同餘式及一些應用

彭志帆

國立臺灣大學數學系學生

我們用英文字母 $a, b, c, \cdots$ 表示整數。

定義1 如果 m 整除 $(a-b)$，我們記作 $a \equiv b \pmod{m}$；如果 m 不能整除 $(a-b)$，我們記作 $a \not\equiv b \pmod{m}$。

由定義1顯然有

引理1 $a \equiv a \pmod{m}$。

引理2 若 $a \equiv b \pmod{m}$，則 $b \equiv a \pmod{m}$。

引理3 若 $a \equiv c \pmod{m}$，$b \equiv c \pmod{m}$，則 $a \equiv b \pmod{m}$。

推論4 若 $a \equiv b \pmod{m}$，則 m 整除 a 的充要條件是 m 整除 b。

證明：在引理3中取 $c = 0$，顯然推出推論4。

引理5 若 $a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$，則 $a \pm c \equiv b \pm d \pmod{m}$。

證明：依假設，得

$$(a-b) = m \times s$$
$$(c-d) = m \times t$$

其中 s，t 爲整數。於是，得

$$(a \pm c) - (b \pm d) = m \times (s \pm t)$$

其中 $(s \pm t)$ 是整數。因此，$a \pm c \equiv b \pm d \pmod{m}$。

引理6 若 $a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$，則 $a \times c \equiv b \times d \pmod{m}$。

證明：依假設，得

$$(a-b) = m \times s$$
$$(c-d) = m \times t$$

其中 s，t 爲整數。於是，得

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= c(a-b) + b(c-d) \\ &= c \times m \times s + b \times m \times t \\ &= m(cs + bt) \end{aligned}$$

其中 $(cs + bt)$ 是整數。因此，$ac \equiv bd \pmod{m}$。

推論7 若 $a \equiv b \pmod{m}$，則 $ac \equiv bc \pmod{m}$。

證明：在引理6中取 $d = c$，立即得證。

推論8 如果 $a \equiv b \pmod{m}$，則 $a^n \equiv b^n \pmod{m}$，其中 n 是正整數。

證明：當 $n = 1$ 時，推論8顯然成立。

假設 $n = k$ 時，推論8成立，即

$$a^k \equiv b^k \pmod{m}$$

則由 $a \equiv b \pmod{m}$，$a^k \equiv b^k \pmod{m}$ 和引理6，我們有

$$a^{k+1} \equiv b^{k+1} \pmod{m}$$

推論9 若 $a_i \equiv b_i \pmod{m}$，其中 $i = 1, 2, \cdots, n$，則

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$$

$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m}$$

這裏 $\sum a_i$ 表示所有 a_i 的和，$\prod a_i$ 表示所有 a_i 的乘積。特別地，取

$$a = a_1 = a_2 = \cdots = a_n$$

$$b = b_1 = b_2 = \cdots = b_n$$

我們得到推論7和推論8。

證明：留給讀者。

引理10 若 $x \equiv y \pmod{m}$，則

$$\sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} a_i y_i \pmod{m}$$

其中 $a_0, a_1, \cdots, a_n$ 都是整數。

證明：留給讀者。

應　用

$753428 = 7\times10^5 + 5\times10^4 + 3\times10^3 + 4\times10^2 + 2\times10 + 8$。一般地

$P=\sum_{i=0}^{n} a_i 10^i$ ，其中 $0 \le a_i \le 9$ 。

定理11 若

$$(\sum_{i=0}^{s} a_i 10^i)(\sum_{i=0}^{t} b_i 10^i) = (\sum_{i=0}^{s+t} c_i 10^i)$$

其中 $0 \le a_i \le 9$ ，$0 \le b_i \le 9$ ，$0 \le c_i \le 9$ ，則

$$(\sum_{i=0}^{s} a_i)(\sum_{i=0}^{t} b_i) \equiv (\sum_{i=0}^{s+t} c_i) \pmod 9$$

證明：在引理10中取 $x = 10$, $y = 1$, $m = 9$, $n = s$ ，則有

$$\sum_{i=0}^{s} a_i 10^i \equiv \sum_{i=0}^{s} a_i \pmod 9$$

同理

$$\sum_{i=0}^{t} b_i 10^i \equiv \sum_{i=0}^{t} b_i \pmod 9$$

$$\sum_{i=0}^{s+t} c_i 10^i \equiv \sum_{i=0}^{s+t} c_i \pmod 9$$

依引理6，得

$$(\sum_{i=0}^{s} a_i 10^i)(\sum_{i=0}^{t} b_i 10^i) \equiv (\sum_{i=0}^{s} a_i)(\sum_{i=0}^{t} b_i) \pmod 9$$

依引理3，得

$$(\sum_{i=0}^{s+t} c_i 10^i) \equiv (\sum_{i=0}^{s} a_i)(\sum_{i=0}^{t} b_i) \pmod 9$$

再依引理3，得

$$(\sum_{i=0}^{s} a_i)(\sum_{i=0}^{t} b_i) \equiv (\sum_{i=0}^{s+t} c_i) \pmod 9$$

〔**例1**〕 742861 × 233463是否等於173330557643？

由於 $(7+4+2+8+6+1)\times(2+3+3+4+6+3) \not\equiv (1+7+3+3+3+0+5+5+7+6+4+3) \pmod 9$，所以由定理11知道 $742861 \times 233463 \neq 173330557643$。事實上，$742861 \times 233463 = 173430557643$。

定理11的逆定理不成立。例如 $(1+7+6+3+4)\times(2+3+1+1+7) \equiv (4+1+6+6+4+5+1+7+8) \pmod 9$ ，但 $17634 \times 23117 \neq 416645178$。

定理12 令 $P = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0$ ，則

(1) 2整除 P 的充要條件是2整除 a_0 。

(2) 3整除P的充要條件是3整除$(\sum_{i=0}^{n} a_i)$。

(3) 4整除P的充要條件是4整除$(2a_1 + a_0)$。

(4) 9整除P的充要條件是9整除$(\sum_{i=0}^{n} a_i)$。

證明：(1)因爲

$$P = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0 \equiv a_0 \pmod 2$$

因此，依推論4，2整除P的充要條件是2整除a_0。

(2)因爲

$$10 \equiv 1 \pmod 3$$

依引理10，可得

$$P = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod 3$$

因此，依推論4，3整除P的充要條件是3整除$\sum_{i=0}^{n} a_i$。

(3)和(4)的證明略去。

〔**例2**〕 由於2整除6，所以由定理12知道，2整除123456。

〔**例3**〕 由於3整除(7+2+3+6+7+8+1+2)，所以由定理12知道，3整除72367812。

參 考 書 籍

(1) 李恭晴：整數論，協進圖書公司。

(2) Ivan Niven & H. S. Zuckerman, AN INTRODUCTION TO THE THEORY OF NUMBERS, 凡異出版社。