中國剩餘定理求解同餘式的進一步研究

王 淑 霞

一、前 言

高中數學第一冊有這樣的問題「自然數以 3 除餘 1，以 5 除餘 2，以 7 除餘 4，求此自然數的特殊解及通解」爲了方便，而且對高一學生來說並不難接受，因此在課堂上介紹了同餘符號及其性質，於是，上述問題可改寫爲「$n\equiv 1\ (mod\ 3)$, $n\equiv 2\ (mod\ 5)$, $n\equiv 4\ (mod\ 7)$」 實驗本裏介紹了一種解法，另外中國剩餘定理（又名孫子算法）是另一種解法，其詳細情形請同學們去看「科學月刊」社出版的數學選粹第一集「韓信點兵的故事」一文，讀過了之後再來繼續本文。如果詳細唸過之後，將會發現其定理中要求除數兩兩互質，對於不互質的情形，沒有提起，本文擬對不互質的情形詳細討論，以供同學們參考。

先看下面的兩個例子:

例 1: 求 $n\equiv 2\ (mod\ 4)$, $n\equiv 4\ (mod\ 6)$ 的解。

解: 除數不互質，不妨直接利用中國剩餘定理試試看:

step 1: 先找 $n_1\equiv 2\ (mod\ 4), n_1\equiv 0\ (mod\ 6)$ 得 $n_1=6$

step 2: 次找 $n_2\equiv 0\ (mod\ 4), n_2\equiv 4\ (mod\ 6)$ 得 $n_2=4$

則 $n_1+n_2=10$ 爲一特殊解，通解爲

$$n=10+[4,6]t=4+12t \quad t\in Z$$

例 2: 求 $n\equiv 3\ (mod\ 8)$, $n\equiv 5\ (mod\ 6)$

解: 除數不互質，不妨也直接用利中國剩餘定理看看:

step 1 先找 $n_1\equiv 3\ (mod\ 8), n_1\equiv 0\ (mod\ 6)$，則 n_1 無解。

例 2 中，孫子算法失效了，但顯然 11 是其一解，我們不禁要問:

⑴除數不互質的同餘式，什麼時候可以直接利用中國剩餘定理?

⑵除數不互質的同餘式，孫子算法又不適用時，到底有沒有解? 有解的話，又該怎麼辦? 是不是只好去用實驗本上的解法，別無他法了?

二、本 文

(一)

問題 1 的答案，經整理得如下定理 1，2，3，其中定理 1 是爲定理 2 舖路，定理 2 是爲定理 3 舖路，同學們唸的時候，不妨先唸定理 3，嘗試自己去證明，就可了解此三個定理的安排用意何在。

定理 1

$$\begin{cases} x\equiv a\ (mod\ m_1) \\ x\equiv 0\ (mod\ m_2) \end{cases} \text{有公解} \Longleftrightarrow (m_1, m_2)\mid a$$

證明: "⇒" ∵ $x\equiv a\ (mod\ m_1)$, $x\equiv 0\ (mod\ m_2)$ 有公解，故 $\exists t_1, t_2\in I$ 使

$$x-a=m_1t_1,\ x=m_2t_2$$

故

$$x=m_1t_1+a=m_2t_2,$$

即

$$m_2t_2-m_1t_1=a$$

故

$$(m_1, m_2)\mid a\ \#$$

"⇐" 設

$$(m_1, m_2)=d,\quad \because\ d\mid a$$

∴ $$\exists\, t \text{ 使 } a=dt$$

又 $\exists h, k\in I$ 使

$$m_1h+m_2k=d$$

兩邊同乘 t 得

$$m_1ht+m_2kt=dt=a$$

取 $x=a-m_1ht=m_2kt$，則

$$x\equiv a\ (mod\ m_1),\ x\equiv 0\ (mod\ m_2)。$$

定理 2：

$$\left\{\begin{array}{l} x\equiv a_1(mod\ m_1) \\ x\equiv 0\,(mod\ m_2) \\ \cdots\cdots\cdots\cdots \\ x\equiv 0\,(mod\ m_l) \end{array}\right. \text{有公解} \Longleftrightarrow (m_1,[m_2,\cdots,m_l])\mid a\text{。}$$

證明：由於

$$\left\{\begin{array}{l} x\equiv 0\,(mod\ m_2) \\ \cdots\cdots\cdots\cdots \\ x\equiv 0\,(mod\ m_l)\ l\geq 2 \end{array}\right. \Longleftrightarrow x\equiv 0\,(mod[m_2,\cdots m_l])$$

由定理 1 卽得證。

定理 3：

$$\text{解}\left\{\begin{array}{l} x\equiv a_1(mod\ m_1) \\ x\equiv a_2(mod\ m_2) \\ \cdots\cdots\cdots\cdots \\ x\equiv a_l(mod\ m_l) \end{array}\right.$$

證明：可以直接利用孫子算法求解

$$(m_1,[m_2,\cdots,m_l])\mid a_1$$
$$\Longleftrightarrow (m_2,[m_1,m_3,\cdots,m_l])\mid a_2$$
$$\cdots\cdots\cdots\cdots$$
$$(m_l,[m_1,m_2,m_3\cdots m_{l-1}])\mid a_l\text{。}$$

例 3：$n\equiv 3\,(mod\ 9),\ n\equiv 4\,(mod\ 10),\ n\equiv 6\,(mod\ 12)$

$\because (9,[10,12])\mid 3,\ (10,[9,12])\mid 4,\ (12,[9,10])\mid 6$

故可用孫子算法求 n 得

$$n=354+180t,\ t\in I$$

例 4：$n\equiv 4\,(mod\ 9),\ n\equiv 4\,(mod\ 10),\ n\equiv 2\,(mod\ 12)$

$\because\quad (9,[10,12])\nmid 4$

故本題不可直接用孫子算法求解。

習題：請同學們比較一下定理 3 與「科學月刊」該文的「中國剩餘定理」。

（二）

問題 2 的答案，經整理得如下的定理 4，5，6，7，8，同學們，不妨先唸完這些定理，再回頭來推想這些定理的安排及用途。

定理 4：若 $m=m_1m_2$ 且 $(m_1,m_2)=1$

$$\text{則 } x\equiv a\,(mod\ m)\Longleftrightarrow\left\{\begin{array}{l} x\equiv a\,(mod\ m_1) \\ x\equiv a\,(mod\ m_2) \end{array}\right.$$

證明："⇒"方向的證明並不難，請同學自己動手吧!

"⇐"$\because\quad x\equiv a\,(mod\ m_1),\ x\equiv a\,(mod\ m_2)$

$\therefore\qquad \exists t_1,t_2\in I$

使

$$x-a=m_1t_1,\ x-a=m_2t_2$$

故

$$m_1t_1=m_2t_2$$

故

$$m_1\mid m_2t_2$$

但

$$(m_1,m_2)=1$$

故

$$m_1\mid t_2$$

設

$$t_2=m_1t$$

則

$$x-a=m_2t_2=m_2m_1t$$

故

$$x\equiv a\,(mod\ m_1m_2=m)\text{。}$$

定理 5：$m\in I,\ m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_k^{\alpha_k}$，$p_i$ 爲質數，$i=1,\cdots,\ k$，則 $x\equiv a\,(mod\ m)\Longleftrightarrow x\equiv a\,(mod\ p_i^{\alpha_i})$，$i=1,2,\cdots,k$

證明：對 k 用數學歸納法

i) $k=2$，OK（由定理 4）

ii) 設 $k=l$ 時原式成立，則 $k=l+1$ 時，

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{l+1}^{\alpha_{l+1}}$$

令

$$m_1=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$$
$$m_2=p_{l+1}^{\alpha_{l+1}}$$

則

$$(m_1,m_2)=1$$

$$x\equiv a\,(mod\ m_1m_2)\Longleftrightarrow x\equiv a\,(mod\ m_i)\quad i=1,2$$

又由歸納法假設得

$x\equiv a\,(mod\ m_1)\Longleftrightarrow x\equiv a\,(mod\ p_i^{\alpha_i})$，$i=1,\cdots,l$ 故得

$x\equiv a\,(mod p_1^{\alpha_1}\cdots p_{l+1}^{\alpha_{l+1}})\Longleftrightarrow x\equiv a\ (mod\ p_i^{\alpha_i})$，$i=1,\cdots,l+1$

定理 6：p 爲質數，$\alpha\geq\beta$，則

$$\left\{\begin{array}{l} x\equiv a_1(mod\ p^{\alpha}) \\ x\equiv a_2(mod\ p^{\beta}) \end{array}\right. \text{有公解} \Longleftrightarrow a_1\equiv a_2(mod\ p^{\beta})$$

證明："⇒" $\because\quad \alpha>\beta$，$\therefore\quad p^{\alpha}=p^{\beta}\cdot p^{\alpha-\beta}$

又已知 $x\equiv a_1(mod\ p^{\alpha})$，故 $x\equiv a_1(mod\ p^{\beta})$

又因 $x\equiv a_2(mod\ p^{\beta})$，$\therefore\quad a_1\equiv a_2(mod\ p^{\beta})$

"⇐"先找 $x\equiv a_1(mod p^{\alpha})$ 之解，則其解必滿足

$$x\equiv a_1(mod\ p^{\beta})$$

又因

$$a_1 \equiv a_2 (mod\ p^{\beta})$$

故此解必滿足

$$x \equiv a_2 (mod\ p^{\beta})。$$

由定理 6 的證明過程知道，只要 $a_1 \equiv a_2 (mod\ p^{\beta})$， 則求 $x \equiv a_1 (mod\ p^{\alpha})$， $x \equiv a_2 (mod\ p^{\beta})$ 之公解，只要求 $x \equiv a_1 (mod\ p^{\alpha})$ 即可。把此結果寫成定理 7 。

定理 7：p 爲質數，$\alpha \geq \beta$ 且 $a_1 \equiv a_2 (mod\ p^{\beta})$

則求 $x \equiv a_1 (mod\ p^{\alpha})$, $x \equiv a_2 (mod\ p^{\beta})$ 之公解相當於求 $x \equiv a_1 (mod\ p^{\alpha})$ 之解。

綜合以上諸定理，得除數不互質時的孫子算法修正解法如下:

（一） 求 x 滿足 $x \equiv a_1 (mod\ m_1)$， $x \equiv a_2 (mod\ m_2)$, $(m_1, m_2) > 1$

解: ⑴將 m_1, m_2，分解因式得

$$m_1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k},\ m_2 = q_1^{\beta_1} \cdots q_l^{\beta_l}$$

⑵原式充要改寫爲

$$x \equiv a_1 (mod\ p_i^{\alpha_i}),\ x \equiv a_2 (mod\ q_j^{\beta_j})$$

其中 $i = 1, \cdots, k$, $j = 1, \cdots, l$ 。

⑶再看諸 p_i 與 q_j 相同者，譬如 $p_1 = q_1$，則對 $x \equiv a_1 (mod\ p_1^{\alpha_1})$, $x \equiv a_2 (mod\ q_1^{\beta_1})$兩式，比較 α_1, β_1 之大小， 不妨設 $\alpha_1 \geq \beta_1$， 則先檢查 $a_1 \equiv a_2 (mod\ q_1^{\beta_1})$ 成立否。若否，則原式無解; 若是， 則將此兩式取代 $x \equiv a_1 (mod\ p_1^{\alpha_1})$ 一式。

⑷經由⑶步驟的刪除工作後，餘下諸式的除數兩兩互質，當然就可安心使用孫子算法了。

（二） $x \equiv a_i (mod\ m_i)$ $i = 1, 2, \cdots, n$, $n > 2$

解: 與(一)′ $n = 2$ 情形的解法一樣，只是在看諸 m_i 的質因數有相同者時，可能不只兩個，例如 $p_1 = q_1 = r_1$ (其中 $p^{\alpha_1}, q^{\beta_1}, r_1^{t_1}$ 分別爲 m_1, m_2, m_3 之因數 p_1, q_1, r_1 爲質數)。則對 $x \equiv a_1 (mod\ p_1^{\alpha_1})$, $x \equiv a_2 (mod\ q_1^{\beta_1})$, $x \equiv a_3 (mod\ r_1^{t_1})$ 三式，應用 (一)′ 中的⑶法，先對兩式判斷有解與否，有解則可刪去指數較小者，餘下的一個再與第三式去刪。

由上述解法步驟中可知諸同餘式有解的充要條件， 如下定理。

定理 8： $x \equiv a_i (mod\ m_i)$, $i = 1, \cdots, l$,

有解 $\Longleftrightarrow a_i \equiv a_j (mod\ (m_i, m_j))\ \forall\ 1 \leq i \neq j \leq l$。

習題: 利用上述解法解下列各題。

1. $n \equiv 3 (mod\ 8)$, $n \equiv 5 (mod\ 6)$。
2. $n \equiv 3 (mod\ 12)$, $n \equiv 4 (mod\ 8)$, $n \equiv 2 (mod\ 9)$。
3. $n \equiv 3 (mod\ 4)$, $n \equiv 5 (mod\ 6)$, $n \equiv 8 (mod\ 9)$。

——本文作者現任教於新竹女中