M_2N_2 + 2M_3N_3 \) 便是其中一個解。[為甚麼？]

即 \( 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \) 是其中一個解。

由於 233 > 105，故可將 233 逐一減去 105 後，便会得到 23 這一答案。

思考題 2.4.1

(a) 試解釋/證明 \( x \equiv 2M_1N_1 + 3M_2N_2 + 2M_3N_3 \pmod{15} \) 必滿足同餘方程(*)。

(b) 明朝程大位的《算法統宗》有歌如下：『三人同行七十稀，五樹梅

花廿一枝，七子團圓整月半，除百零五便得知。』這歌內容與上面的題解
有些什麼關係呢?

例 2.4.1

解：

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} ，且 0 \leq x \leq 70 \\ x \equiv 6 \pmod{13} \end{cases}$$

解：三條同餘式中的模是 2, 3, 11，它們都是兩兩互質的，而它們的最小公倍數是 66。

設 $M_1 = 3 \times 13 = 39$, $M_2 = 2 \times 13 = 26$, $M_3 = 2 \times 3 = 6$。

從 $M_1N_1 \equiv 1 \pmod{2}$ 得：

$$39N_1 \equiv 1 \pmod{2}$$

$$1 \times N_1 \equiv 1 \pmod{2}$$

∴ $N_1$ 的其中一個解是 1。

從 $M_2N_2 \equiv 1 \pmod{3}$ 得：

$$26N_2 \equiv 1 \pmod{3}$$

$$2 \times N_2 \equiv 1 \pmod{3}$$

∴ $N_2$ 的其中一個解是 2。

從 $M_3N_3 \equiv 1 \pmod{11}$ 得：

$$6N_3 \equiv 1 \pmod{11}$$

$$N_2 \equiv 2 \pmod{11}$$

∴ $N_2$ 的其中一個解是 2。

因此，$x \equiv 1 \times M_1N_1 + 2M_2N_2 + 5M_3N_3 \pmod{66}$

∴ $x \equiv 1 \times 39 \times 1 + 2 \times 26 \times 2 + 5 \times 6 \times 2 \pmod{66}$

$$x \equiv 203 \pmod{66}$$

∴ $0 \leq x \leq 70$ ∴ $x = 203 - 2 \times 66 = 71$。
習作 2.4.1
解下列同餘方程:
(a) \(31x \equiv 1 \pmod{15}\)。
(b) \(25x + 4 \equiv 3 \pmod{26}\)。
(c) \[
\begin{cases}
  x \equiv 4 \pmod{5} \\
  x \equiv 3 \pmod{6} \quad & \text{且} \quad 1 \leq x \leq 100 \\
  x \equiv 1 \pmod{7}
\end{cases}
\]
(d) \[
\begin{cases}
  x \equiv 3 \pmod{7} \\
  x \equiv 4 \pmod{5} \quad & \text{且} \quad 0 \leq x \leq 100 \\
  x \equiv 0 \pmod{2}
\end{cases}
\]

習作 2.4.2
假設王老師的歲數為 \(x\)，已知 \(x\) 滿足 \[
\begin{cases}
  2x \equiv 1 \pmod{3} \\
  10x \equiv 1 \pmod{11} \\
  x \equiv 1 \pmod{8}
\end{cases}
\]

思考題 2.4.2
試解以下的韓信點兵問題:
「有兵一列，若列成五行縱隊，則末行一人；列成六行縱隊，則末行五人；列成七行縱隊，則末行四人；列成十一行縱隊，則末行十人，求兵數。」
網上或電腦資源

若想得知更多有關孫子定理，可瀏覽以下網頁：

http://mikekong.uhome.net/Maths/Problems/chinese_remainder01.html

有關衍生孫子定理的過程，可瀏覽以下有關韓信點兵的網頁：

http://episte.math.ntu.edu.tw/articles/sm/sm_01_01_2/index.html