分數符號在同餘方程之應用與展望

國小教師組數學科第二名

宜蘭順安國小　　　　　　　　　　　　作　　者：李鏞榮

一、研究過程與方法

同餘方程的理論，原本十分複雜，舉凡判別一個方程式是否有解；當有解時會有幾個解？該如何求解？這些問題至今仍難有終南捷徑，問其困難之所自，固是數論之對象，僅限於整數上面却也因而限制了討論的層面，即限制了使用符號的靈動性，更影響了思維的便利，常令人如霧中看花，難以清晰。

有感於此，自忖數論之對象固是整數，但探討過程却未必限於整數之上，我們何妨引進分數做爲討論的媒介，使整個討論過程，得以簡化和明朗，這個手段猶如下跳棋，綠色棋子雖不能停在紅色國裏，却仍可能經過紅色國一樣。是故：

跳出整數模子的窠臼，將是海濶天空。

引進分數符號，同餘方程的理論，有望花開朵朵。

二、分數符號的基本理論和應用

定義(一)(分數符號)：設 P 爲質數，$a \not\equiv 0 \mod P$，則方程式 $ax \equiv b \mod P$，同義於 $x \equiv \dfrac{b}{a} \mod P$；若且唯若存在一 x 滿足該式，則稱 $\dfrac{b}{a}$ 爲模 P 的分數符號，且稱 x 與 $\dfrac{b}{a}$ 對模 P 同餘，x 爲 $\dfrac{b}{a}$ 對模 P 之同餘數，$\dfrac{b}{a}$ 爲 x 對模 P 之分數符號。

以下所用的英文或希臘字母，均表示整數，P 爲質數，在沒有混淆的情形下，符號 mod P 將常省略。

定理1：每個質數模P的分數符號$\frac{b}{a}$，$a \not\equiv 0 \bmod P$，存在唯一對模P的同餘數X，使$X \equiv \frac{b}{a} \bmod P$。

證明：P為質數，$2(a, b)=1$，所以$ax \equiv \bmod P$ 有唯一解。

例(1)：$\frac{2}{3} \equiv 7 \bmod 19$

解 $\because 3 \times 7 \equiv 2 \bmod 19$

有關如何解分數符號$\frac{b}{a}$，或解 $ax \equiv b \bmod P$，請參考廿一屆全國科展；「同餘方程研究」。

定理2（乘法性質）：設$\frac{b}{a}$，$\frac{d}{c}$為質數模P之分數符號，則

$$\frac{b}{a} \cdot \frac{d}{c} \equiv \frac{bd}{ac} \bmod P .$$

證明：設 $X \equiv \frac{b}{a} \bmod P$，$Y \equiv \frac{d}{c} \bmod P$，故得

$ax \equiv b$，$cy \equiv d$，使 $ac\ xy \equiv bd \bmod P$.

由定義 $xy \equiv \frac{bd}{ac} \equiv \frac{b}{a} \cdot \frac{d}{c} \bmod P$.

定理3（加減性質）：設$\frac{b}{a}$，$\frac{d}{c}$為質數模P的分數符號，則

$$\frac{b}{a} \pm \frac{d}{c} \equiv \frac{bc \pm ad}{ac} \bmod P .$$

證明：設 $x \equiv \frac{b}{a}$，$y \equiv \frac{d}{c} \bmod P$，故得

$ax \equiv b \Rightarrow acx \equiv bc \quad \therefore ac(x \pm y) \equiv bc \pm ad \bmod P$

$cy \equiv d \Rightarrow acy \equiv ad$

$$\therefore \quad x \pm y \equiv \frac{b}{a} \pm \frac{d}{c} \equiv \frac{bc \pm ad}{ac} \bmod P$$

定理4：設$\frac{a}{c}$，$\frac{d}{b}$爲質數模P的分數符號，則 $ab \equiv cd \bmod P$

同義於$\frac{a}{c} \equiv \frac{d}{b} \bmod P$.

證明： $ab \equiv cd \bmod P$

$\Rightarrow \frac{ab}{c} \equiv d$ （定義㈠）

$\Rightarrow (\frac{a}{c})\, b \equiv d$ （定理2）

$\Rightarrow \frac{a}{c} \equiv \frac{d}{b}$ （定義㈠）

定理5（除法性質）：設$\frac{b}{a}$，$\frac{d}{c}$爲質數模P的分數符號，

$d \equiv 0 \bmod P$ 則 $\frac{b}{a} / \frac{d}{c} \equiv \frac{bc}{ad} \bmod P$.

證明：設 $X \equiv \frac{b}{a}$ 亦即 $ax \equiv b \bmod P$

$Y \equiv \frac{d}{c}$ $cz \equiv d$

故得 $acx \equiv bc$ $acy \equiv bd$

$acx / acy \equiv \frac{x}{y} \equiv \frac{bc}{ad} \equiv \frac{b}{a} / \frac{d}{c}$

定理6（約分擴分）：設$\frac{b}{a}$爲質數模P的分數符號，若

$c \equiv 0 \bmod P$ 則 $\frac{b}{a} \equiv \frac{bc}{ac} \bmod P$

證明：設　$x \equiv \frac{b}{a} \bmod P$　亦即　$ax \equiv b$　又　$c \not\equiv 0 \bmod P$

故得　$acx \equiv bc \bmod P$　　$x \equiv \frac{bc}{ac} \equiv \frac{b}{a} \bmod P$

定理7（帶分數性質）：設$\frac{b}{a}$爲質數模P的分數符號，且n爲整數，則　$n + \frac{b}{a} \equiv \frac{na+b}{a} \bmod P$

證明：令$X \equiv \frac{b}{a} \bmod P$　則　$X+n \equiv n + \frac{b}{a} \bmod P$

而得　$a(X+n) \equiv an+b \bmod P$　（定理4，6）

$X+n \equiv \frac{an+b}{a} \bmod P$　（定理4）

$\therefore \quad X+n \equiv n + \frac{b}{a} \equiv \frac{an+b}{a} \bmod P$

例(2)：解　$7X \equiv 27 \bmod 29$

解：　$X \equiv \frac{27}{7} \equiv 3 + \frac{6}{7} \bmod 29$　（帶分數）

$\equiv 3 + \frac{6 \times 4}{7 \times 4}$　（擴分）

$\equiv 3 + \frac{24}{-1}$　（分母$7 \times 4 \equiv -1 \bmod 29$）

$\equiv -21$

定理8（乘法反元素性質）：設$\frac{b}{a}$爲質數模P的分數符號，且

$b \not\equiv 0 \bmod P$，則$\frac{b}{a} \times \frac{a}{b} \equiv 1 \bmod P$

證明：$\frac{b}{a} \times \frac{a}{b} \equiv \frac{ba}{ab} \bmod P$　（乘法性質）

$$\equiv \frac{a\,b}{a\,b} \equiv 1$$

定理9：$\dfrac{b}{a}$為質數模P的分數符號，且 $b \not\equiv 0 \mod P$，

則 $\dfrac{b}{a} \equiv 1 \,/\, \dfrac{a}{b} \mod P$.

證明：由定理8立得

定義(二)（指數符號）：設$a \not\equiv 0 \mod P$，n為整數，P為質數

，則定義：$\dfrac{1}{a} \equiv a^{-1} \mod P$

$$\frac{1}{a^n} \equiv a^{-n} \mod P$$

$$a^0 \equiv 1 \mod P$$

定理10（指數定律）：設m，n為任意整數，P為質數，

$a \not\equiv 0 \mod P$ 則 $a^n \times a^m \equiv a^{m+n} \mod P$

$(a^n)^m \equiv a^{mn} \mod P$

證明：①若n，m為非負整數，則由乘法性質立得。

②若$n \geqslant 0$，$m < 0$，則

$$a^n \times a^m \equiv a^n \times \frac{1}{a^{|m|}} \equiv a^{n-|m|} \mod P \text{，又}$$

$$(a^n)^m \equiv (a^n)^{-|m|} \equiv a^{-n|m|} \equiv a^{nm} \mod P$$

相似的，可證其他：

由以上定理，可知模為質數的同餘式的分數符號，相互關係，有如一般的分數四則，及指數定律，所以，在運用上十分方便。

基本應用：

例(1)：解聯之同餘方程式：

$$\begin{cases} 5X \equiv 4Y - 6 \\ 3Y \equiv 2X - 1 \end{cases} \mod 37. \qquad \begin{matrix} ㄅ \\ ㄆ \end{matrix}$$

解：有了分數符號的便利，故引「代入消去法」解之

由 $X \equiv \dfrac{3Y+1}{2} \mod 37$ 代入ㄅ得

$$5\left(\frac{3Y+1}{2}\right) \equiv 4Y-6$$

$$15Y+5 \equiv 8Y-12$$

$$7Y \equiv -17$$

得
$$\begin{cases} Y \equiv -\dfrac{17}{7} \equiv -2-\dfrac{3}{7} \equiv -2-\dfrac{3\times 16}{7\times 16} \equiv -2-\dfrac{48}{1} \\ \equiv -13 \equiv 24 \mod 37 \\ X \equiv \dfrac{3\cdot(-13)+1}{2} \equiv \dfrac{-38}{2} \equiv -19 \equiv 18 \mod 37. \end{cases}$$

例(2)：化簡 $X \equiv 36^6 \mod 73$

解：底數 36 較大，乘方多次比較難算，故改用分數符號

因 $2\times 36 \equiv -1 \mod 73$

$\therefore \quad 36 \equiv -\dfrac{1}{2}$

故 $X \equiv 36^6 \equiv \left(-\dfrac{1}{2}\right)^6 \equiv \dfrac{1}{64} \equiv 8 \mod 73$

例(3)：設
$$\begin{cases} 73X \equiv 59 & & ㄅ \\ 83X \equiv 7Y & \mod 127 & ㄆ \\ 23Y \equiv 48Z & & ㄇ \end{cases}$$

求 Z 對模127之同餘數

解：由ㄅ $X \equiv \dfrac{59}{73} \mod 127$ 代入ㄆ得 $Y \equiv \dfrac{83}{7}X \equiv \dfrac{83\times 59}{7\times 73}$

$\mod 127$ 再代入ㄇ得 $Z \equiv \dfrac{23}{48}Y \equiv \dfrac{23\times 83\times 59}{48\times 7\times 73} \equiv -\dfrac{18}{17}$

$\equiv -1-\dfrac{1}{17} \equiv -1+30 \equiv 29 \mod 127$

例(4)：解 $X \equiv 32^{92} \bmod 97$

解：由Fermat定理知，$32^{96} \equiv 1 \bmod 97$

由指數定律，$32^{96-4} \equiv \dfrac{1}{32^4} \bmod 97$　又 $\dfrac{1}{32} \equiv -3 \bmod 97$

所以　$X \equiv (-3)^4 \equiv 81 \bmod 97$

這個例子可以推廣如下：

設 P 爲質數，$a \not\equiv 0 \bmod P$ 則 $a^k \equiv a^{Hk-p} \bmod P$

（由 $a^{p-1} \equiv 1 \bmod P$ 得 $a^k \equiv a^{Hk-p} \bmod P$）

(二)　次數最大公因數定理(一)

設 P 爲質數，$a \equiv 0 \bmod P$，且 $(P-1, m) = l$，又 $\dfrac{m}{P-1}$

之漸近分數爲 $\dfrac{P_0}{q_0}, \dfrac{P_1}{q_1} \cdots\cdots, \dfrac{P_{n-1}}{q_{n-1}}, \dfrac{P_n}{q_n} = \dfrac{m}{P_1}$ 使

$$a^{(-1)^{n-1}} q_{n-1} \equiv b \bmod P$$

則　(1) $\begin{cases} X^l \equiv b \bmod P \text{ 無解} \Rightarrow X^m \equiv a \bmod P \text{ 亦無解} \\ X^m \equiv a \bmod P \text{ 有解} \Rightarrow X^l \equiv b \bmod P \text{ 有相同之解} \end{cases}$ (2)

證明：

(1)由已知 $LP_n = m$，$Lq_n = P-1$，由連分數之定理知：

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

$$LP_n q_{n-1} - LP_{n-1} q_n = (-1)^{n-1} L$$

$$mq_{n-1} - (P-1) P_{n-1} = (-1)^{n-1} L$$

故若　$X^m \equiv a \bmod P$　則有 $X^{mq_{n-1}} \equiv a^{q_{n-1}} \bmod P$

而得　$X^{(p-1)p_{n-1} + (-1)^{n-1} L} \equiv a^{q_{n-1}}$ 由Fermat定理得

$X^{p-1} \equiv 1 \bmod P$

所以，$X^{(p-1)p_{n-1}} \equiv 1$　故 $X^{(-1)^{n-1} L} \equiv a^{q_{n-1}} \bmod P$

立得　$X^l \equiv a^{(-1)q_{n-1}} \equiv b \bmod P$。故得定理第一部分

(2) 若存在 X 使 $X^m \equiv a \bmod P$，則有

$(X^m)^{q_n} \equiv a^{q_n} \equiv X^{p_n l q_{n-1}} \equiv X^{p_n(p-1)} \equiv 1 \bmod P$，

再由定理第一部分知：恒存在　$X^l \equiv b \bmod P$ 則

$$X^{l\,p_n} \equiv X^m \equiv a^{(-1)^{n-1} q_{n-1} p_n} \equiv a^{(-1)^{n-1}(p_{n-1}q_n + (-1)^{n-1})}$$

$$\equiv a^{(-1)^{n-1} p_{n-1} q_n + 1} \bmod P$$

$$\equiv a^1 \equiv a$$　也就是 $X^l \equiv a^{(-1)^{n-1} q_{n-1}} \equiv b \Rightarrow$

$X^m \equiv a \bmod P$　定理得證。

這個定理告訴我們，一個質數模的同餘 m 次方程式，最多有 $(m,\ p-1)$ 個解或無解，但要注意　$X^m \equiv a$ 及 $X^l \equiv b \bmod P$　並不等價，因為 $X^l \equiv b \bmod P$ 之解未必為 $X^m \equiv a$ 之解，例如：設 $X^8 \equiv 4 \bmod 13$，則有 $X^4 \equiv 4^2 \bmod 13$，今 $2^4 \equiv 4^2 \bmod 13$，但 $2^8 \not\equiv 4 \bmod 13$ 。

故 $X^8 \equiv 4 \bmod 13$ 無解，（因 $4^3 \not\equiv 1 \bmod 13$，故若 $X^l \equiv b \bmod P$ 之解不為 $X^m \equiv a \bmod P$ 之解。

則 $X^m \equiv a \bmod P$ 無解。

下面這個定理將告訴我們，什麼情形之下，兩方程式等價。次數最大公因數定理㈡：

一切假設如次數最大公因數定理㈠，又當 $a^{q_n} \equiv a^{\frac{p-1}{l}}$

$\equiv a^{\frac{p-1}{(p-1,\ m)}} \equiv 1 \bmod P$，則 $X^l \equiv b \bmod P$ 同義於

$X^m \equiv a \bmod P$

證明：

1．$X^l \equiv b \bmod P$　無解　$\Rightarrow$　$X^m \equiv a \bmod P$，這個證明與㈠相同。

2．若 X 為 $X^l \equiv b \bmod P$ 之解，且 $a^{q_n} \equiv 1 \bmod P$

則有　$X^{l p_n} \equiv X^m \equiv a^{(-1)^{n-1}(p_{n-1} q_n + (-1)^{n-1})}$

$$\equiv a^{(-1)^{n-1} p_{n-1} q_n + 1} \equiv a \bmod P$$

故　X 為 $X^m \equiv a \bmod P$ 之解 。

推論(1)：設 $\alpha X^m = \beta \bmod P$，且 $\alpha \not\equiv 0 \bmod P$, $\frac{\beta}{\alpha} \equiv a \bmod P$，其餘假設如次數最大公因數定理（I），則有與定理相同之結果。

證明：$\alpha X^m \equiv \beta \bmod P \Rightarrow X^m \equiv \frac{\beta}{\alpha} \equiv a \bmod P$ 立得。

推論(2)：若 P 爲質數，$(P-1, m)=1$，則方程式 $X^m \equiv a \bmod P$ 之解爲 $X \equiv b \equiv a^{(-1)^{n-1} q_{n-1}} \bmod P$

證明：於次數最大公因數定理中，令 $l=1$，又當

$X \equiv a^{(-1)^{n-1} q_{n-1}} \bmod P \Rightarrow X^m \equiv a^{(-1)^{n-1} m q_{n-1}}$

$\equiv a^{(-1)^{n-1}[(p-1)p_{n-1}+(-1)^{n-1}]} \equiv a^1 \equiv a \bmod P$

這個推論，實質說明了 X 之次數與 $p-1$ 互質之同餘方程式，則恒有唯一解。

例ㄅ：解 $X^7 = 45 \bmod 73$

解 $(7, 73-1)=1$，而 $\frac{7}{72}$ 之漸近分數爲 $\frac{1}{10}$，$\frac{3}{31}$，$\frac{7}{72}$，得 $X^{7 \cdot 31} \equiv X^{3 \cdot 72+1} \equiv X \equiv 45^{31} \bmod 73$ 即 $X \equiv 45^{31} \bmod 73$ 爲解。

例ㄆ：$29X^8 = 123 \bmod 127$

解：$X^8 \equiv \frac{123}{29} \equiv 13 \bmod 127$，再由 $\frac{8}{126}$ 之漸近分數得

$X^{8\times 16} \equiv X^{2(63+1)} \equiv X^2 \equiv 13^8 \bmod 127$，故 $X \equiv \pm 13^4$

$\equiv \pm 14 \bmod 127$

但 $14^8 \equiv 34 \not\equiv 13$ 不爲方程式之解，故原方程式無解。

例ㄇ：$X^{14} \equiv 5 \bmod 97$

解：$X^{14 \cdot 7} \equiv X^2 \equiv 5^7 \equiv 40 \bmod 97$，但 $(\frac{40}{97}) = (\frac{8}{97})$

$$(\frac{5}{97}) = (\frac{2}{97})(\frac{5}{97}) = -1$$

故　方程式無解。

推論(3)：若 $(m,\ p-1)=1$，且 P 爲質數，若 $\{a_1, a_2 \cdots\cdots a_{p-1}\}$ 爲模 P 之完全剩餘系，若且唯若，$\{a_1^m,\ a_2^m,\ a_3^m \cdots\cdots a_{p-1}^m\}$ 亦爲模 P 之完全剩餘系。

證明：由推論(2)：方程式 $X_i^m \equiv a_i \bmod P$ 有唯一解，若 $a_i^m \equiv a_j^m \equiv K \bmod P$，則 $a_i \equiv a_j \bmod P$，又若 $a_i \equiv a_j$，則 $a_i^m \equiv a_j^m$，故 a_i 與 a_j^m $(1 \leqslant i,\ j \leqslant p-1)$，一一對應，定理得證。

㈢　判別定理：先證引理：

引理：設 $K \mid p-1$，K 爲正整數，P 爲質數，則方程式

$Y^k \equiv 1 \bmod P$　有 k 解。

證明：㈠若方程式多於 k 解，則與 lagrange　定理矛盾。

㈡若少於 k 解，且設其解之完全剩餘系爲

$\{Y_1,\ Y_2 \cdots Y_i\} = A$，$(1 < k)$。

由於 $(X^n)^k \equiv X^{p-1} \equiv 1 \bmod P$ 有 $P-1$ 個解，且其解之完全剩餘系爲 $\{1,\ 2,\ \cdots\cdots P-1\} = B$，則

$X^n \in A$ $(\because (X^n)^k = 1 \bmod P)$。

所以 $\{X_1^n \mid X_i \in B\} \subset A$，今方程

$$(1)\quad \begin{cases} X_1^n \equiv Y_1^1 \\ X_2^n \equiv Y_2 \\ \vdots \\ Y_{l_1}^n \equiv Y_1 \qquad 1 \leqslant l \end{cases} \bmod P$$

其解集合之聯集爲 $X^{p-1} \equiv 1 \bmod P$　之全部，但(1)中每一方程式至多有 n 個解，故 $X^{p-1} \equiv 1 \bmod P$　之解總數最多 $= ml < nk = P-1$，而得矛盾。

判別定理㈠：

設方程式　$\alpha X^n \equiv \beta \bmod P$，其中 P 爲質數，α，$\beta \not\equiv 0 \bmod P$ 且 $nk = P-1$，若且唯若 $\alpha^k \equiv \beta^k \bmod P$ 時，有 n 解，否則無解。

證明：

㈠必要條件：令$\frac{\beta}{\alpha} \equiv a \bmod P$，則原方程式可化爲

$X^n \equiv \frac{\beta}{\alpha} \equiv a \bmod P$，今若有一$X$存在，使方程成立，則有

$(X^n)^k \equiv a^k \equiv X^{p-1} \equiv 1 \bmod P$，故得 $\alpha^k \equiv \beta^k \bmod P$。

㈡充分條件：若$\alpha^k \equiv \beta^k \bmod P$，則有 $a^k \equiv 1 \bmod P$
由於$Y \equiv a \bmod P$ 爲$Y^k \equiv 1 \bmod P$之一解，再由引理知
$Y^k \equiv 1 \bmod P$ 有 k解，令其解之完全剩餘系爲$\{Y_1, Y_2 \cdots\cdots Y_k\} = A$，則$a \in A$，由此得$k$個方程式。

$$(2)\quad \left\{\begin{array}{l} X_1^n \equiv Y_1 \\ X_2^n \equiv Y_2 \\ \vdots \\ X_i^n \equiv a \\ \vdots \\ X_k^n \equiv Y_k \end{array}\right. \qquad \bmod P$$

但之所有方程之解爲$X^{p-1} \equiv 1$ 之解的全部，Ⅱ 的每一方程式之解若有少於n解者，其解總數將少於$nk = P-1$，所以$X_i^n \equiv a$ 之解亦有n個，乃得定理。

推論：Euler判別法：若P爲一奇數質，$a \not\equiv 0 \bmod P$則 $a^{\frac{p-1}{2}}$

$$= \left(\frac{a}{p}\right) \bmod P，其中\left(\frac{a}{p}\right)爲\text{Legendre}符號$$

證明：令$m = 2$立得

Euler 判別法，實爲判別定理之一例。

例1：判別$X^6 \equiv 7 \bmod 19$有無解。

解：$6 \times 3 = 19 - 1$ 而$7^3 = 1 \bmod 19$故方程式有6解。

例2：判別 $47X^{28} \equiv 19 \bmod 113$

解：$113 - 1 = 28 \times 4$ 而 $47^4 \equiv 2 \bmod 113$

$19^4 \equiv 32$

$47^4 \not\equiv 19^4 \bmod 113$故方程式無解

判別定理(二)：

設 $\alpha X^m = \beta \bmod P$，$P$為質數，$\alpha$，$\beta \not\equiv 0 \bmod P$，

$(m, P-1)=1$，若且唯若，$\left[\frac{\beta}{\alpha}\right]^{\frac{p-1}{l}} \equiv 1 \bmod P$，則方程式有解

，否則無解。

證明：設 $\frac{m}{P-1}$ 之漸近分數為 $\frac{p_1}{q_0}$，$\frac{p_1}{q_1}$……$\frac{p_{n-1}}{q_{n-1}}$，$\frac{p_n}{q_n} = \frac{m}{P-1}$；

則 $q_n = \frac{P-1}{l}$，令 $\frac{\beta}{\alpha} \equiv a \bmod P$，則當 $a^{q_n} \equiv 1 \bmod P$ 時，由次

數最大公因數定理Ⅱ知：方程式同義於 $X^l \equiv a^{(-1)^{n-1} q_{n-1}} \equiv b \bmod P$

而 $b^{\frac{p-1}{l}} \equiv b^{q_n} \equiv a^{(-1)^{n-1} q_{n-1} q_n} \equiv 1 \bmod P$，由判別定理1知方

程式有 l 解。

若有 X 使 $X^m \equiv a \bmod P$，則 $(X^m)^{q_n} \equiv a^{q_n} \equiv X^{p_n(p-1)}$

$$\equiv 1 \bmod P$$

定理得證：

例3：判別 $7X^{115} \equiv 3 \bmod 139$ 之解

解：因 $(115, 139-1)=23$ 故先降 X 之次數為23，得

$X^{115} \equiv X^{-23} \equiv \frac{3}{7} \bmod 139$ 故 $X^{23} \equiv \frac{7}{3} \bmod 139$

今 $139-1=23\times 6$，而 $\left[\frac{7}{3}\right]^6 \equiv \frac{54}{64} \not\equiv 1 \bmod 139$，故方程式無

解。

例4：判別 $29X^8 \equiv 123 \bmod 127$ 之解

解：$X^8 \equiv \frac{123}{29} \equiv 13 \bmod 127$，而 $\frac{126}{(8, 126)} \equiv 63$

$13^{63} \equiv \frac{97}{13} \not\equiv 1 \bmod 127$，故方程式無解。

(四) 秩數定理：

若a對質數模P之秩數（Rank）爲n，且$n|P-1$，則 $X^n \equiv 1 \bmod P$ 之解爲$X \equiv 1$，a，$a^2 \cdots\cdots a^{n-1} \bmod P$

證明：由前定理知$X^n \equiv 1 \bmod P$ 有n解，設其解之完全剩餘系爲 $A = \{ a_i \,|\, X \equiv a_i \bmod P \}$，又設$a^i$ 對模P之完全剩餘系爲 $B = \{ x_i \,|\, X_i \equiv a^i \bmod P \}$，其中$1 \leqslant X_i \leqslant P-1$，$1 \leqslant i \leqslant n$，則有$(X_i)^n \equiv (a^i)^n \equiv (a^n)^i \equiv 1 \bmod P$， 故 $X_i \in A$，亦卽$B \subset A$，又由秩數之定義，知B中無相同元素，其元素有n個，而A中亦僅有n個不同元素，故知A之元素亦爲B之元素，所以$A = B$，定理得證。

推論 1：設g爲P之一原根（Primitive Root）則$X^n \equiv 1 \bmod P$ 之諸解爲$X \equiv 1$，g^k，$g^{2k} \cdots\cdots g^{(n-1)k}$ mood P。其中P爲質數，且$nk = P-1$。

證明：由原根之定義g^1，g^2，$\cdots\cdots g^{p-1}$ 對模P無同餘者，而 $(g^{ik})^n \equiv g^{i(p-1)} \equiv 1 \bmod P$，故$g^{ik} \equiv X \bmod P$ 爲方程之一解。而g^k，g^{2k}，$\cdots\cdots g^{nk}$， 對模P均不同餘，其中$g^{nk} \equiv 1 \bmod P$，故g^k 之秩數爲n，可得推論。

推論 2：設α，$\beta \not\equiv 0 \bmod P$，$P$爲質數，而$X \equiv f \bmod P$ 爲 $\alpha X^n \equiv \beta \bmod P$ 之一解，g之秩數爲n，則其全部解爲 $X \equiv f$，fg，fg^2，$\cdots\cdots fg^{n-1} \bmod P$。

證明：若$\alpha f^n \equiv \beta \bmod P$，且$g^n \equiv 1 \bmod P$
則 $\alpha(fg^i)^n \equiv \alpha f^n g^{in} \equiv \alpha f^n \equiv \beta \bmod P$，所以$fg^i \equiv X$亦爲其一解，但$f$，$fg$，$fg^2$，$\cdots\cdots fg^{n-1}$皆不同餘，可得$n$解，而無其他。

例1：7爲$5X^6 \equiv 19 \bmod 37$ 之一根，試求其他諸根。

解：2爲37之一原根，故2^6之對模37之秩數爲$\frac{37-1}{6} = 6$，由推論 2 知，其他各解爲：

$X \equiv 7$

$X \equiv 7 \times 2^6 \equiv 4$

$X \equiv 7 \times 2^{12} \equiv 34$

$$X \equiv 7 \times 2^{18} \equiv 30$$
$$X \equiv 7 \times 2^{24} \equiv 33$$
$$X \equiv 7 \times 2^{30} \equiv 3$$

(五) $\alpha X^k \equiv \beta \bmod P$ 之解法(一)：

設 $\alpha X^k \equiv \beta \bmod P$ 中，P 爲質數，α，$\beta \not\equiv 0 \bmod P$，且 $\left(\frac{\beta}{\alpha}\right)^l \equiv 1 \bmod P$，$kl \mid P-1$，若 $(k, l)=1$，且 $\frac{l}{k}$ 之漸近分數爲 $\frac{p_0}{q_0}$，$\frac{p_1}{q_1}$，$\cdots\cdots \frac{p_{n-1}}{q_{n-1}}$，$\frac{p_n}{q_n}=\frac{l}{k}$，則 $X \equiv \left[\frac{\beta}{\alpha}\right](-1)^n p_{n-1} \bmod P$ 爲其一解。

證：$k\ l \mid P-1 \Rightarrow \left[\frac{\beta}{\alpha}\right]^k \equiv 1 \bmod P$ 故方程有解，又 $(k, l)=1$

$\therefore P_n = l$，$q_n = k$，今由連分數之定理得 $lq_{n-1}-p_{n-1}k=(-1)^{n-1}$ 使

$(-1)^n l q_{n-1}+1=(-1)^n p_{n-1} k$

今 $\left[\frac{\beta}{\alpha}\right]^l \equiv 1 \bmod P$ 故 $\left[\frac{\beta}{\alpha}\right](-1)^n q_{n-1}+1 \equiv \frac{\beta}{\alpha}$

$$\equiv \left[\frac{\beta}{\alpha}\right](-1)^n p_{n-1} k \bmod P$$

故 $\left(\left[\frac{\beta}{\alpha}\right](-1)^n p_{n-1}\right)^k \equiv \frac{\beta}{\alpha} \bmod P$ 而得定理。

這個定理實質上是說明：若 $(k, l)=1$，則不定方程式 $l\,y+1=KZ$，可利用漸近分數解之，而得方程式之解。

例1：解 $X^{17} \equiv 100 \bmod 239$

解：因 $17 \times 14 = 239-1$，又 $100^7 \equiv 1 \bmod 239$，因 $7 \mid 239-1$，所以方程式有解（或以判別式 $100^{14} \equiv 1 \bmod 239$ 亦同），又 $(7, 17)=1$ 今 $\frac{7}{17}$ 之漸近分數爲 $\frac{1}{2}$，$\frac{2}{5}$，$\frac{5}{12}$，$\frac{7}{17}$ 故得 $100 \equiv 100^{7\times 12+1} \equiv 100^{5\times 17} \equiv (100^5)^{17} \bmod 239$

所以 $X\equiv 100^5\equiv 42 \bmod 239$ 爲方程式之一解，又7亦爲模 239 之原根，故其解集合爲 $\{X\equiv 42\times 7^{14i} \bmod 239 \mid 0\leqslant i \leqslant 16\}$。

例2：解 $19X^{69}\equiv 453 \bmod 461$

解： $X^{69}\equiv \dfrac{453}{19}\equiv 315 \bmod 461$，又 $(461-1, 69)=23$

由於 $315^{\frac{461-1}{23}}\equiv 315^{20}\equiv 1 \bmod 461$，由判別定理知方程式有解。今 $\dfrac{69}{460}$ 之漸近分數爲 $\dfrac{1}{6}$，$\dfrac{1}{7}$，$\dfrac{3}{20}=\dfrac{69}{460}$，再由次數最大公因數定理化爲同義方程式得 $X^{69\times 7}\equiv X^{23}\equiv 315^7\equiv 252 \bmod 461$

$\because$ $252^{20}\equiv 315^{7\times 20}\equiv 1 \bmod 461$，而 $(20, 23)=1$，再解

$20y+1=23z$，得 $y=8$，$z=7$，故得

$252\equiv 252^{20\times 8+1}\equiv 252^{7\times 23}\equiv (252^7)^{23} \bmod 461$

令 $X\equiv 252^7\equiv 60 \bmod 461$ 爲其一解。今2爲模461之原根，故得 2^{20} 對模461之秩數爲23，其餘諸解爲

$X\equiv 60$，60×2^{20}，$60\times 2^{40}\cdots\cdots 60\times 2^{440} \bmod 461$

當 $(k, l)\neq 1$ 時，我們有下列定理可解。

$\alpha X^k\equiv\beta \bmod P$ 之解法(二)

設 $\alpha X^k\equiv\beta \bmod P$，$P$ 爲質數，α，$\beta\neq 0 \bmod P$ 且 $n=lkj=P-1$，$\left(\dfrac{\beta}{\alpha}\right)^l\equiv 1 \bmod P$，若 g 爲 P 之一原根，則於 $X\equiv g^j$，g^{2j}，$\cdots\cdots g^{lj} \bmod P$ 中有一解。

證明：因 $k\mid P-1$，故方程式有解，又 $\left(\dfrac{\beta}{\alpha}\right)^l\equiv 1 \bmod P$

故爲 $y^l\equiv 1 \bmod P$ 之一解，由秩數定理之推論2，

$Y\equiv g^n, g^{2n}\cdots\cdots g^{ln} \bmod P$，則必有 $\dfrac{\beta}{\alpha}\equiv g^{in}\equiv (g^{ij})k \bmod P$

$(1\leqslant i\leqslant l)$，故得 $X\equiv g^{ij} \bmod P$ 爲其一解。

例1：解 $X^{10}\equiv 48 \bmod 61$

解1：$48^6 \equiv 1 \mod 61$　故原方程式有解，但$(6,10)=2 \neq 1$　故不能用（Ⅰ）的解法（也就是$6Y+1=10Z$　無解）今2爲模61之一原根，而$61-1=6\times10$，故$X^{10}\equiv 48\equiv Y$爲$Y^6\equiv 1 \mod 61$之一解，所　$48\equiv 2^{10}, 2^{20}, 2^{30}\cdots\cdots 2^{60} \mod 60$之一，經過試驗得知$2^{10}\equiv 48$，故$X\equiv 2 \mod 61$爲其一解，全部解

$$X\equiv 2, 2^7, 2^{13}, 2^{19}, 2^{25}, 2^{31}, 2^{37}, 2^{43}, 2^{49}, 2^{55} \mod 61$$
$$\equiv 2, 6, 18, 54, 40, -2, -6, -18, 7, 21$$

解2：$48^6\equiv 1 \mod 61$

令$(X^2)^5\equiv Y^5 \mod 61$（Ⅱ），則$(5,6)=1$　故解法Ⅰ可用。

今解　$6k+1\equiv 5$，則$k\equiv -1$，$l\equiv -1$，而得

$$48\equiv 48^{6\times(-1)+1}\equiv(48^{-1})^5，故Y\equiv\frac{1}{48}\equiv 14 \mod 61$$

爲Ⅱ之一解，Ⅱ的全部解爲$Y\equiv 14, 14\times2^{12}, 14\times2^{24}, 14\times2^{36}, 14\times2^{48} \mod 61$，再解$X^2\equiv 14 \mod 61$，利用平方試驗法（參觀廿一屆科展同餘方程研究）

得　$3^2\times14\equiv 2^2 \mod 61$　即　$3X\equiv\pm2 \mod 61$　得

$$X\equiv\pm\frac{2}{3}\equiv\pm 21 \mod 61$$

而其他各解爲$X\equiv\pm21\times2^6$，$\pm21\times2^{12}$，$\pm21\times2^{18}$，$21\times2^{24} \mod 61$.

三、附　　記

㈠完全剩餘系：設S爲整數Z之集合，P爲正整數，若

(1) $\forall c\in Z$，$\exists a\in S \Rightarrow a\equiv c \mod P$

(2) $a, b\in S$，$a\neq b \Rightarrow a\not\equiv b \mod P$

則S爲模P之一完全剩餘系。

㈡秩數：令$m\in$正整數Z，a爲整數，令$M_a=\{n\in Z \mid a^n\equiv 1 \mod m\}$，若$k$爲$M_a$之最小元素，則稱$k$爲$a$對模$m$之秩數。

㈢原根：令P爲質數，$P-1$爲a對模P之秩數，則a爲P之原

根。

四、回顧與展望

在這篇論文中，作者首先引進了分數符號，使一次同餘方程式之應用更覺方便，並由此基礎，確立了指數的意義，再引連分數的理論，成功的證明了「次數最大公因數定理」，可將高次的方程式，降為與質數模 $P-1$ 之最大公因數來討論，這對作者來說，是十分難以忘懷的創見，因為這個定理的發現過程十分曲折，而且證明亦不易，效用也十分廣泛。

接着，又證明了判別定理，吸收了Euler 判別法；尤其是判別定理(二)，更將判別法的理論，擴張至X的次數非質數模$P-1$之因數，亦為作者所雀躍之作。

再次證明了秩數定理，使方程式得由一解而推至其他。

最後，作者提出了兩種同餘方程之解法，使整個同餘方程式，更臻於完備。

以上這些微所得，為作者歷盡辛勞而創獲，然而，學無止境，作者希望能將分數符號之應用層面更擴大，引進根式符號，如$X\equiv\sqrt{a} \mod P$及 Fourier 分析求發展同餘式一直為作者所鑽研，展望成果更豐碩，對前賢之賜教，有厚望焉。

評語：1.作者在數論方面下很多功夫研究，所得的結論雖然不是完全創新，但以國小教師所受的訓練而言，誠屬難可貴。

2.作者所受的數學基本訓練尚少，若能得專家的指導，從事進修，將來應有更大的成就。

3.作者表示對於數學研究很有興趣，進修之慾望很高，但限於在鄉下任教，苦無進修機會，尋找參考資料他很困難。若有可能，作者希望得到進修的安排與輔導。