同餘方程研究

教師組數學第一名

多山鄉武洲國小　　作　　者：李鐘榮

一、研究動機：

縱觀同餘方程理論的發展，雖已有十分輝煌的成就，但二次剩餘却還僅止於有無解的判別，而沒有良好的求解方法，有之，僅是以嘗試法，逐一代入求解（如李恭晴先生著整數論第61、61頁解$X \equiv 21 \mod 37$），或以逐步捨棄法，去其不可能數，以待數目較小，計算不太麻煩時，直接代入試驗得之（如數論導引第48頁，解$X \equiv 73 \mod 127$），這些方法在理論上，雖非站不住脚，但其不夠完美乃人盡皆知，尤其是數字一大，困難更是接踵而來；至於一次同餘式，目前更有多種形式的解法，那些理論雖稱完備，但其演算過程，都不夠單純明快，更由於不能一氣呵成，所以，也很難避免不必要的失誤，有鑑於此，而研究一次同餘式的連分解法，及中國餘數定理研究，以及二次剩餘的二次非剩餘解法和平方試驗法，這些方法及名稱，均爲作者自己假設，希望能彌補時下理論之不足，並願以此新的嘗試，爲您帶來一段思考的愉快時光。

二、第一部份：一次同餘方程的連分解法。

爲避免不必要的誤會，在此先敍述連分數之定義及幾個重要定理，以下均以此爲準。

定義1：分數

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\vdots+\cfrac{1}{a_N}}}}$$

$$=a_0+\frac{1}{a_1}+\frac{1}{a_2}\cdots\cdots\frac{1}{a_N}$$

$$=[a_0, a_1, \cdots\cdots a_N]$$

謂之有限連分數（ finite, continued fraction ），如果a_0爲整數，a_1 ，a_2 ……a_N皆爲正整數，則稱爲簡單連分數，本文所討論僅限於簡單有限連分數，若〔 a_0 ，a_1 ……a_N 〕$=p_n/q_n$ ，其中p_n ，q_n 爲a_0 ，a_1 ……a_n之多項式，對任一a皆爲一次式，則p_n/q_n 名爲〔 a_0 ，a_1 ……a_n 〕之第n個漸近分數（ n-th convergent ），a_0 ，a_1 ，a_2 ……a_n 各爲其部分商。

定理 1 ：諸漸近分數有次之關係：

$$P_0=a_0 \quad , P_1=a_1a_0+1\cdots\cdots P_n=a_nP_{n-1}+P_{n-2}$$

$$q_0=1 \qquad q_1=a_1\cdots\cdots q_n=a_nq_{n-1}+q_{n-2} \quad 2\leq n\leq N$$

定理 2 ：P_n 及q_n 適合下列諸式

$$P_nq_{n-1}-P_n+q_n=(-1)^{n-1} \qquad n\geq 1$$

$$P_nq_{n-2}-P_{n-2}q_n=(-1)^{n-1}a_n \qquad n\geq 2$$

定理 3 ：凡簡單連分數之漸近分數，皆爲既約分數。

定理 4 ：凡有理數必可表爲有限簡單連分數，且其表法唯有兩種，而最後一項可以加以調整，使展開式的項數爲偶數或奇數以上諸定理及其證明，均見於數論有關書籍，不在法重述。

定理 5 ：$ax\equiv 1 \bmod m$ 之連分數解。

設 $(a,m)=1$ $\quad \dfrac{a}{m}=〔 a_0 , a_1\cdots\cdots a_n 〕$

$\dfrac{P_{n-1}}{q_{n-1}}=〔 a_0 , a_1\cdots\cdots a_{n-1} 〕$爲$\dfrac{a}{m}$之第$n-1$個漸近分數

則 $X\equiv q_{n-1}(-1)^{n-1} \bmod m$

證 明：由定理 4 ，可令$\dfrac{a}{m}=\dfrac{P_n}{q_n}=〔 a_0 , a_1\cdots\cdots a_n 〕$

由定理 3 知$(P_n , q_n)=(a , m)=1$ ，故得

$q_n=m \quad P_n=a$ 再由定理 2

$q_{n-1}P_n-P_{n-1}q_n=(-1)^{n-1}$ 代入立得

$aq_{n-1}-mP_{n-1}=(-1)^{n-1}$ 由同餘數定義知

$aq_{n-1} \equiv (-1)^{n-1} \mod n$　　顯然

$q_{n-1}(-1)^{n-1}$ 爲解，既 $X \equiv q_{n-1}(-1)^{n-1}$　故證。

定理6：若 $(a, m)=1$，　$ax \equiv b \mod m$　且

$ay \equiv 1 \mod m$ 則 $X \equiv by \mod m$

證　明：$ay \equiv 1 \mod m$，故 $a(by) \equiv b \mod m$

得　$X \equiv by \mod m$

例　1：解　$36865\ x \equiv 1 \mod 7167$

解：

	$a_0=$		$a_1=q_1$
	5	36865 | 7167	6
$q_2\ q_0\ q_1\ a_2$		35835 | 6·180	$a_3\ q_2\ q_1\ q_3$
$7=1+6\times1$		1030 | 987	$22\times7+6=160$
$q_4\ q_2\ q_3\ a_0$		987 | 946	$a_5\ q_4\ q_3\ q_5$
$167=7+160\times1$		43 | 41	$20\times167+160=3500$
	a_6	41 | 40	
	2	2 | 1	
		2	
		0	

得　$X \equiv 3500(-1)^5 \equiv -3500$

證　明：(1)先得 x 係數與模數輾轉相除，求得 $\frac{36865}{7167}$ 的連分數

$=[5, 6, 1, 22, 1, 20, 2]$

(2) $a_0=5$ 與分母無關，a_6 爲最後一個部分商，不計。

(3)如定理1所示法則

$q_0=1$　$q_2=a_2\times a_1+q_0=1+6\times1=7\cdots\cdots$

(4)以定理5所得解

例　2：$43676\times \equiv 13 \mod 867$

解：　先以例1方法解

$43676\ y \equiv 1 \mod 867$　　得

$y \equiv 125 \mod 867$

由定理6 $X \equiv 13y \mod 867$

$\equiv 13\times 125$

$\equiv 758$

三、第二部份：新中國餘數定理：設

$m_1, m_2 \cdots\cdots m_r$ 兩兩互質，則同餘組

$$\begin{cases} X\equiv b_1 & \mod m_1 \\ X\equiv b_2 & \mod m_2 \\ \vdots & \vdots \\ \vdots & \vdots \\ X\equiv b_r & \mod m_r \end{cases}$$

則模 $m_1, m_2 \cdots\cdots m_r$ 恰有一解，令 $M_i = \dfrac{m_1 m_2 \cdots\cdots m_r}{m_i} = \dfrac{m}{m_i}$

則此解爲 $(M_1+M_2+\cdots\cdots M_r)X \equiv (M_1 b_1 + M_2 b_2 \cdots\cdots M_r b_r)$ mod m之解。

證　明：由中國餘數定理知原同餘組恰有一解 X_0 模 m 此解顯然適合模 m 之各同義同餘組

$$\begin{cases} M_1 X\equiv M_1 b_1 & \mod m \\ M_2 X\equiv M_2 b_2 & \mod m \\ \vdots \quad \vdots & \vdots \\ \vdots \quad \vdots & \vdots \\ M_r X\equiv M_r b_r & \mod m \end{cases}$$

故得 $(M_1+M_2+\cdots\cdots M_r)X \equiv (M_1 b_1 + M_2 b_2 \cdots\cdots M_r b_r)$ mod m

而 X_0 爲上式之一解，因 m 之任一因數（∓ 1）均不爲 $(M_1+M_2+\cdots\cdots M_r)$ 之因數，故 X 之係數與模 m 互質，所以上式唯有一解，故得定理。

例：解 $\begin{cases} X\equiv 6 & \mod 7 \\ X\equiv 2 & \mod 3 \\ X\equiv 3 & \mod 5 \end{cases}$

解　1：利用中國餘數定理解法。

先解

$$\begin{cases} 3\times 5X_1 \equiv 6 \mod 7 \\ 7\times 5X_2 \equiv 2 \mod 3 \\ 7\times 3X_3 \equiv 3 \mod 5 \end{cases} \text{得} \begin{cases} X_1 \equiv 6 \\ X_2 \equiv 1 \\ X_3 \equiv 3 \end{cases}$$

得 $X \equiv 6\times 3\times 5+1\times 7\times 5+3\times 3\times 7 \mod 105$

$\equiv 83$

解 2：利用中國餘數定理研究的解法

化爲模 $7\times 3\times 5=105$ 之同義同餘組，得

$$\begin{cases} 15X \equiv 90 \mod 105 \\ 35X \equiv 70 \mod 105 \\ 21X \equiv 63 \mod 105 \\ 71X \equiv 223 \mod 105 \end{cases}$$

相加得 解之

得 $X \equiv 83 \mod 105$

以上兩種雖異曲同工，但第一種解法要解3次的同餘式，而解法2僅解一次，顯然單純得多，因此解2有別於中國餘數定理之解法，故名。

四、第三部分：二次剩餘的二次非剩餘解法

如同第一部分，先敍述幾個必要的定義和定理：（以下P均爲奇質數）。

定義1：m爲大於1之整數，且$(m, n)=1$

若 $X^2 \equiv n \mod m$ 可解，則稱n爲m之二次剩餘，不然爲二次非剩餘。

定義2：（Legendre Symbol） 設$(2a, p)=1$ 則

$$\left(\frac{a}{p}\right)=\begin{cases} 1 \text{若} a \text{爲} p \text{之二次剩餘} \\ -1 \text{若} a \text{爲} p \text{之二次非剩餘} \end{cases}$$

定理1：（Enler 判別法）設設$(2a, p)=1$ 則

$$a^{\frac{P-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

定理2：$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

定理3：互逆定律（Law of reciprocity）設P，q爲相異

奇質數，則$(\frac{P}{q})=(\frac{q}{P})(-1)$

定理4：$(\frac{-1}{P})(-2)^{\frac{P-1}{2}}$ 當 $P>2$

定理5：$(\frac{2}{P})=(-1)^{\frac{P^2-1}{8}}$ 當 $P>2$

定理6：$X^2\equiv 1 \bmod P$ 則 $X\equiv\pm 1 \mod P$

定義3：$X\equiv\pm 1 \bmod P$ 稱爲 $X^2\equiv 1 \bmod P$之同餘開方

定理7：1，2……$P-1$中恰有$1/2(P-1)$個二次剩餘，其餘爲二次非剩餘。

定理8：$X^2\equiv a \mod \mod P$的二次非剩餘解。

假設(1) $X^2\equiv a \mod P$有解，且$P=2^n(2^k+1)+1=2^n c+1$

(2) $A=\{1,2\cdots\cdots n-2,n-1\}$，$\phi_i$爲$A$之任意部分集合之各元素和，且空集合之元素和爲$\phi$。

(3) 令$2^{\phi_1}=0$

則對任意$(\frac{e}{P})\equiv -1$，恒存在$-\phi_i$使

$a^c e^{2\phi i c}\equiv 1 \mod P$

且 $X\equiv\pm a^{\frac{c+1}{2}} e^{\frac{2\phi i c}{2}}$

證 明：由定理7知恒有$(\frac{e}{P})\equiv -1$，任取其一，

令$a^c\equiv\alpha \mod P$ $e^c\equiv\beta \mod P$

由Enler 判別式

$a^{\frac{P-1}{2}}\equiv\alpha^{2^{n-1}}\equiv 1 \bmod P$ $\beta 2^{n-1}\equiv -1 \mod P$

爲簡便計，以下將符號mod P略去。

由$\alpha 2^{n-1}\equiv 1$經同餘開方得

若$\alpha 2^{n-2}\equiv -1$則得$\alpha 2^{n-1}\beta 2^{n-1}\equiv 1$，我們將此結果表示如下：

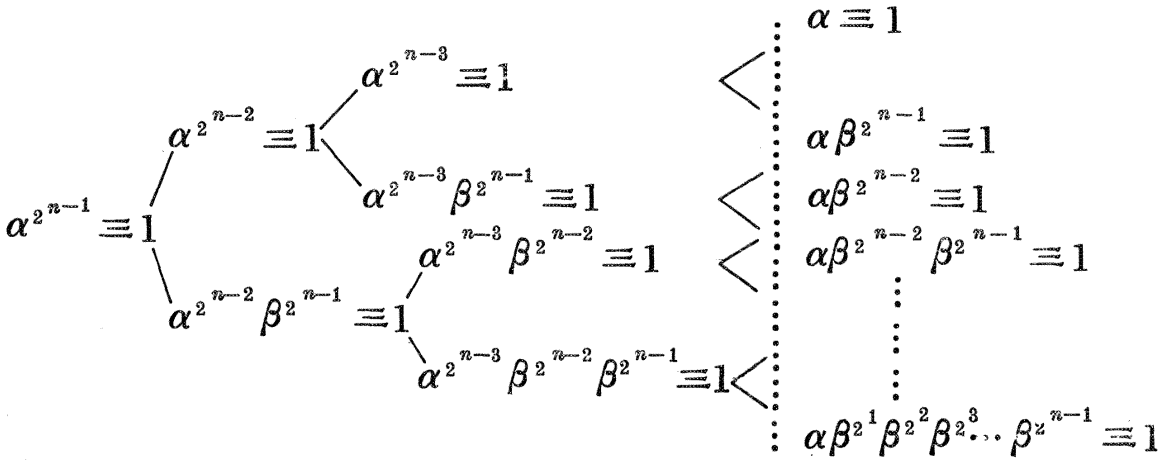
$$\alpha^{2^{n-1}} \equiv 1 \begin{cases} \alpha^{2^{n-2}} \equiv 1 & (1) \\ \text{或} \\ \alpha^{2^{n-2}}\beta^{2^{n-1}} \equiv 1 & (2) \end{cases}$$

再由(1)得$\alpha^{2^{n-3}} \equiv \pm 1$，如$\alpha^{2^{n-3}} \equiv -1$則$\alpha^{2^{n-3}}\beta^{2^{n-1}} \equiv 1$

再由(2)得$\alpha^{2^{n-3}}\beta^{2^{n-2}} \equiv \pm 1$，如果$\alpha^{2^{n-2}}\beta^{2^{n-2}} \equiv -1$則

$\alpha^{2^{n-3}}\beta^{2^{n-2}}\beta^{2^{n-1}} \equiv 1$

重覆以上的同餘開方法，可進行$n-1$次則之指數爲$1 = 2^0$，我們以「＜」表示同餘開方的步驟和結果。



由以上同餘開方$n-1$次之結果，共得2^{n-1}個同餘式，其中最少有一個成，而P之指數恰爲$2^{\phi i}$，而ϕi爲｛1，2，……$n-1$｝之任意部分集合之和之一，此乃明示定理的第一部分。

又當$\alpha\beta^{2\phi i} \equiv 1$亦即$a^c e^{2\phi ic} \equiv 1$

由於C爲奇數，$2^{\phi i}C$爲偶數，故$\frac{c+1}{2}$，$\frac{2^{\phi i}c}{2}$爲整數，

故得$a^{c+1}e^{2\phi ic} \equiv a$故

$$\left(a^{\frac{c+1}{2}}e^{\frac{2\phi ic}{2}}\right) \equiv a$$

顯然$X \equiv \pm a^{\frac{c+1}{2}}e^{\frac{2\phi ic}{2}} \mod P$

實際解法：我們並沒有必要逐一去嘗試β之每一指數之可能性，只要決定$\alpha^{n-j}\beta^{n-\phi i}$是$\pm 1$而捨去不能數，可決定演算方向。

例：$X^2 \equiv 5 \mod 4001$

解：$(\frac{5}{4001})=1$ 故原二次剩餘式有解，先任取一$(\frac{3}{4001})=-1$，又$4001-1=2^5\times125$，並計算一些備用數字。（以下符號mod 4001略去）

$5^{63}\equiv919$　　$\beta\equiv3^{125}\equiv3339$

$\alpha\equiv5^{125}\equiv70$　　$\beta^2\equiv2135$

$\alpha^2\equiv899$　　$\beta^4\equiv1086$

$\alpha^4\equiv-1$　　$\beta^8\equiv3102$

$\beta^{16}\equiv-1$

由$\alpha^4\equiv-1$　得$\alpha^4\beta^{16}\equiv1$　同餘開方得

$\alpha^2\beta^8\equiv899\times3102\equiv-(899\times899)\equiv-(\alpha^2)^2\equiv1$

再同餘開方得$\alpha\beta^4\equiv70\times1086\equiv1$　　即

$5^{1063}\beta^4\equiv1$　立得$(5^{63}\beta^2)^2\equiv5$

故　$X\equiv\pm5^{63}\cdot2135\equiv\pm1575$　mod 4001

五　第四部分：乘方試驗法

定理1：設$(a,m)=1$

且　$\frac{P_n}{q_n}$爲$\frac{a}{m}$之第n個漸近分數，則

$$\frac{a}{m}-\frac{P_n}{q_n}\leq\frac{1}{q_nq_{n+1}}$$

定理2：對任意$a<m$，m爲奇質數$(a,m)\equiv1$，恒存在$|\alpha|,|\beta|<\sqrt{m}$使$\alpha a\equiv\beta$ mod m

證　明：(1)當$a<\sqrt{m}$，則$1\cdot a\equiv$a mod m顯然成立。

(2)故$a>\sqrt{m}$，且$\frac{a}{m}=[a_0,a_1,a_2\cdots\cdots a_n]$爲簡單連分數，因$m$爲奇質數，故在其漸近分數中，可取分母$q_n<\sqrt{m}$，$q_{n+1}>\sqrt{m}$

再由定理1，知必有$|\frac{a}{m}-\frac{P_n}{q_n}|\leq\frac{1}{q_nq_{n+1}}$立得

$$\left|\frac{aq_n - mP_n}{mq_n}\right| \leq \frac{1}{q_n q_{n+1}} \quad \left|\frac{aq_n - mp_n}{m}\right| \leq \frac{1}{q_{n+1}}$$

故 $q_{n+1} \mid aq_n - mP_n \mid \leq m$，因 $q_{n+1} > \sqrt{m}$，故 $\mid aq_n - mP_n \mid < \sqrt{m}$

令 $aq_n - mP_n = \beta$ 則 $\mid \beta \mid < \sqrt{m}$，由同餘式之定義，得 $q_n a \equiv \beta \mod m$ 令 $q_n = \alpha < \sqrt{m}$，故得定理。

定理3（平方試驗法）：設 $X^2 \equiv a \mod P$ 有解，P 爲奇質數，則恒存在二數 $\mid \alpha \mid \mid \beta \mid < \sqrt{P}$ 使 $\alpha^2 a \equiv \beta^2 \mod P$ 且 X 爲 $\alpha X \equiv \pm \beta \mod P$ 之解

證　明：由定理2知對任意 X，恒有二數 $\alpha\beta < \sqrt{P}$ 使

$\alpha X \equiv \beta \mod P$ 故得 $\alpha^2 X^2 \equiv \beta^2 \mod P$

故　$\alpha^2 a \equiv \beta^2 \mod P$　故證

在較小數字的計算，就可用平方試驗法迅速求解，因爲我們在試驗時，僅以小於 $\sqrt{P}$ 之各數即可。

例：解 $X^2 \equiv 73 \mod 127$

解1：$\left(\frac{73}{127}\right) = 1$ 有解由定理3，知在小於 $\sqrt{127}$ 之正數必有二數 α、β 使 $73\alpha^2 \equiv \beta^2 \mod 127$

令　$73 \cdot 2^2 \equiv 38$

$73 \cdot 3^2 \equiv 73 \cdot (2+1)^2 \equiv 38 + 73 \times 4 + 73 \equiv 22$

$73 \cdot 4^2 \equiv 73 \cdot (3+1)^2 \equiv 22 + 73 \times 6 + 73 \equiv 25 \equiv 5^2$

故得 $4x \equiv \pm 5 \mod 127$

解之得 $X \equiv \pm 33 \mod 127$

解2：應用輾轉相除法

$2 = 1 + 1 \times 1$	73	127	1
$16 = 2 + 7 \times 2$	54	73	$3 \times 2 + 1 = 7$
	19	54	
	−6	57	
	25	−3	

故　$16X^2 \equiv 25(-1)^4 \bmod 127$ 得 $4X \equiv \pm 5$

解之　$X \equiv \pm 33$

讀者可比較數論導引第 48 頁解此題方法，將發現平方試驗法容易甚多。

評語：1. 對於複雜的同餘方程組研究出比較簡單的求解方法。

2. 利用教學之餘，潛心研究值得鼓勵。