

中華民國第四十五屆中小學科學展覽會
作品說明書

高中組 數學科

佳作

040422

作品名稱：滿足 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m}$ ， $(m,n)=1$ ， $\forall k$ 恆有解

$(x_1, x_2, \dots, x_n)$ 且 $0 < a_i < m$ 的數對 $(a_1, a_2, \dots, a_n)$ 之條件及組數 $f_n(m)$

的下界估計

臺北市立建國高級中學

作者姓名：

高二 劉奕賢

指導老師：

李瑞

中華民國第 45 屆中小學科學展覽會
作品說明書

科 別：數學科

組 別：高中組

作品名稱：滿足 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m}$, $(m,n)=1$, $\forall k$ 恆有解

$(x_1, x_2, \dots, x_n)$ 且 $0 < a_i < m$ 的數對 $(a_1, a_2, \dots, a_n)$ 之條件及組數 $f_n(m)$

的下界估計

關 鍵 詞：同餘、中國剩餘定理、歐拉函數（最多三個）

編 號：

製作說明：

- 1.說明書封面僅寫科別、組別、作品名稱及關鍵詞。
- 2.編號由國立臺灣科學教育館統一編列。
- 3.封面編排由參展作者自行設計。

滿足 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m}$, $(m, n) = 1$, $\forall k$ 恆有解 $(x_1, x_2, \dots, x_n)$ 且

$0 < a_i < m$ 的數對 $(a_1, a_2, \dots, a_n)$ 之條件及組數 $f_n(m)$ 的下界估計

註：本篇文中所用之運算全為剩餘系中之運算，在未說明的情況下，

a, b, c, d, r, m, n, t 表常數(為自然數)， p 表質數， x, y 表變數， x_i, y_i 表數值， $\{ax^n + b\}_p$

表示模 p 的 n 次剩餘系乘以常數 a 後，再加上常數 b

貳、研究動機

因為讀數論的同餘方程時，看到許多一元二次同餘方程的解法，又在不定方程中遇到 $ax^2 + by^2 = k$ 這樣的題目，使我開始思考這個問題。

參、研究目的

一 $ax \equiv k \pmod{m} \quad \forall k$ 恆有解時\

a 需滿足的條件及 a 的個數

二 $ax^2 + by^2 \equiv k \pmod{m} \quad \forall k$ 恆有解時

(a, b) 需滿足的條件及 (a, b) 的個數

三 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m} \quad \forall k$ 恆有解時

$(a_1, a_2, \dots, a_n)$ 需滿足的條件及 $(a_1, a_2, \dots, a_n)$ 的個數

肆、符號解釋

一 $\varphi(m)$ ：表示小於 m 且與 m 互質的數的個數

二 $\{x^n\}$ ：表示模 p 的 n 次剩餘系

三 $\{ax^n\}$ ：表示模 p 的 n 次剩餘系乘以常數 a

四 $f_n(m)$ ：表示 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m} \quad \forall k$ 恆有解時

數對 $(a_1, a_2, \dots, a_n)$ 的個數

伍、使用定理

一 鴿籠原理：將 $a+1$ 個數分為 a 組，必有兩個數同組

二 中國剩餘定理：對任意數對 $(c_1, c_2, \dots, c_n, p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_n^{\alpha_n})$

總存在唯一的 $0 \leq c < \prod_{i=1}^n p_i^{\alpha_i}$

滿足 $c \equiv c_i \pmod{p_i^{\alpha_i}}$

三 若 $0 \in A, 0 \in B, C = \{x + y \mid x \in A, y \in B\}$ ，則 $|C| \geq \min\{|A| + |B| - 1, p\}$

四 設 $f(x)$ 為多項式

若 $f(t) = k' \equiv k \pmod{p^n}, (p, f'(t)) = 1$ ，則 $f(ap^n + t) \equiv k \pmod{p^{2n}}$

(定理三、四證明寫於附錄中)

陸、研究內容

一 $ax \equiv k(\text{mod } m)$

顯然 $\forall k$ 有解之條件為 $(a, m) = 1$

所以 a 有 $\varphi(m)$ 個

即 $f_1(m) = \varphi(m)$

二 $ax^2 + by^2 \equiv k(\text{mod } m)$

(一) $m = p$

上式移項得 $by^2 \equiv k - ax^2(\text{mod } p)$

因 p 的二次剩餘系有 $\frac{p+1}{2}$ 個元素

所以 $\{by^2\} \{k - ax^2\}$ 都有 $\frac{p+1}{2}$ 個元素

若 $by^2 \equiv k - ax^2(\text{mod } p)$ 無解 (x, y)

則 p 的完全剩餘系至少有 $\frac{p+1}{2} + \frac{p+1}{2} = p+1$ 個元素

但 p 的完全剩餘系只有 p 個元素 矛盾

所以 $\forall a, b \quad ax^2 + by^2 \equiv k(\text{mod } p)$ 恆有解 (x, y)

(a, b) 有 $(p-1)^2$ 組

$f_2(p) = (p-1)^2 = \varphi(p)^2$

(二) $m = p^t, t \in \mathbb{N}$

若 $(a, p) \neq 1$ 則 $(a, p) = p$

$ax^2 + by^2 \equiv k(\text{mod } p^t) \Rightarrow ax^2 + by^2 \equiv k(\text{mod } p)$

$\because (a, p) = p \quad \therefore by^2 \equiv k(\text{mod } p)$ 恆有解 明顯矛盾

$\therefore (a, p) = (b, p) = 1$

若 $x^2 \equiv y^2(\text{mod } p^t) \Leftrightarrow x \equiv y(\text{mod } p^t)$ 或 $x \equiv -y(\text{mod } p^t)$

設 $(x, p) = (y, p) = 1$

則 $\{x^2\}$ 有 $\frac{\varphi(p^t)}{2} = \frac{p-1}{2} \times p^{t-1}$ 個元素

$\because x^2 \equiv k(\text{mod } p^t) \Rightarrow x^2 \equiv k(\text{mod } p)$

p 的二次剩餘系扣掉 0 後有 $\frac{p-1}{2}$ 個元素

$\therefore \{x^2\} = \{\alpha p + \beta \mid \alpha \in \mathbb{N}, \beta \equiv c^2(\text{mod } p), (\beta, p) = 1\}$

$\therefore \{ax^2\} = \{\alpha p + \beta \mid \alpha \in \mathbb{N}, \beta \equiv ac^2(\text{mod } p), (\beta, p) = 1\}$

$\therefore ax^2 + by^2 \equiv k(\text{mod } p^t)$ 恆有解 $\Leftrightarrow ax^2 + by^2 \equiv k(\text{mod } p)$ 恆有解

$ax^2 + by^2 \equiv 0(\text{mod } p)$ 有非 $(0, 0)$ 的解

又 $ax^2 + by^2 \equiv 0(\text{mod } p)$ 有非 $(0, 0)$ 的解時

可分為 $p = 4k+1$ 和 $p = 4k-1$ 來討論

$p = 4k+1$ 時

$\because x^2 + y^2 \equiv 0(\text{mod } p)$ 有解

$\therefore ax^2 + by^2 \equiv 0 \pmod{p}$ 有解 $\Leftrightarrow a, b \in \{x^2\}$ 或 $a, b \in \{x\} - \{x^2\}$

$p = 4k - 1$ 時

$\therefore x^2 + y^2 \equiv 0 \pmod{p}$ 無解

$\therefore ax^2 + by^2 \equiv 0 \pmod{p}$ 有解 $\Leftrightarrow a \in \{x^2\}$ 且 $b \in \{x\} - \{x^2\}$ 或反過來

所以 $ax^2 + by^2 \equiv k \pmod{p^t} \quad \forall k$ 恆有解的數對 (a, b)

設先取 a

有 $p^t - p^{t-1}$ 種取法

接著 b 只有 $\frac{p^t - p^{t-1}}{2}$ 個數可取

故 (a, b) 有 $\frac{(p^t - p^{t-1})^2}{2}$ 組

$$f_2(p^t) = \frac{(p^t - p^{t-1})^2}{2} = \frac{\phi(p^t)^2}{2}$$

(三) $m \in N$

$$\text{設 } m = \prod_{i=1}^n p_i^{\alpha_i}$$

易知 $ax^2 + by^2 \equiv k \pmod{m}$ 有解 $\Rightarrow a_i x^2 + b_i y^2 \equiv k \pmod{p_i^{\alpha_i}}$ 有解

又若 $a_i x^2 + b_i y^2 \equiv k \pmod{p_i^{\alpha_i}} \quad \forall k$ 恆有解

從滿足條件的數對中任取一組

則可得到一系列 (a_i, b_i)

由中國剩餘定理知可找到唯一一組 (a, b) 滿足

$$a \equiv a_i \pmod{p_i^{\alpha_i}}, b \equiv b_i \pmod{p_i^{\alpha_i}} \quad \text{且 } 0 < a, b < m$$

又 (a_i, b_i) 系列有 $\prod_{i=1}^n f_2(p_i^{\alpha_i})$

而此恰等於 $f_2(m)$

$$\text{故 } f_2(m) = \prod_{i=1}^n f_2(p_i^{\alpha_i})$$

$$\text{若令 } m = \prod_{i=1}^k p_i \prod_{j=k+1}^n p_j^{\alpha_j} \quad p_i \neq p_j$$

$$\text{則 } f_2(m) = \frac{\phi(m)^2}{2^{n-k}}$$

$$\text{三} \quad \sum_{i=1}^n a_i x_i^n \equiv k \pmod{m}$$

(一) $m \in P \quad (m, n) = 1$

令 s 為 p 的原根

因此 p 的 n 次剩餘可寫為 $\{s^n, s^{2n}, \dots, s^{(p-1)n}\}$

若

則 $\{s^n, s^{2n}, \dots, s^{(p-1)n}\}$ 等於是 p 的完全剩餘系

若 $(p-1, n) \neq 1$

則 $\{s^n, s^{2n}, \dots, s^{(p-1)n}\}$ 有 $\frac{p-1}{(p-1, n)}$ 個元素

由定理三可得 $\left| \left\{ \sum_{i=1}^n a_i x_i^n \right\} \right| \geq n \times \left(\frac{p-1}{(p-1, n)} + 1 \right) - (n-1) \geq p$

故對任意 $(a_1, a_2, \dots, a_n)$

$$\sum_{i=1}^n a_i x_i^n \equiv k \pmod{p} \quad \forall k \text{ 恆有解}$$

又由以上引理

可得 $\sum_{i=1}^{(p-1, n)} a_i x_i^n \equiv k \pmod{p} \quad \forall k \text{ 恆有解}$

因此 $f_n(p) \geq \varphi(p)^n$

(二) $m = p^t, t \in N$

由定理四

令 $f(x) = a_1 x^n + \sum_{i=2}^n a_i x_i^n, x_1 \geq x_2 \geq \dots \geq x_n$

$$f(x_1) = \sum_{i=1}^n a_i x_i^n \equiv k \pmod{p}$$

$$f'(x_1) = n a_1 x_1^{n-1}$$

只要 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{p}$ 有非零解

則 $f'(x_1) = n a_1 x_1^{n-1} \neq 0$

1. 若 $k \not\equiv 0 \pmod{p}$

明顯無全為零的解

2. 若 $k \equiv 0 \pmod{p}$

(1) $n > p$

考慮 $\sum_{i=1}^k a_i (k=1, 2, \dots, n)$

由鴿籠原理知必有兩個和相等

設為 $\sum_{i=1}^j a_i, \sum_{i=1}^l a_i \quad l > j$

則 $\sum_{i=j+1}^l a_i = 0$

故令

$$x_1 = x_2 = \dots = x_j = x_{l+1} = x_{l+2} = \dots = x_n = 0, x_{j+1} = x_{j+2} = \dots = x_l = 1$$

即可得一非零解

(2) $n < p$

因尚未處理完畢，故僅討論 $n = p-1, (n, p-1)=1$ 兩種情況

a. $n = p-1$

易見若 $a_1 = a_2 = \cdots = a_n$

$$\sum_{i=1}^n a_i x_i^n \equiv 0 \pmod{p} \text{ 無非零解}$$

$$\text{故 } \sum_{i=1}^n a_i x_i^n \equiv kp \pmod{p^t} \text{ 無解 } (k \neq mp^{n-1}, m \in \mathbb{N})$$

若 a_i 中有兩個以上不同

設 $a_{n-1} \neq a_n$

$$\text{考慮 } \sum_{i=1}^k a_i, k=1, 2, \dots, n-2, \left(\sum_{i=1}^{n-2} a_i \right) + a_{n-1} \\ \left(\sum_{i=1}^{n-2} a_i \right) + a_n, \left(\sum_{i=1}^{n-2} a_i \right) + a_{n-1} + a_n \text{ 共 } p \text{ 個數}$$

若有一個等於 0

$$\text{設為 } \sum_{i=1}^l a_i$$

則 $x_1 = x_2 = \cdots = x_l = 1, x_{l+1} = x_{l+2} = \cdots = x_n = 0$ 即為一非零解

若無

則必有兩式相等

$$\text{又 } \left(\sum_{i=1}^{n-2} a_i \right) + a_{n-1} \neq \left(\sum_{i=1}^{n-2} a_i \right) + a_n$$

故相等兩式可寫為

$$\sum_{i=1}^l a_i = \sum_{i=1}^r a_i \text{ 或 } \sum_{i=1}^l a_i = \left(\sum_{i=1}^{n-2} a_i \right) + a_n$$

$$\text{移項得 } \sum_{i=r+1}^l a_i = 0 \text{ 或 } \left(\sum_{i=l+1}^{n-2} a_i \right) + a_n = 0$$

同①的方法取 x_i

即可得一非零解

b. $(n, p-1)=1$

因 p 的 n 次剩餘系恰為 p 的完全剩餘系

$$\text{故 } \{x^n\} = \{x\}$$

$$\sum_{i=1}^n a_i x_i^n \equiv 0 \pmod{p} \text{ 等價於 } \sum_{i=1}^n a_i x_i \equiv 0 \pmod{p}$$

$$\text{又 } \sum_{i=1}^n a_i x_i \equiv 0 \pmod{p} \text{ 一定有非零解}$$

$$\text{故 } \sum_{i=1}^n a_i x_i^n \equiv 0 \pmod{p} \text{ 必有非零解}$$

由上述可得

當 $n > p$ 時

$$f_n(p^t) \geq \varphi(p^t)^n$$

當 $n = p - 1$ 時

$$f_n(p^t) = \varphi(p^t)^n - (p - 1) \geq \varphi(p^t)^n - \varphi(p)$$

當 $n = p - 2$ 時

$$f_n(p^t) \geq \varphi(p^t)^n$$

(三) $m \in N$

$$\text{設 } m = \prod_{i=1}^s p_i^{\alpha_i}$$

$$\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m} \Leftrightarrow \sum_{i=1}^n a_i x_i^n \equiv k \pmod{p_j^{\alpha_j}}, j = 1, 2, \dots, n$$

又由中國剩餘定理

對任意一系列 $(a_{1_j}, a_{2_j}, \dots, a_{n_j})$

有且僅有一組 $(a_1, a_2, \dots, a_n)$ 滿足

$$a_i \equiv a_{i_j} \pmod{p_j^{\alpha_j}} \quad \forall j = 1, 2, \dots, s \text{ 成立}$$

而 $(a_{1_j}, a_{2_j}, \dots, a_{n_j})$ 系列有 $\prod_{i=1}^s f_n(p_j^{\alpha_j})$ 個

$$\text{故 } f_n(m) = \prod_{i=1}^s f_n(p_j^{\alpha_j})$$

又由上述 a. b.

$$\text{改令 } m = \prod_{i=1}^k p_i \prod_{j=k+1}^s p_j^{\alpha_j}$$

可得以下結論：

$$\text{若 } n > \max\{p_j\}, j = k + 1, k + 2, \dots, s \text{ 或 } (n, \varphi(m)) = 1$$

$$\text{則 } f_n(m) = \prod_{i=1}^k f_n(p_k) \prod_{j=k+1}^s f_n(p_j^{\alpha_j}) \geq \prod_{i=1}^k \varphi(p_k)^n \prod_{j=k+1}^s \varphi(p_j^{\alpha_j})^n = \varphi(m)^n$$

柒、結論

$$(一) f_1(m) = \psi(m)$$

$$(二) \text{ 令 } m = \prod_{i=1}^k p_i \prod_{j=k+1}^n p_j^{\alpha_j} \quad p_i \neq p_j$$

$$\text{則 } f_2(m) = \frac{\varphi(m)^2}{2^{n-k}}$$

$$(三) \text{ 令 } m = \prod_{i=1}^k p_i \prod_{j=k+1}^s p_j^{\alpha_j}$$

$$\text{若 } n > \max\{p_j\}, j = k + 1, k + 2, \dots, s \text{ 或 } (n, \varphi(m)) = 1$$

則 $f_n(m) \geq \varphi(m)^n$

(四)在過程中

可看出 f 為積性函數

$$\text{即 } \prod_{i=1}^n f(p_i^{\alpha_i}) = f\left(\prod_{i=1}^n p_i^{\alpha_i}\right)$$

(五)當 $n = p - 1$ 時

$$f_n(p^t) \geq \varphi(p^t)^n - (p-1) = \varphi(p^t)^n - \varphi(p)$$

當 $(n, p-1) = 1$ 時

$$f_n(p^t) = \varphi(p^t)^n$$

捌、未來展望

(一) 求出 $f_n(m)$ 的數值

(二) $\sum_{i=1}^t a_i x_i^n \equiv k \pmod{m}$ 恆有解的條件

玖、參考文獻

潘承洞、潘承彪 初等數論 凡異出版社出版

拾、附錄

(一)定理三的證明：

先令 $A = \{a_1 = 0, a_2 \cdots a_n\}$ $B = \{b_1 = 0, b_2 \cdots b_m\}$ $m, n < p$

(1) 設 $m = 2$

$$C = \{a_1, a_2 \cdots a_n, a_1 + b_2, a_2 + b_2 \cdots a_n + b_2\}$$

$$\text{若 } |C| = |A|$$

$$\text{則 } \{a_1 + b_2, a_2 + b_2 \cdots a_n + b_2\} = A$$

$$\sum_{i=1}^n (a_i + b_2) = \sum_{i=1}^n a_i + nb_2 \equiv \sum_{i=1}^n a_i$$

$$nb_2 \equiv 0 \pmod{p}$$

$$\because b_2 \neq 0 \quad \therefore n \equiv 0 \pmod{p} \text{ 不合}$$

$$\therefore |C| \geq |A| + 1 = |A| + |B| - 1 \text{ 成立}$$

(2) 設 $m \leq k$ 時成立

$$m = k + 1 \text{ 時}$$

先考慮 $a_i + b_2$

由上知必存在一 a_i

使 $a_i + b_2 \notin A$

設為 a_2

令 $A' = A + \{a_2 + b_j\}$ $B' = \{b_j \mid a_2 + b_j \in A\}$

由 a_2 取法知 $A' > A$ $B' < B$ $|A| + |B| = |A'| + |B'|$

且 $(a_2 + b_j) + b'_j = (a_2 + b'_j) + b_j \in C$

$\therefore |A| + |B| - 1 = |A'| + |B'| - 1 \leq |C| = |\{x + y \mid x \in A', y \in B'\}|$

$\leq |\{x + y \mid x \in A, y \in B\}| = |C|$

由數學歸納法知命題成立

(二)定理四的證明：

因 $f(x)$ 為一多項式函數

故可將 $f(x)$ 寫為

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2 \cdot 1}(x-a)^2 \dots$$

令 $x = \alpha p^n + a$

$$f(x) \equiv f(a) + f'(a)\alpha p^n \pmod{p^{2n}}$$

$$\because f(a) \equiv c \pmod{p^n}$$

$$\therefore f(a) = c + rp^n$$

$$f(x) \equiv f(a) + f'(a)\alpha p^n = c + (r + f'(a)\alpha)p^n \pmod{p^{2n}}$$

設 $f(x) \equiv c$

$$\text{得 } (r + f'(a)\alpha)p^n \equiv 0 \pmod{p^{2n}} \Leftrightarrow r + f'(a)\alpha \equiv 0 \pmod{p^n}$$

又因 $(f'(a), p^n) = 1$

故滿足條件的 α 存在

命題成立

中華民國第四十五屆中小學科學展覽會
評 語

高中組 數學科

佳作

040422

作品名稱：滿足 $\sum_{i=1}^n a_i x_i^n \equiv k \pmod{m}$ ， $(m,n)=1$ ， $\forall k$ 恆有解

$(x_1, x_2, \dots, x_n)$ 且 $0 < a_i < m$ 的數對 $(a_1, a_2, \dots, a_n)$ 之條件及組數 $f_n(m)$

的下界估計

臺北市立建國高級中學

評語：

1. 數學能力頗具深度。
2. 標題應簡單明瞭，作品名稱有待改善。
3. 成功的科展作品，應增強其直觀性，並能兼具幾何及代數之含意。