數學傳播　34卷1期, pp. 58-64

n 元數與同餘式組

許家甄・李昱宏・潘信鴻・何青瀚・徐含馥・羅春光

1. 前言

在 [2] 文中, 作者討論一組循環型的同餘式組問題

$$\begin{cases} ab \equiv p \pmod{c} \\ bc \equiv p \pmod{a} \\ ca \equiv p \pmod{b} \end{cases}$$

的質數三元數解 (a, b, c) 存在之充要條件, 並證明了當 $p = 1$ 或 -1 時, 同餘式組有唯一解 $(2, 3, 5)$ 和 $(2, 3, 7)$。本文目的是簡化 [2, 定理 3] 的證明, 並將問題推廣至 n 維的同餘式組, 即對 $i = 1, \ldots, n$,

$$\prod_{j \neq i} a_j \equiv p \pmod{a_i}.$$

其中 $a_1, \ldots, a_n$ 只須互質。當 $p = -1$ 時, 我們最少能找到一組解, 當 $p = 1$ 時, 最少能找到兩組解。而且這些解都有一定的規律。當 $n = 4$ 時, 唯一性問題也可清楚討論 (請參考定理 3.1 和定理 3.2)。更進一步地, 我們建立了互質 n 元數解存在的充分必要條件。

2. 解存在的充要條件

若 a, b, c 是互質正整數, 且 $a < b < c$, 我們稱 (a, b, c) 爲三元數。在 a, b, c 是質數的假設下, [2] 文作者討論如 (2.1) 的循環型同餘式組的求解狀況。他們發現, 當 $p = \pm 1$ 時, 同餘式組只有一組解, 分別是 $(2, 3, 5)$ 和 $(2, 3, 7)$。但對一般的 p, 不同的狀況都可能出現, 同餘式組可能無解, 可能有一組解或二組解、甚至三組解。我們猜想任意多組解均可能出現。衆所皆知, 在同餘式組中, 中國剩餘定理是最重要的定理:

若 $m_1, m_2, \ldots, m_k$ 是兩兩互質的正整數, 則同餘式組

$$\begin{cases} x = b_1 \pmod{m_1} \\ x = b_2 \pmod{m_2} \\ \cdots \quad \cdots \\ x = b_k \pmod{m_k} \end{cases}$$

有唯一解: $x = b_1\theta_1 N_1 + b_2\theta_2 N_2 + \cdots + b_k\theta_k N_k \pmod{\theta}$。其中 $\theta = m_1 m_2 \cdots m_k$, $\theta_i = \theta/m_i$, 而 N_i 是 θ_i 對 m_i 的乘法逆元素。

這個定理的證明方法, 是先構造 $\theta_i N_i$ 使得 $\theta_i N_i \equiv 1 \pmod{m_i}$, 但對其它的 m_j, 則有 $\theta_i N_i \equiv 0 \pmod{m_j}$, 而所求 x 即爲衆多 $b_i\theta_i N_i$ 的總和 (見 [1])。在本文中, 我們利用這個精神簡化 [2] 文中定理3的證明。值得注意的是, 此處我們不必假設 a, b, c 是質數, 只須假設 a, b, c 兩兩互質, 正如中國剩餘定理的假設。

定理 2.1: 三元數 (a, b, c) 是同餘式組

$$\begin{cases} ab \equiv p \pmod{c} \\ bc \equiv p \pmod{a} \\ ca \equiv p \pmod{b} \end{cases} \tag{2.1}$$

的整數解若且唯若

$$p \equiv ab + bc + ca \pmod{abc}.$$

證明:

($\Leftarrow$) 顯而易見, 故略。

($\Rightarrow$) 由 (2.1) 式知

$$ab + bc + ca \equiv ab \equiv p \pmod{c};$$

$$ab + bc + ca \equiv bc \equiv p \pmod{a};$$

$$ab + bc + ca \equiv ca \equiv p \pmod{b}.$$

因爲 a、b、c 兩兩互質, 故

$$ab + bc + ca \equiv p \pmod{abc}. \qquad \square$$

我們定義 $(a_1, a_2, \ldots, a_n)$ 爲 n 元數若 $a_1, \ldots, a_n$ 是兩兩互質的 n 個正整數, 且滿足 $a_1 < a_2 < \cdots < a_n$。

定理 2.2: 若 $(a_1, a_2, \ldots, a_n)$ 爲 n 元數, 令 $\gamma = a_1 a_2 \cdots a_n$, $\Gamma_i = \dfrac{\gamma}{a_i}$, 則對所有 $i = 1, 2, \ldots, n$

$$\Gamma_i \equiv p \pmod{a_i} \tag{2.2}$$

若且唯若

$$p \equiv \sum_{i=1}^{n} \Gamma_i \pmod{\gamma}.$$

證明: 明顯若 $p \equiv \sum_{j=1}^{n} \Gamma_i \pmod{\gamma}$, 則對每一 a_i, 有 $p \equiv \Gamma_i \pmod{a_i}$。反過來, 若 $p \equiv \Gamma_i \pmod{a_i}$, 則

$$\sum_{j=1}^{n} \Gamma_j \equiv \Gamma_i \equiv p \pmod{a_i}.$$

因 $a_1, a_2, \cdots, a_n$ 兩兩互質, 故

$$\sum_{j=1}^{n} \Gamma_j \equiv p \pmod{\gamma}. \qquad \square$$

3. 4 元數解

定理 3.1: 若 (a, b, c, d) 是 4 元數, 且滿足

$$\begin{cases} abc \equiv 1 \pmod{d} \\ abd \equiv 1 \pmod{c} \\ acd \equiv 1 \pmod{b} \\ bcd \equiv 1 \pmod{a} \end{cases}$$

則 $(a, b, c, d) = (2, 3, 7, 41)$ 或 $(2, 3, 11, 13)$。

證明: 利用以下引理 3.3, 得 $a = 2$, $b = 3$。又令

$$6c = 1 + kd, \tag{3.1}$$

$$6d = 1 + lc, \tag{3.2}$$

$$2cd = 1 + mb. \tag{3.3}$$

從 (3.2) 減去 (3.1) , (3.3) 減去 (3.1) 後可得:

$$d(k + 6) = c(l + 6),$$

$$d(k + 2c) = 3(m + 2c).$$

因 b,c,d 兩兩互質且 $b=3$, 所以 $c|(k+6)$, 且 $3|(k+2c)$。令

$$\begin{aligned} k+2c &= 3x, \\ k+6 &= cy, \end{aligned} \tag{3.4}$$

得

$$3(x+2) = c(y+2).$$

故 $3|(y+2)$。從 (3.1) 知 $k<6$, 以此代入 (3.4), 得 $y<4$, 所以 $y=1$。又從 (3.4) 知

$$1 \le k = c-6 < 6.$$

故 $c=7$ 或 11, 即 $k=1$ 或 5, 且由 (3.1) 可得 $d=41$ 或 13。因此 $(a,b,c,d)=(2,3,7,41)$ 或 $(2,3,11,13)$。 □

定理 3.2: 若 (a,b,c,d) 是 4 元數, 且滿足

$$\begin{cases} abc \equiv -1 \pmod{d} \\ abd \equiv -1 \pmod{c} \\ acd \equiv -1 \pmod{b} \\ bcd \equiv -1 \pmod{a} \end{cases}$$

則 $(a,b,c,d)=(2,3,7,43)$。

證明: 與上一定理相似。$a=2$, $b=3$, 且

$$\begin{aligned} 6c &= kd-1, \\ 6d &= lc-1, \\ 2cd &= 3m-1. \end{aligned}$$

又 $k+2c=3x$, $k+6=cy$, 則 $3|(y+2)$。因 $k<6$, 故 $y=1$, 且 $7 \le c < 12$, 得 $c=7$, $d=43$。 □

引理 3.3: 設 (a,b,c,d) 爲4元數, 滿足

$$\begin{cases} abc \equiv p \pmod{d} \\ abd \equiv p \pmod{c} \\ acd \equiv p \pmod{b} \\ bcd \equiv p \pmod{a} \end{cases}$$

若 $abc > p > -5$, 則 $a = 2$, $b = 3$, 且 $c < 12$。

證明: 令

$$\begin{cases} abc = dk + p \\ abd = cl + p \\ acd = bm + p \\ bcd = an + p \end{cases} \tag{3.5}$$

其中 k, l, m, n 均爲正整數, 且 a, b, c, d, 兩兩互質。將以上等式兩兩相減, 可得 $abc - abd = dk - cl$, 故 $c(ab + l) = d(ab + k)$, 導致 $c|(ab + k)$。同理, 有 $abc - acd = dk - bm$, 且 $b(ac + m) = d(ac + k)$, 故 $b|(ac + k)$。另外, $a(bc + n) = d(bc + k)$, 得 $a|(bc + k)$。令

$$ab + k = cx, \tag{3.6}$$

$$ac + k = by, \tag{3.7}$$

$$bc + k = az. \tag{3.8}$$

從 (3.6) 減去 (3.7) 得

$$c(a + x) = b(a + y).$$

即 $b|(a + x)$, 令

$$bs = a + x \tag{3.9}$$

現在, 從 $p > -5$ 和 (3.5) 知

$$dk < abc + 5 < abd$$

故 $k < ab$, 代入 (3.6), 得 $x < 2a$, 再代入 (3.9) 後, 得 $0 < s < 3$。

若 $s = 2$, 則從 (3.9)、(3.6) 知 $2b = a + x < 3a$, 且

$$k = 2bc - ab - ac < ab. \tag{3.10}$$

故有 $2bc < a(2b + c)$, 即 $c < 2b$。再將 (3.10) 代入 (3.8), 得

$$az = 3bc - ab - ac.$$

因此 $a = 3$, $b = 4$, $x = 5$。代入 (3.10), $k = 5c - 12 < 12$, 矛盾。故 $s = 1$, 即 $b = a + x < 3a$。代入 (3.6),

$$k = bc - ab - ac < ab. \tag{3.11}$$

再代入 (3.8), $az = 2bc - ab - ac$, 故 $a = 2$, $b = 3$ 或 5。若 $b = 5$, 從 (3.11) 得 $c < 6$, 矛盾。故 $b = 3$, 從 (3.11) 知 $c < 12$。證畢。 □

利用定理 2.2 和 引理 3.3, 我們可以得到一個快速求循環型同餘式組的方法。例如: 如果 $p = 2n$ 是一偶數, 且 $1 < p < 30$, 則 $a = 2$, $b = 3$, 所以

$$\begin{aligned} 2n &\equiv 6(c+d) + 5cd \pmod{6cd} \\ &\equiv 6(c+d) - cd \pmod{6cd} \end{aligned}$$

因此,

$$2n + cd \equiv 6(c+d) \pmod{6cd}.$$

故 cd 必爲偶數。同餘式組 (2.2) 無 4 元數解。

4. n 元數解的規律

以此規律進行, 則知 $(2, 3, 7, 43, 1807)$ 和 $(2, 3, 7, 43, 1805)$ 是同餘式組 (2.2) 對應著 $p = -1$ 和 $p = 1$ 的5元數解。而下一組的6元數解, 是 $(2, 3, 7, 43, 1807, 3263443)$ 和 $(2, 3, 7, 43, 1807, 3263441)$。

構造數列 $\beta_1 = 2$, $\beta_2 = 3$, $\beta_{n+1} = \beta_1\beta_2 \ldots \beta_n + 1$。顯然, 數列 $\{\beta_i\}$ 遞增且兩兩互質。

定理 4.1: 對所有 $n \geq 2$, 向量 $\mathcal{B}_n := (\beta_1, \beta_2, \ldots, \beta_n)$ 滿足同餘式組

$$\Gamma_i(\mathcal{B}_n) \equiv -1 \pmod{\beta_i}, \qquad i = 1, 2, \ldots, n, \tag{4.1}$$

其中 $\Gamma_i(\mathcal{B}_n) = \prod_{j \neq i} \mathcal{B}_{n,j}$, 而 $\mathcal{B}_{n,j}$ 是向量 $\mathcal{B}_n$ 的第 j 項。又令 $\mathcal{A}_n := (\beta_1, \beta_2, \ldots, \beta_{n+1} - 2)$, 若 $\mathcal{A}_n$ 滿足同餘式組, 則

$$\Gamma_i(\mathcal{A}_n) \equiv 1 \pmod{\mathcal{A}_{n,i}}, \qquad i = 1, 2, \ldots, n. \tag{4.2}$$

證明: 利用數學歸納法。當 $n = 2$ 時, $\mathcal{B}_2 = (2, 3)$; 當 $n = 3$ 時, $\mathcal{B}_3 = (2, 3, 7)$, 已知命題成立。假設命題對 $n = k$ 成立, 即

$$\Gamma_i(\mathcal{B}_k) \equiv -1 \pmod{\beta_i}, \qquad i = 1, 2, \ldots, k.$$

則對 $i = 1, 2, \ldots, k$,

$$\begin{aligned} \Gamma_i(\mathcal{B}_{k+1}) &= \Gamma_i(\mathcal{B}_k) \cdot \beta_{k+1} \\ &\equiv (-1) \cdot \beta_{k+1} \pmod{\beta_i} \\ &\equiv -1 \pmod{\beta_i}. \end{aligned}$$

又

$$\begin{aligned}\Gamma_{k+1}(\mathcal{B}_{k+1}) &\equiv \beta_1\beta_2\cdots\beta_k \pmod{\beta_{k+1}},\\ &\equiv -1 \pmod{\beta_{k+1}}.\end{aligned}$$

同理, 也有 $\Gamma_i(\mathcal{A}_{k+1}) \equiv 1 \pmod{\mathcal{A}_{k+1,i}}$, 其中, $i = 1, 2, \ldots, k+1$。定理得證。 □

另外, 我們還找到另一規律, 已知 $(2, 3, 11, 13)$ 是對應 $p = 1$ 的 4 元數解, 容易得知 $11 = 2\cdot 6 - 1$, $13 = 2\cdot 6 + 1$。以此規律, 得知 $(2, 3, 7, 83, 85)$, $(2, 3, 7, 43, 3611, 3613)$ 也是同餘式組 (2.2) 對應於 $p = 1$ 的 5 元數解和 6 元數解。從而引伸出以下定理。

定理 4.2: 考慮 $(n+2)$ 元數 $\mathcal{C}_{n+2} = (\beta_1, \beta_2, \ldots, \beta_n, 2\gamma - 1, 2\gamma + 1)$, 其中 $\gamma = \beta_1\beta_2\cdots\beta_n$。則有

$$\Gamma_i(\mathcal{C}_{n+2}) \equiv 1 \pmod{\mathcal{C}_{n+2,i}}$$

$i = 1, \ldots, n+2$。

證明: 當 $n = 1$ 時, $\mathcal{C}_3 = (2, 3, 5)$, 命題成立。事實上, 對任意 $n \geq 1$, 若 $1 \leq i \leq n$, 由定理 4.1 知

$$\Gamma_i(\mathcal{C}_{n+2}) \equiv (-1)(-1)\cdot 1 \equiv 1 \pmod{\beta_i}.$$

另外,

$$\Gamma_{n+1}(\mathcal{C}_{n+2}) \equiv 2\gamma \equiv 1 \pmod{2\gamma - 1}; \quad \Gamma_{n+2}(\mathcal{C}_{n+2}) \equiv -2\gamma \equiv 1 \pmod{2\gamma + 1}.$$

由數學歸納法, 定理得證。 □

後記: 此論文是97學年度中山大學應用數學系高高屏數學科高中科技人才培育計畫高三班專題研究課程之部份成果, 感謝教育部中教司對本研究的補助。

參考資料

1. 華羅庚, 從孫子的神奇妙算談起, 見『華羅庚科普著作選集』, 凡異出版社, 2002年。
2. 羅春光、洪劭軒、黃拓儒, 質數三元數和同餘式組, 數學傳播季刊, 第21卷, 第二期 (1997), 66-70。

—本文作者許家甄是中山大學附屬中學高三生; 李昱宏是高雄中學高三生; 潘信鴻是高雄市立中正高中高三生; 何青翰是高雄師範大學附屬中學高三生; 徐含馥是屏東女中高三生; 羅春光是中山大學應用數學系教授。—