
IMO 數論練習題連解答

第一題：

設 a 是整數， n 和 r 是大於 1 的整數， p 是奇質數，並且 $(n, p-1) = 1$ 。

試求以下同餘方程的不同的解的數目：

$$x_1^n + x_2^n + \cdots + x_r^n \equiv a \pmod{p}。$$

請注意上述方程的解 (x_1, x_2, \dots, x_r) 和 $(x'_1, x'_2, \dots, x'_r)$ 當且僅當

$$x_j \equiv x'_j \pmod{p}, \quad j = 1, 2, \dots, r$$

時，才認為兩個解是相同的。

解答：

先證明一個引理：

對任何的整數 y ，存在（同餘意義下）唯一的 x 使 $x^n \equiv y \pmod{p}$ ，這裏 n, p 為題目所給定的。

若 $y \equiv 0 \pmod{p}$ ，則 $x \equiv 0 \pmod{p}$ 顯然是唯一解。

若 $y \not\equiv 0 \pmod{p}$ ，則 $(y, p) = 1$ ，由費馬小定理 (Fermat Little Theorem) 可知

$$y^{p-1} \equiv 1 \pmod{p}。$$

利用條件 $(n, p-1) = 1$ 及斐蜀定理可知：存在 $u, v \in \mathbb{N}$ 使得 $nu - (p-1)v = 1$ ，於是

$$(y^u)^n \equiv y^{(p-1)v+1} \equiv (y^{p-1})^v \cdot y \equiv y \pmod{p}。$$

故可以取 $x \equiv y^u \pmod{p}$ ，這樣便有 $x^n \equiv y \pmod{p}$ 。由於對任何的整數 y 我們都找到合適的 x ，所以 x 必定是唯一的。

利用上述引理，可知方程 $x_1^n + x_2^n + \cdots + x_r^n \equiv a \pmod{p}$ 的解共有 p^{r-1} 組。（事實上， $x_1^n, x_2^n, \dots, x_{r-1}^n$ 可取 $0, 1, 2, \dots, p-1$ 中任意數，而 x_r 由此及 a 唯一確定）

第二題：

考察不定方程 $x^2 - y^2 = n$ 。約定將這方程的不同的正整數解的數目記為 $f(n)$ ，試對所有的正整數 n ，求 $f(n)$ 。

解答

當 n 為奇數時，由 $(x-y)(x+y) = n$ ，而 $x-y$ 與 $x+y$ 具有相同的奇偶性，且 $0 < x-y < x+y$ ，可知所求的數目是 $\left[\frac{d(n)}{2} \right]$ 。這裏 $d(n)$ 表示正整數 n 的正因數之個數， $[t]$ 表示不大於 t 的最大整數。

當 n 為偶數時，由 $(x-y)(x+y) = n$ 及 $x-y$ 與 $x+y$ 奇偶性相同可知 $x+y$ 和 $x-y$ 都是偶數。若 $4 \nmid n$ 則 $f(n) = 0$ ；若 $4 \mid n$ ，所求數目為 $\left[\frac{1}{2} d\left(\frac{n}{4}\right) \right]$ 。

第三題：

設 a 和 b 是正整數， p 是奇質數， $p > a > b > 1$ 。試求最大的整數 c ，使得對所有滿足上述條件的 a, b 和 p 都有

$$p^c \left| \binom{ap}{bp} - \binom{a}{b} \right|,$$

這裏，我們記

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

解答：

取 $p = 5$ 、 $a = 3$ 、 $b = 2$ 可知 $5^c \left| \binom{15}{10} - \binom{3}{2} \right|$ ，即 $5^c \mid 3000$ ，故 $c \leq 3$ 。

以下證明：對任意滿足條件的 p, a, b ，均有 $p^3 \left| \binom{ap}{bp} - \binom{a}{b} \right|$ 。

利用 $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$ ，我們有

$$\begin{aligned} \binom{ap}{bp} &= \frac{(ap)(ap-1)\cdots((a-b)p+1)}{(bp)!} \\ &= \frac{a(a-1)\cdots(a-b+1)}{b!} \times \frac{\prod_{k=a-b}^{a-1} (kp+1)(kp+2)\cdots(kp+(p-1))}{\prod_{k=0}^{b-1} (kp+1)(kp+2)\cdots(kp+(p-1))} \\ &= \binom{a}{b} \times \frac{\prod_{k=a-b}^{a-1} f(kp)}{\prod_{k=0}^{b-1} f(kp)} \end{aligned}$$

這裏 $f(x) = (x+1)(x+2)\cdots(x+p-1)$ 。

於是

$$\binom{ap}{bp} - \binom{a}{b} = \binom{a}{b} \times \frac{\prod_{k=a-b}^{a-1} f(kp) - \prod_{k=0}^{b-1} f(kp)}{\prod_{k=0}^{b-1} f(kp)}。$$

留意到 $f(kp) \equiv (p-1)! \not\equiv 0 \pmod{p}$ ，故上式的分母不是 p 的倍數。

所以，接下來只需證明 p^3 整除分子，即證明

$$p^3 \mid \prod_{k=a-b}^{a-1} f(kp) - \prod_{k=0}^{b-1} f(kp)。$$

為此，我們首先證明一個引理： $f(kp) \equiv (p-1)! \pmod{p^3}$ 。

設 $f(x) = (x+1)(x+2)\cdots(x+p-1) = x^{p-1} + S_1x^{p-2} + S_2x^{p-3} + \cdots + S_{p-2}x + (p-1)!$ 。

留意到，對於 $x = 1, 2, \dots, p-1$ ，都有 $f(x) \equiv 0 \pmod{p}$ 。考慮同餘式

$$f(x) - x^{p-1} + 1 \equiv 0 \pmod{p} \quad \text{-----} \quad (1)$$

利用費馬小定理 (Fermat Little Theorem) 可知 $x = 1, 2, \dots, p-1$ 都是(1)的解，另一方面留意到(1)式左邊是一個 $p-2$ 次多項式，可是我們卻找到了 $p-1$ 個解，故這個 $p-2$ 次多項式的每一個係數都必定是 p 的倍數。

於是 S_1, S_2, \dots, S_{p-2} 全是 p 的倍數。利用這個結果，再在

$$f(x) = x^{p-1} + S_1x^{p-2} + S_2x^{p-3} + \cdots + S_{p-2}x + (p-1)!$$

中取 $x = -p$ ，得到

$$f(-p) = p^{p-1} - S_1p^{p-2} + S_2p^{p-3} - \cdots - S_{p-2}p + (p-1)!$$

因為 $f(-p) = (p-1)!$ ，故有

$$p^{p-1} - S_1 p^{p-2} + S_2 p^{p-3} - \cdots - S_{p-2} p = 0。$$

細心考慮這個式子，發現除了最後一項 $S_{p-2} p$ 之外，每一項都是 p^3 的倍數，所以

$S_{p-2} p$ 也必定是 p^3 的倍數(等價地說 S_{p-2} 是 p^2 的倍數，這是 [Wolstenholme 定理](#))，

所以， $f(kp) = (kp)^{p-1} + S_1 (kp)^{p-2} + \cdots + S_{p-2} (kp) + (p-1)! \equiv (p-1)! \pmod{p^3}$ 。

現在返回主要問題，我們作以上準備功夫是為了證明

$$p^3 \mid \prod_{k=a-b}^{a-1} f(kp) - \prod_{k=0}^{b-1} f(kp)。$$

利用 $f(kp) \equiv (p-1)! \pmod{p^3}$ 這個結果，

$$\prod_{k=a-b}^{a-1} f(kp) - \prod_{k=0}^{b-1} f(kp) \equiv [(p-1)!]^{b-1} - [(p-1)!]^{b-1} \equiv 0 \pmod{p^3}。$$

從而完成了我們的證明， c 的最大值是 3。

第四題：

A 是任意的有限正整數集，試證：存在一個有限正整數集 B ，使得 $A \subseteq B$ 且

$$\prod_{x \in B} x = \sum_{x \in B} x^2。$$

解答：

設 $A = \{a_1, a_2, \dots, a_k\}$ ，以下證明存在正整數 $a_{k+1}, a_{k+2}, \dots, a_n$ ($n > k$) 滿足

$$a_1 a_2 \cdots a_n = a_1^2 + a_2^2 + \cdots + a_n^2。$$

這裏 a_1, a_2, \dots, a_n 不一定互不相同。

不妨假設 $a_1 a_2 \cdots a_k > a_1^2 + a_2^2 + \cdots + a_k^2$ ，因為若果這個不等式不成立的話我們可以在 a_1, a_2, \dots, a_k 之後加上足夠多個「2」使其成立。(每加一個「2」左邊大一倍而右邊只加了 4)

記 $m = a_1 a_2 \cdots a_k - (a_1^2 + a_2^2 + \cdots + a_k^2)$ (留意 m 是正整數), 我們在 a_1, a_2, \cdots, a_k 之後加上 m 個「1」, 於是

$$a_1 a_2 \cdots a_k \underbrace{(1 \times 1 \times \cdots \times 1)}_{m \text{ 個}} = a_1^2 + a_2^2 + \cdots + a_k^2 + m = a_1^2 + a_2^2 + \cdots + a_k^2 + \underbrace{1^2 + 1^2 + \cdots + 1^2}_{m \text{ 個}}$$

所以正整數 $a_1, a_2, \cdots, a_k, \underbrace{1, 1, \cdots, 1}_{m \text{ 個}}$ 滿足條件。

故此, 我們只需為原來的 k 個數加入有限個「1」和「2」便可滿足條件, 以下證明可以將這有限個數透過有限步的操作使其兩兩不同 (且包含原來的 k 個數)。

假設正整數 $b_1 \leq b_2 \leq \cdots \leq b_n$ 滿足 $b_1 b_2 \cdots b_n = b_1^2 + b_2^2 + \cdots + b_n^2$, 將這個式子看成一個關於 b_1 的二次方程 $(b_1)^2 - (b_2 b_3 \cdots b_n) b_1 + (b_2^2 + b_3^2 + \cdots + b_n^2) = 0$, 若 b_1 是根, 則另一個根是 $b'_1 = b_2 b_3 \cdots b_n - b_1$, 只要 $b_2 b_3 \cdots b_{n-1} > 2$, 便有 $b'_1 > b_n$, 所以 b'_1 與 b_2, b_3, \cdots, b_n 不相同, 且正整數 $b_2 \leq b_3 \leq \cdots \leq b_n < b'_1$ 亦滿足條件。

所以, 即使我們因為加入了有限個「1」和「2」而出現相同的數, 也可以利用上述的操作將其中一個重複出現的數變換成一個未出現過的數。透過有限次這樣的操作, 便可得到題目要求的集合 B 。

第五題：

已知不定方程 $x^4 + y^4 = z^2$ 和不定方程 $x^4 - y^4 = z^2$ 都沒有使得 $xyz \neq 0$ 的整數解。據此求出不定方程 $8y^4 + 1 = z^2$ 的所有整數解 (簡明扼要寫出求解過程)。完成上述準備後, 開始解決主要問題：求以下不定方程組的所有整數解

$$\begin{cases} 1 + x = 8y^2 \\ 1 + x^2 = 2z^2 \end{cases}$$

解答：

首先解方程 $8y^4 + 1 = z^2$, 把它寫成 $y^4 = \frac{(z+1)(z-1)}{8}$ 。留意到 $z+1$ 和 $z-1$ 同是偶數, 它們之中有且僅有一個是 4 的倍數。所以

$$\begin{cases} z+1=2a^4 \\ z-1=4b^4 \end{cases} \quad \text{或} \quad \begin{cases} z+1=4b^4 \\ z-1=2a^4 \end{cases}$$

其中 a, b 是非負整數。

相減有 $a^4 - 2b^4 = \pm 1$ ，即 $a^4 - b^4 = b^4 \pm 1$ 。兩邊平方得

$$(a^4 - b^4)^2 = b^8 \pm 2b^4 + 1$$

$$(a^4 - b^4)^2 = b^8 \pm a^4$$

$$(a^4 - b^4)^2 = (b^2)^4 \pm a^4$$

解這方程，得 $(a, b) = (0, k), (1, 0), (1, 1)$ (k 是非負整數)，於是 $(y, z) = (0, \pm 1)$ 或 $(\pm 1, \pm 3)$ 。

現在開始解決主要問題。

$$\begin{cases} 1+x=8y^2 \\ 1+x^2=2z^2 \end{cases}$$

消去 x 得到

$$1+(8y^2-1)^2=2z^2$$

$$64y^4-16y^2+2=2z^2$$

$$32y^4-8y^2+1=z^2$$

$$(4y^2)^2+(4y^2-1)^2=z^2$$

所以 $(4y^2-1, 4y^2, z)$ 為一基本勾股數組，於是

$$\begin{cases} 4y^2=2mn \\ 4y^2-1=m^2-n^2 \end{cases}$$

其中 m 是偶數、 n 是奇數， $(m, n) = 1$ 。從 $4y^2 = 2mn$ 可知 $m = 2u^2, n = v^2$ (u, v 是非負整數)，於是

$$4u^2v^2-1=(2u^2)^2-(v^2)^2$$

$$(2u^2+v^2)^2=8u^4+1$$

$$u=0, 1 \Rightarrow (m, n) = (0, 1), (2, 1) \Rightarrow y = 0, \pm 1。$$

所以， $(x, y, z) = (-1, 0, \pm 1), (7, \pm 1, \pm 5)$ 。

第六題：

求同時滿足以下條件的一切正整數組 (a, b, c, d) ：

- (a) $2^{2\alpha} \parallel a$ (即 $2^{2\alpha}$ 整除 a ，但 $2^{2\alpha+1}$ 不整除 a)，其中 α 是正整數；
- (b) $4 \mid b+1$ ， $2 \mid d$ ；
- (c) c^d 的 b 進制表示恰由 a 個數字 1 組成，即

$$c^d = (\underbrace{11 \cdots 1}_{a \text{ 位}})_b \circ$$

解答：

設 $a = 2^{2\alpha} q$ ，其中 q 是正奇數。於是

$$\begin{aligned} c^d &= \frac{b^a - 1}{b - 1} \\ &= \frac{b^{2^{2\alpha} q} - 1}{b - 1} \end{aligned}$$

把 $b^{2^{2\alpha} q} - 1$ 分解成 $(b^{2^{2\alpha-1} q} + 1)(b^{2^{2\alpha-2} q} + 1) \cdots (b^q + 1)(b^q - 1)$ ，我們有

$$c^d = (b^{2^{2\alpha-1} q} + 1)(b^{2^{2\alpha-2} q} + 1) \cdots (b^q + 1) \times \frac{b^q - 1}{b - 1} \quad \text{----- (1)}$$

留意到 $(x \pm 1, x^{2^k} + 1) \mid (x^{2^k} - 1, x^{2^k} + 1) = 2$ ($k = 1, 2, \dots, 2\alpha - 1$)，

當 x 是偶數時便有 $(x \pm 1, x^{2^k} + 1) = 2$ ，於是

$$\begin{cases} (b^{2^m q} + 1, b^{2^n q} + 1) = 2 \\ (b^q - 1, b^{2^k q} + 1) = 2 \end{cases} \quad (k, m, n \in \mathbb{N})$$

將 (1) 式兩邊除以 $2^{2\alpha}$ ，得到

$$\left(\frac{c^{d/2}}{2^\alpha} \right)^2 = \left(\frac{b^{2^{2\alpha-1} q} + 1}{2} \right) \left(\frac{b^{2^{2\alpha-2} q} + 1}{2} \right) \cdots \left(\frac{b^q + 1}{2} \right) \times \left(\frac{b^q - 1}{b - 1} \right) \quad \text{----- (2)}$$

這式左邊是平方數，而右邊是 $2\alpha + 1$ 個兩兩互質的正整數之積，故右邊每項都是

平方數。特別地， $\frac{b^q + 1}{2}$ 和 $\frac{b^{2q} + 1}{2}$ 都是平方數。

$$\begin{cases} \frac{b^q + 1}{2} = u^2 \\ \frac{b^{2q} + 1}{2} = v^2 \end{cases}$$

其中 u, v 是互質的正整數。由於 $b \equiv -1 \pmod{4}$ 且 q 是奇數，故 u 是偶數。不妨設 $u = 2w$ ，其中 w 是正整數。於是

$$\begin{cases} b^q + 1 = 8w^2 \\ b^{2q} + 1 = 2v^2 \end{cases}$$

這是第五題的不定方程組，利用第五題的解答，我們可以證明 $b^q = 7$ 。所以 $b = 7$ 且 $q = 1$ 。代入 (2) 式，

$$\left(\frac{c^{d/2}}{2^\alpha}\right)^2 = \left(\frac{7^{2^{2\alpha-1}} + 1}{2}\right) \left(\frac{7^{2^{2\alpha-2}} + 1}{2}\right) \cdots \left(\frac{7+1}{2}\right)$$

留意到 $\frac{7^4 + 1}{2} = 1201$ 不是平方數，所以 $2^{2\alpha-1} < 4 \Rightarrow \alpha = 1$ ，從而 $c^d = 400$ 。

所以， $(a, b, c, d) = (4, 7, 20, 2)$ ，經驗算它確實滿足題目給定的條件。

第七題：

給定大於 1 的正整數 b 和奇質數 p 。已知 $p \parallel b$ (即 p 整除 b ，但 p^2 不整除 b)。試求正整數 c ，使得 c^p 的 b 進制表示僅由數字 1 組成，即

$$c^p = (11 \cdots 1)_b,$$

位數多少不限。

解答：

顯然 $c = 1$ 滿足條件，以下證明沒有其它正整數 c 適合條件。

假設 $c > 1$ 滿足

$$c^p = 1 + b + b^2 + \cdots + b^k \quad \text{-----} \quad (1)$$

其中 k 是正整數。

對 (1) 式取模 p , 得 $c \equiv 1 \pmod{p}$ 。故可設 $c = pq + 1$ (q 是正整數) , 於是

$$c^p = (pq + 1)^p = 1 + C_1^p(pq) + C_2^p(pq)^2 + \cdots + C_p^p(pq)^p \equiv 1 \pmod{p^2}$$

再對 (1) 式取模 p^2 ,

$$c^p \equiv 1 + b \pmod{p^2}。$$

故 $1 \equiv 1 + b \pmod{p^2}$, $b \equiv 0 \pmod{p^2}$, 矛盾。

從而 $c = 1$ 是唯一適合條件的正整數。

第八題 :

設 a 是非負整數 , p 是奇質數 , $a < p$, 試求以下同餘方程的解 (x, y, z) 的數目 :

$$x^2 + y^2 + z^2 \equiv a \pmod{p}。$$

解答 :

答案是 $p(p+k)$, 其中 $k = \left(\frac{-a}{p}\right)$ 是 Legendre 符號。證明如下 :

留意到同餘式 $x^2 \equiv s \pmod{p}$ 的解的數目 $N[x^2 \equiv s \pmod{p}] = 1 + \left(\frac{s}{p}\right)$ 。於是

$$\begin{aligned} N[x^2 + y^2 \equiv t \pmod{p}] &= \sum_{s=0}^{p-1} N[x^2 \equiv s \pmod{p}] \times N[y^2 \equiv t - s \pmod{p}] \\ &= \sum_{s=0}^{p-1} \left[1 + \left(\frac{s}{p}\right) \right] \times \left[1 + \left(\frac{t-s}{p}\right) \right] \\ &= \sum_{s=0}^{p-1} \left[1 + \left(\frac{s}{p}\right) + \left(\frac{t-s}{p}\right) + \left(\frac{s(t-s)}{p}\right) \right] \\ &= p + \sum_{s=0}^{p-1} \left(\frac{s(t-s)}{p}\right) \\ &= p + \sum_{s^{-1}=1}^{p-1} \left(\frac{ts^{-1}-1}{p}\right) \\ &= p - \left(\frac{-1}{p}\right) + \sum_{s^{-1}=0}^{p-1} \left(\frac{ts^{-1}-1}{p}\right) \end{aligned}$$

$$N[x^2 + y^2 \equiv t \pmod{p}] = \begin{cases} p + (p-1)\left(\frac{-1}{p}\right) & \text{若 } p \mid t \\ p - \left(\frac{-1}{p}\right) & \text{若 } p \nmid t \end{cases}$$

利用上述結果，

$$\begin{aligned} & N[x^2 + y^2 + z^2 \equiv a \pmod{p}] \\ &= \sum_{t=0}^{p-1} N[x^2 + y^2 \equiv t \pmod{p}] \times N[z^2 \equiv a-t \pmod{p}] \\ &= \left[p + (p-1)\left(\frac{-1}{p}\right) \right] \times \left[1 + \left(\frac{a}{p}\right) \right] + \left[p - \left(\frac{-1}{p}\right) \right] \times \sum_{t=1}^{p-1} \left[1 + \left(\frac{a-t}{p}\right) \right] \\ &= \left[p + (p-1)\left(\frac{-1}{p}\right) \right] \times \left[1 + \left(\frac{a}{p}\right) \right] + \left[p - \left(\frac{-1}{p}\right) \right] \times \left[(p-1) - \left(\frac{a}{p}\right) \right] \\ &= p^2 + p\left(\frac{-a}{p}\right) \end{aligned}$$

所以 $N[x^2 + y^2 + z^2 \equiv a \pmod{p}] = p(p+k)$ ，其中 $k = \left(\frac{-a}{p}\right)$ 是 Legendre 符號。

第九題：

對怎樣的奇質數 p ，存在整數 x 和 y ，使得 $p = 5x^2 + y^2$ ，請證明你的結論。

解：

假設有這樣的奇質數 p ，取模 4 得 $p \equiv x^2 + y^2 \pmod{4}$ 。

留意到任何平方數 $k^2 \equiv 0, 1 \pmod{4}$ ，不難知道 $p \equiv 1 \pmod{4}$ 。

類似地，取模 5 得 $p \equiv y^2 \pmod{5}$ ，於是 $p = 5$ 或 $p \equiv \pm 1 \pmod{5}$ 。

所以，任何滿足條件的奇質數 p 都必定是 5 或形如 $20t+1, 20t+9$ 的。

顯然 $p = 5 = 5(1^2) + 0^2$ 滿足條件，以下證明任何形如 $20t+1$ 或 $20t+9$ 的質數都滿足條件。

若 p 是形如 $20t+1$ 或 $20t+9$ 的質數，則存在整數 a 使得 $a^2 \equiv -5 \pmod{p}$ 。

考慮集合 $S = \{n \mid n = ax + y, x, y \in \mathbb{Z}, 0 \leq x, y < \sqrt{p}\}$ 。

留意到 $|S| = \left(\left[\sqrt{p}\right] + 1\right)^2 > p$ ，所以必有 $m, n \in S$ 使得 $m \equiv n \pmod{p}$ 。

設 $m = ax_1 + y_1, n = ax_2 + y_2$ ，則

$$a(x_1 - x_2) + (y_1 - y_2) \equiv 0 \pmod{p}$$

取 $u = x_1 - x_2, v = y_1 - y_2$ (留意 $|u|, |v| < \sqrt{p}$)，則

$$au + v \equiv 0 \pmod{p} \Rightarrow v^2 \equiv (-au)^2 \equiv -5u^2 \pmod{p}$$

即 $5u^2 + v^2 \equiv 0 \pmod{p}$ ，另一方面我們知道 $5u^2 + v^2 < 5(\sqrt{p})^2 + (\sqrt{p})^2 = 6p$ ，於

是可設 $5u^2 + v^2 = pk$ ，其中 $k = 1, 2, \dots, 5$ 。

若 $k = 1$ ，則問題已解決。現在假設 $k > 1$ ，以下就 k 的值分 4 種情況討論：

1. 若 $5u^2 + v^2 = 2p$ ，則 u, v 同是奇數 (否則它們同是偶數，式中兩邊都是 4 的倍數，這是不可能的)
於是 $2p \equiv 5u^2 + v^2 \equiv 6 \pmod{8} \Rightarrow p \equiv 3 \pmod{4}$ ，矛盾。
2. 若 $5u^2 + v^2 = 3p$ ，取模 4 得 $u^2 + v^2 \equiv 3 \pmod{4}$ ，這是不可能的。
3. 若 $5u^2 + v^2 = 4p$ ，則 u, v 必定是偶數，兩邊除 4 得 $5\left(\frac{u}{2}\right)^2 + \left(\frac{v}{2}\right)^2 = p$ 。
4. 若 $5u^2 + v^2 = 5p$ ，則 v 是 5 的倍數，兩邊除 5 得 $u^2 + 5\left(\frac{v}{5}\right)^2 = p$ 。

所以，存在整數 x, y 滿足 $p = 5x^2 + y^2$ 當且僅當 $p = 5$ 或 $p \equiv 1, 9 \pmod{20}$ 。

第十題：

設質數 $p \equiv 3 \pmod{4}$ ，對於 $i, k \in \{0, 1, \dots, p-1\}$ ，試構造 $x_{i,k} \in \{0, 1\}$ 滿足以下條件：

(a) $\sum_{k=0}^{p-1} x_{i,k} = \frac{p+1}{2}, \quad i = 0, 1, \dots, p-1$ ；

(b) 對於 $i, j \in \{0, 1, \dots, p-1\}$ ， $i \neq j$ 有 $\sum_{k=0}^{p-1} |x_{i,k} - x_{j,k}| = \frac{p+1}{2}$ 。

解答：

對任意的 $i, k \in \{0, 1, \dots, p-1\}$ ，取

$$x_{i,k} = \begin{cases} 1 & \text{若 } y^2 \equiv i+k \pmod{p} \text{ 有解} \\ 0 & \text{若 } y^2 \equiv i+k \pmod{p} \text{ 無解} \end{cases}$$

以下證明這樣的 $x_{i,k}$ 滿足條件。

它滿足 (a) 是顯然的，因為使同餘式

$$y^2 \equiv s \pmod{p} \text{ ----- (1)}$$

有解的正整數 s 有 $\frac{p+1}{2}$ 個，其中 $\frac{p-1}{2}$ 個是模 p 的二次剩餘，另外 $s=0$ 亦使 (1) 有解。

以下證明 $x_{i,k}$ 滿足 (b)：

取 $d = j - i \not\equiv 0 \pmod{p}$ ，若 $s = t$ 和 $s' = t + d$ 同時使 (1) 有解或同時使 (1) 無解，則我們稱整數 t 為「好數」。

留意到若 t 是好數則必有 $t \equiv 0, -d \pmod{p}$ 或 $\left(\frac{t}{p}\right)\left(\frac{t+d}{p}\right) = 1$ 。

因為 $p \equiv 3 \pmod{4}$ ，故 d 和 $-d$ 有且僅有一個是模 p 的二次剩餘，即是說「0」和「 $-d$ 」有且僅有一個是好數。

接下來我們數算使 $\left(\frac{t}{p}\right)\left(\frac{t+d}{p}\right) = 1$ 成立的整數 t (在同餘意義下) 共有多少個。

考慮和式

$$\begin{aligned} \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)\left(\frac{t+d}{p}\right) &= \sum_{t^{-1}=1}^{p-1} \left(\frac{t^{-1}}{p}\right)\left(\frac{t+d}{p}\right) \\ &= \sum_{t^{-1}=1}^{p-1} \left(\frac{t^{-1}d+1}{p}\right) \\ &= -\left(\frac{1}{p}\right) \\ &= -1 \end{aligned}$$

故使 $\left(\frac{t}{p}\right)\left(\frac{t+d}{p}\right) = 1$ 成立的 t 共有 $\left[\frac{p-2}{2}\right] + 1 = \frac{p-3}{2}$ 個。

所以，在模 p 的既約剩餘系中共有 $\frac{p-3}{2} + 1 = \frac{p-1}{2}$ 個好數。

留意到

$$\begin{cases} x_{i,k} = x_{j,k} & \text{若 } i+k \text{ 是好數} \\ x_{i,k} \neq x_{j,k} & \text{若 } i+k \text{ 不是好數} \end{cases}$$

當 k 取遍 $0, 1, \dots, p-1$ 時， $x_{i,k} = x_{j,k}$ 的情況出現了 $\frac{p-1}{2}$ 次，即是說

$$\sum_{k=0}^{p-1} |x_{i,k} - x_{j,k}| = \frac{p+1}{2}。$$

所以我們構造出來的 $x_{i,k}$ 滿足題目的兩個條件。