# 質數三元數與同餘式組

羅春光・洪劭軒・黃拓儒

## 0. 前言

質數2,3和5有一些有趣的循環性質。我們證明這三個質數是以下同餘式組當 $p = 1$ 時的唯一相異質數解,

$$\begin{aligned} ab &\equiv p \pmod{c}, \\ bc &\equiv p \pmod{a}, \\ ca &\equiv p \pmod{b}。 \end{aligned}$$

即是說, 當 $p = 1$ 時, 以上同餘式組刻劃了質數 (2,3,5)。類似地當 $p = -1$ 時, 同餘式組刻劃了質數 (2,3,7)。我們進一步考慮 $p$ 作爲任意整數的情形。在本文中, 我們證明同餘式有質數三元數解 $(a, b, c)$, 若且唯若

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

以上等價條件可控制同餘式組的解的範圍。但一般來說, 同餘式的解即使存在也不一定是唯一。我們將列舉一些例子說明之。

## 一. 質數三元數

考慮三個最簡單的質數2,3和5, 他們有下列的循環性質。

(i)

$$\begin{aligned} &2 \times 3 + 5 = 11, \\ &5 \times 2 + 3 = 13, \quad \text{三數皆爲質數。} \\ &3 \times 5 + 2 = 17, \end{aligned}$$

(ii)

$$\begin{aligned} 2 \times 3 &\equiv 1 \pmod{5}, \\ 3 \times 5 &\equiv 1 \pmod{2}, \\ 5 \times 2 &\equiv 1 \pmod{3}。 \end{aligned}$$

(iii)

$$\begin{aligned} 3^2 &\equiv -1 \pmod{5}, \\ 2^5 &\equiv -1 \pmod{3}, \\ 5^3 &\equiv -1 \pmod{2}。 \end{aligned}$$

(iv)

$$\begin{aligned} 2^5 \times 3 \equiv 2 \times 3^5 &\equiv 1 \pmod{5}, \\ 3^2 \times 5 \equiv 3 \times 5^2 &\equiv 1 \pmod{2}, \\ 5^3 \times 2 \equiv 5 \times 2^3 &\equiv 1 \pmod{3}。 \end{aligned}$$

(v)

$$2^4 \equiv 3^4 \pmod{5},$$

$$3^4 \equiv 5^4 \pmod 2,$$
$$5^4 \equiv 2^4 \pmod 3。$$

其中 (iv) 可從 (ii) 推導出, 因爲2,3,5皆爲質數, 由 Fermat(費馬) 定理 [1,2]可知:

$$2^4 \equiv 1 \pmod 5,$$
$$3^4 \equiv 1 \pmod 5。$$

所以

$$1 \equiv 2\times3 \equiv (2^4)\times2\times3 \equiv (2^5)\times3 \pmod 5,$$
$$1 \equiv 2\times3 \equiv 2\times3\times(3^4) \equiv 2\times(3^5) \pmod 5。$$

其餘可類推。

至於 (v) 的第一項同餘等式已在前面說明。第二項等式成立是因爲 $3^4$ 和 $5^4$ 皆爲奇數。此外

$$2 \equiv 5 \pmod 3,$$

因此

$$2^4 \equiv 5^4 \pmod 3。$$

所以(v) 乃是2,3,5之間的自然關係。

又考慮另一組質數2,3,7的性質:

(i′)

$$2\times3+7=13,$$
$$7\times2+3=17, \quad \text{三數皆爲質數。}$$
$$3\times7+2=23,$$

(ii′)

$$2\times3 \equiv -1 \pmod 7,$$
$$3\times7 \equiv -1 \pmod 2,$$
$$7\times2 \equiv -1 \pmod 3。$$

(iii′)

$$2^3 \equiv 1 \pmod 7,$$
$$3^7 \equiv 1 \pmod 2,$$
$$7^2 \equiv 1 \pmod 3。$$

(iv′)

$$2^7\times3 \equiv 2\times3^7 \equiv (-1) \pmod 7,$$
$$3^2\times7 \equiv 3\times7^2 \equiv (-1) \pmod 2,$$
$$7^3\times2 \equiv 7\times2^3 \equiv (-1) \pmod 3。$$

(v′)

$$2^6 \equiv 3^6 \pmod 7,$$
$$3^6 \equiv 7^6 \pmod 2,$$
$$7^6 \equiv 2^6 \pmod 3。$$

換言之 (2,3,5) 和 (2,3,7) 有著對偶的關係。其中 (iv′) 可由 (ii′) 推出, (v′) 爲2,3,7之間的自然關係, 原因和前面2,3,5時相同, 而且性質 (ii′) 刻劃了 (2,3,7) 這組質數三元數。我們稱 $(a,b,c)$ 爲質數三元數, 若 $a,b,c$ 俱爲正質數, 且有 $a<b<c$。

## 二. 質數三元數的刻劃

從前面的討論可知 (ii) 較爲重要, 事實上, 質數三元數 (2,5,31) 同樣擁有性質 (iii′)。說明性質 (iii) 或 (iii′) 不能刻劃對應之質數三元數。故此嘗試從 (ii) 著手。

定理1: 若質數三元數 $(a,b,c)$ 滿足:

$$\begin{aligned} ab &\equiv 1 \pmod c \\ bc &\equiv 1 \pmod a \\ ca &\equiv 1 \pmod b \end{aligned} \qquad (*)$$

則 $a=2$, $b=3$, $c=5$ 。

證明: 從 $(*)$ 可知, 存在正整數 $k, m, n$ 使

$$ab - 1 = kc, \tag{1}$$

$$bc - 1 = ma, \tag{2}$$

$$ca - 1 = nb。 \tag{3}$$

(1) 和 (3) 給出

$$ab - ca = kc - nb,$$

因此,

$$c(a + k) = b(a + n)。$$

由於 $b, c$ 互質,

$$b|(a + k)。 \tag{4}$$

同樣地,

$$a(b + m) = c(b + k),$$

所以

$$a|(b + k)。$$

從(1) 得知 $0 < k < a$, 因此 (4) 推出 $b = a + k$ 。又令

$$b + k = ya,$$

則 $2k = (y - 1)a$, 既然 $a$ 是質數, 且 $a$ 不整除 $k$, 則 $a$ 整除2。亦即 $a = 2, k = 1$ 。因此 $b = 3$, 而 $c = 2 \cdot 3 - 1 = 5$。

同樣的思路也能證明(ii′) 刻劃質數三元數 (2,3,7)。證明從略。

定理2: 若質數三元數 $(a, b, c)$, 且滿足

$$\begin{aligned} ab &\equiv -1 \pmod{c} \\ bc &\equiv -1 \pmod{a} \\ ca &\equiv -1 \pmod{b} \end{aligned} \tag{$*$}$$

則 $a = 2, b = 3, c = 7$。

## 三. 同餘式組

接著我們來討論有關性質 (ii) 的推廣。考慮以下同餘式組的解:

$$\begin{aligned} ab &\equiv p \pmod{c} \\ bc &\equiv p \pmod{a} \\ ca &\equiv p \pmod{b} \end{aligned} \tag{$**$}$$

若對某一整數 $p$, 存在質數三元數 $(a, b, c)$ 滿足同餘式組 $(**)$, 則稱 $(a, b, c)$ 爲同餘式組 $(**)$ 的質數三元數解。

定理3: 給定任意整數 $p, (a, b, c)$ 是 $(**)$ 的質數三元數解, 若且唯若

$$p \equiv (ab + bc + ca) \pmod{abc}。 \tag{5}$$

證明: 若已知 (5) 成立, 代入 $(**)$ 驗證即可。反過來, 若 $a$,$b$,$c$ 爲正質數, 且 $a < b < c$, 令

$$ab - p = cm, \tag{6}$$

$$bc - p = an, \tag{7}$$

$$ca - p = br。 \tag{8}$$

其中 $m, n, r$ 爲整數。不妨假設 $0 < p < abc$ 。我們可跟定理1一般證明

$$a|(b + m), \quad b|(a + m)。$$

因此令

$$m + a = yb, \tag{9}$$

可推出

$$a|(y + 1)。 \tag{10}$$

又從 (6) 知

$$cm < ab < ca,$$

所以 $m < a$, 代入 (9), 得

$$yb = a + m < 2a < 2b。$$

所以

$$y < 2。 \tag{11}$$

另外, 從 (6) 知

$$cm > -p > -abc,$$
$$m > -ab。 \tag{12}$$

代入 (9),

$$by > a - ab,$$

所以 $b(y + a) > a > 0$, 由此可知 $y > -a$, 與 (11) 合推出

$$a + 3 > y + a + 1 > 1。$$

但 $a|(y+a+1)$, 且 $a$ 爲質數, 因此, $y+a+1$ 等於 $a$ 或 $a + 2$

(A) 若 $y + a + 1 = a$, 則 $y = -1$, 代入 (9), $m = -a - b$。再代入(6), 得

$$p = ab + bc + ca。$$

(B) 若 $y + a + 1 = a + 2$, 則 $y = 1$, 由 (9) 和 (10) 得 $a = 2$, 和 $m = b - 2$, 代入 (6), 得

$$b(b - 4) < -p < 0,$$

得 $2 = a < b < 4$, 因此 $b = 3$ 。而$abc = 30$, 亦即

$$ab + bc + ca = 31 \equiv p \pmod{abc},$$

證畢。

引理 4: 若 $(a, b, c)$ 爲質數三元數, 則

$$ab + bc + ca < abc,$$

除非 $(a, b, c) = (2, 3, 5)$。

證明: 若 $a \geq 3$, 則上式顯然成立。若 $a = 2$, 則上式等價於:

$$2(b + c) < bc。 \tag{13}$$

若 $b \geq 4$, 則

$$2(b + c) < 4c < bc,$$

即 (13) 成立。

若 $b = 3$, 則 $2(b+c)-bc = 6-c < 0$ 除非 $c = 5$。

推論 5: 若 $p$ 爲正偶數, 則同餘式 $(**)$ 沒有質數三元組解 $(a, b, c)$ 使得 $0 < p < abc$。

證明: 設$(a, b, c)$ 是 $(**)$ 的質數三元數解, 且 $abc > p > 0$, 既然 $p$ 爲偶數,$(a, b, c) \neq (2, 3, 5)$。因此從定理3和引理 4, 得

$$p = ab + bc + ca。$$

但式子右邊恆爲奇數, 矛盾.所以 $(**)$ 沒有質數三元數解。

推論 6: 若 $p = 2k + 1$ 爲奇數, 其中 $k > 0$, 則 $(**)$ 沒有質數三元數解 $(a, b, c)$ 使得 $ab > k$。

證明: 設 $(a, b, c)$ 是 $(**)$ 的質數三元數解, 且 $ab > k$, 既然 $c > 4$, $abc > 4k >$

$p > 1$, 故 $(a, b, c)$ 不爲 $(2, 3, 5)$。因此引用引理4:

$abc > ab + bc + ca > 3ab > 3k > p > 1$。

這和定理3矛盾, 故 $(**)$ 沒有質數三元數解 $(a, b, c)$ 使得 $ab > k$。

例1: $p = 26$ 時, 既然最小質數三元數解爲 (2,3,5), 其乘積爲30。因此若 $(a, b, c)$ 是 $(**)$ 的質數三元數解, 必有 $abc > 26$, 由推論5知此解不存在。

例2: $p = 33$ 時, 則 $k = 16$, 由推論5知沒有質數三元數解 $(a, b, c)$ 使得 $ab > 16$, 考慮 $ab < 16$ 的不同組合, 有 $(a, b) = (2, 3), (2, 5), (2, 7)$ 或 $(3, 5)$ 代入 (5), 分別得:

$$5c + 6 = 33,$$
$$7c + 10 = 33,$$
$$9c + 14 = 33,$$
$$8c + 15 = 33。$$

導出 c 不是整數, 矛盾。因此結論 $p = 33$ 時, $(**)$ 沒有質數三元數解。

質數三元數解的個數也是個重要的問題。我們找出若干有兩個解, 甚至三個解的同餘式組。

例3: $p = 101$ 時, 則 (2,3,19),(2,5,13) 均爲解。

例4: $p = 211$ 時, 則 (2,3,41),(3,7,19) 均爲解。

例5: $p = 711$ 時, 則 $(2, 11, 53)$ , $(5, 11, 41)$ , $(7, 13, 31)$ 均爲解。

從以上例子得知, 若 $1 < p < 31$ 時, $(**)$ 沒有質數三元數解。當 $p$ 逐漸增加, 可能出現解的個數也相應增加。

最後指出若 $p = 2k + 1$ 爲負奇數, 且 $5-2k = 6-p$ 爲質數時, 則 $(2, 3, 5-2k)$ 是同餘式組的一個質數三元數解, 但此解也不一定是唯一的, 例如當 $p = -23$ 時,(2,3,29) 和 (2,5,11) 均爲解。

## 後言

我們感謝葉永南和黎景輝兩位老師的熱情指導和鼓勵。本文源自八十三年高雄區高中數學科學成就優異學生輔導實驗計劃的暑假輔導計劃。感謝國科會與教育部的支持。

## 參考文獻

1. 陳景潤著 初等數論 (I)、(II) 科學出版社 (北京),1978。
2. 八十一學年度高雄區高中數學科自然科學習成就優異學生輔導實驗研習班高二班講義之數論 (一), (二),(三)。

—本文作者羅春光任教於中山大學應數系, 洪劭軒和黃拓儒則分別就讀於高雄中學及屏東高中—