中華民國第 65 屆中小學科學展覽會

作品說明書

高級中等學校組　數學科

050418

負負得正

學校名稱：花蓮縣私立海星高級中學

作者：	指導老師：
高二 陳治宇 高二 林姮瑋 高二 盧顥仁	王寶能

關鍵詞：矩陣、循環、同餘

研究摘要

一群人熟識彼此身分的朋友圍圓桌而坐，每個人可能是老實人(說實話)，也有可能是騙子(說謊話)，對於老闆的提問「右手邊的是騙子還是老實人」每個人做出回答。本文就每位顧客所答的身分進行分析，然後延伸問題，假設答題者會繼承所答的身分(我們稱為繼承身分)，舉例來說：如果顧客小明的回答是老實人(騙子)，那麼小明的身分在答題後就會變成老實人(騙子)，接著進行第二輪答題、第三輪答題、...，重複進行下去。文中我們解出了只有當顧客人數是 2^k 時繼承身分才會收斂，並且證明出在第 n 次必然收斂到全好人；若顧客人數不是 2^k 時，則會產生循環。

壹、研究動機：

在科學研習期刊第 63 卷第 2 期的特約專欄中「森棚教官數學題—騙子或老實人」，看到了這個有趣的題目：『五位熟識的朋友在小吃店圍著圓桌而坐，但是每個人可能是騙子(永遠說謊)，也可能是老實人(永遠誠實)。老闆問每一個人坐在他右邊的人是騙子還是老實人，然後統計答案』。在解題過程當中，我們發現了些有趣的現象以及可以延伸討論，因此有了本文的討論。

貳、研究目的：

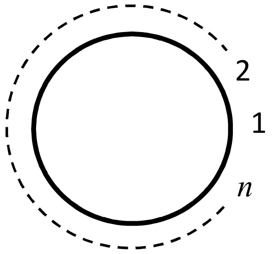
1. 找出 n 位顧客答題後有規律的部分並加以證明。
2. 延伸問題，假設答題者會繼承所答的身分，進行第二次答題，第三次答題...，我們想了解的是，對於任意的初始身分，需要何種的條件才能保證答後身分收斂，以及幾次後能保證收斂。若是不收斂，找出循環的規則並加以證明。

參、研究設備：

紙、筆、電腦

肆、研究方法

圖為本團隊自製



我們將圓周上 n 位置 給予逆時針編號 $1,2,\ldots,n$ 如右圖

一、名詞與符號定義 1：

1. **初始身分向量** $\overrightarrow{X_n}=[x_1,x_2,...,x_n]^T$

   將這 n 人的身分以 $\overrightarrow{X_n}=[x_1,x_2,...,x_n]^T$ 來表示，稱為『初始身分向量』。

   其中，如果第 i 個位置是老實人，則 $x_i=0$，否則 $x_i=1$

2. **答後身分向量** $\overrightarrow{\mathrm{Y}_n}=[y_1,y_2,...,y_n]^T$

   將回答的結果以 $\overrightarrow{\mathrm{Y}_n}=[y_1,y_2,...,y_n]^T$ 表示，稱為『答後身分向量』。

   也就是，如果第 i 個位置回答是騙子則 $y_i=1$，否則 $y_i=0$。

3. **互補身分向量** $\overrightarrow{X_n}^c=[1-x_1,1-x_2,...,1-x_n]^T$

   將每個位置的身分變換，老實人換成騙子，騙子換成老實人，所得到的身分向量，稱為『互補身分向量』。

4. **交錯身分向量** $\overrightarrow{X}_{2m}=[1,0,1,0,...,1,0]^T$ 或是 $\overrightarrow{X}_{2m}=[0,1,0,1,...,0,1]^T$

   有 $2m$ 的人圍圓桌而坐，騙子與老實人各半，且這 $2m$ 個人的身分圓桌上形成騙子與老實人的交錯排列，則稱這樣的身分向量為交錯向量。

二、 列舉顧客人數 2~4 人，並觀察其共同現象

1. 顧客 2 人：初始身分 $\overrightarrow{X_2}=[x_1,x_2]^T$，答後身分 $\overrightarrow{Y_2}=[y_1,y_2]^T$

x_1	0	0	1	1
x_2	0	1	0	1

↓ 表格為本團隊自製

y_1	0	1	1	0
y_2	0	1	1	0

2. 顧客 3 人：初始身分 $\overrightarrow{X_3}=[x_1,x_2,x_3]^T$，答後身分 $\overrightarrow{Y_3}=[y_1,y_2,y_3]^T$

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1

↓

表格為本團隊自製

y_1	0	0	1	1	1	1	0	0
y_2	0	1	1	0	0	1	1	0
y_3	0	1	0	1	1	0	1	0

3. 顧客 4 人：初始身分 $\overrightarrow{X_4}=[x_1,x_2,x_3,x_4]^T$，答後身分 $\overrightarrow{Y_4}=[x_1,x_2,x_3,x_4]^T$

x_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

↓

y_1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
y_2	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
y_3	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
y_4	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0

表格為本團隊自製

由上可看出底下幾點，並在後續的分析裡給出證明

(1) 若答後身分是全老實人，則初始身分是全老實人或全騙子。

(2) 答後的騙子總數必然為偶數。

(3) 若答後身分等於初始身分，則初始身分為全老實人。

(4) 若初始身分互補，則答後身分相同

(5) 若答後身分是全騙子，則初始身分為交錯身分。

三、 定義答題運算

考慮 $\overrightarrow{X_n}=[x_1,x_2,\cdots,x_n]^T$ 與 $\overrightarrow{\mathrm{Y}_n}=[y_1,y_2,\cdots,y_n]^T$ 之間的對應關係

令 $x_{n+1}=x_1$，則 對於 $i=1,2,...,n$ 我們有

(1) 若 $x_i=0$ 且 $x_{i+1}=0$ 則 $y_i=0=x_i+x_{i+1}$

(2) 若 $x_i=0$ 且 $x_{i+1}=1$ 則 $y_i=1=x_i+x_{i+1}$

(3) 若 $x_i=1$ 且 $x_{i+1}=0$ 則 $y_i=1=x_i+x_{i+1}$

(4) 若 $x_i=1$ 且 $x_{i+1}=1$ 則 $y_i=0\equiv x_i+x_{i+1}$ **(mod2)**

綜合以上(1)~(4) 可知 $y_i\equiv x_i+x_{i+1}$ **(mod2)**

我們定義一個答題運算矩陣 **An**，來表示 $\overrightarrow{\mathrm{X}_n}$ 與 $\overrightarrow{\mathrm{Y}_n}$ 之間的轉換關係，如下

$$\mathbf{A_n}=\begin{bmatrix}1 & 1 & 0 & \cdots & 0\\ 0 & 1 & 1 & \ddots & \vdots\\ \vdots & \ddots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & 1 & 1\\ 1 & 0 & \cdots & 0 & 1\end{bmatrix}$$

也就是 $\mathbf{A_n}=\left[a_{i,j}\right]_{n\times n}$，其中 $a_{i,j}=\begin{cases}1 \ , \ if\ j=i \ \vee \ j=i+1\\ 0 \ , \ otherwise\end{cases}$，另外 $a_{n,n+1}=a_{n,1}$

於是有 $\overrightarrow{\mathrm{Y}_n}\equiv\mathbf{A_n}\overrightarrow{\mathrm{X}_n}$ **(mod2)**

四、 分析答後身分

【定理一】 若答後身分是全老實人，則初始身分是全老實人或全騙子。

證明：

令初始身分 $\overrightarrow{X_n}=[x_1,x_2,...,x_n]^T$，答後身分 $\overrightarrow{Y_n}=[y_1,y_2,...,y_n]^T$，

若 $\overrightarrow{\mathrm{Y}_n}=[0,0,...,0]^T$，而 $y_i\equiv x_i+x_{i+1}$ **(mod2)**，其中 $x_{n+1}=x_n$

所以 $x_i + x_{i+1} \equiv 0$ **(mod2)** $\Rightarrow$ $x_i + x_{i+1} = 0$ 或 $x_i + x_{i+1} = 2$，其中 $x_{n+1} = x_n$

若 $x_i + x_{i+1} = 0 \Leftrightarrow x_i = x_{i+1} = 0 \Leftrightarrow \overrightarrow{\mathrm{X}_n} = [0,0,...,0]^T$，此時初始身分全為老實人。

若 $x_i + x_{i+1} = 2 \Leftrightarrow x_i = x_{i+1} = 1 \Leftrightarrow \overrightarrow{\mathrm{X}_n} = [1,1,...,1]^T$，此時初始身分全為騙子。

證明完畢。

【定理二】 答後身分的騙子總數必然為偶數

證明：答後的騙子總數為 $\sum_{i=1}^{n} y_i$，而 $y_i \equiv x_i + x_{i+1}$ **(mod2)** 其中 $x_{n+1} = x_1$

所以 $\sum_{i=1}^{n} y_i \equiv \sum_{i=1}^{n} (x_i + x_{i+1}) = 2\sum_{i=1}^{n} x_i \equiv 0$ **(mod2)**

因此，答後騙子總數為偶數，**證明完畢**。

【定理三】 若答後身分等於初始身分，則初始身分為全老實人。

證明：當『答題後身分等於初始身分』，此時 $y_i \equiv x_i$ **(mod2)**

所以 $x_i + x_{i+1} \equiv x_i$ **(mod2)** $\Rightarrow$ $x_{i+1} \equiv 0$ **(mod2)** 其中 $x_{n+1} = x_1$，

所以初始身分為全老實人，**證明完畢**。

【定理四】 若初始身分互補，則答後身分相同

證明：考慮互補身分向量 $\overrightarrow{X_n}^c = [1-x_1, 1-x_2, ..., 1-x_n]^T$

答題後為 $A_n \overrightarrow{X_n}^c = [2-(x_1+x_2), 2-(x_2+x_3), ..., 2-(x_n+x_1)]^T$

令 $x_{n+1} = x_1$，則對於 $i = 1,2,...,n$

$2-(x_i+x_{i+1}) \equiv (x_i+x_{i+1}) - 2 \equiv x_i + x_{i+1}$ **(mod2)**

所以 $\mathbf{A_n} \overrightarrow{X_n}^c \equiv [x_1+x_2, x_2+x_3, ..., x_n+x_1]^T = \mathbf{A_n} \overrightarrow{X_n}$ **(mod2)**，**證明完畢**。

【定理五】 若答後身分是全騙子，則初始身分為交錯身分

證明：若答後身分全是騙子，此時 $\overrightarrow{\mathrm{Y}_n}=[1,1,...,1]^T$

對於 $i=1,2,...,n$，因為 $0\le x_i\le 1$，所以 $0\le x_i+x_{i+1}\le 2$，其中 $x_{n+1}=x_1$，

而 $y_i\equiv x_i+x_{i+1}$ **(mod2)**，所以，$1\equiv x_i+x_{i+1}$ **(mod2)**

若 $x_1=1$，則 $\overrightarrow{\mathrm{X}_n}=[1,0,1,0,...,1,0]^T$。 若 $x_1=0$，則 $\overrightarrow{\mathrm{X}_n}=[0,1,0,1,...,0,1]^T$。

證明完畢。

五、 延伸討論

接著我們做延伸討論，『假設答題者會繼承所答的身分』，也就是說，當第一次答題後，每位顧客會繼承其回答出來的身分，然後進行第二次答題，然後繼承身分，然後進行第三次答題…，重複進行下去。

明顯的當身分向量變成『全好人』時，繼承身分就不會再因答題而變動(我們稱為收斂到全好人)。因此，若初始身分為『全好人』，則繼承身分便不再變動，直接收斂到『全好人』。若初始身分為『全壞人』，則繼承身分會在第 1 次繼承後收斂到『全好人』。若初始身分為『交錯身分』，則繼承身分會在第 2 次繼承後收斂到『全好人』。而身分向量裡的每一個分量都只有 0,1 這兩選擇，也就是說，在繼承夠多次之後就會與先前的某一次重複，從而產生循環。所以，當身分不斷的繼承下去，最終只會產生 2 種結果，收斂或是循環。

我們想了解的是，在一般的初始身分下，是否能夠保證收斂，又有甚麼條件限制，(這裡的收斂指的是身分不再因答題而產生改變)。

名詞與符號定義 2：

1. **繼承身分向量** $\overrightarrow{Z_n}(m)=[z_1(m),z_2(m),...,z_n(m)]^T$，其中 $m\in N$，

   表示 n 個人在繼承所答身分之下，第 m 次回答的身分向量。

即，若第 i 位客人的第 m 次回答是老實人則 $z_i(m)=0$，否則為 1。

引進答題運算後，我們有

$$\overrightarrow{Z_n}(m) \equiv \mathbf{A_n}\overrightarrow{Z_n}(m-1) \equiv (\mathbf{A_n})^2\overrightarrow{Z_n}(m-2) \equiv \ldots \equiv (\mathbf{A_n})^{\mathbf{m}}\overrightarrow{Z_n}(0) \quad \mathbf{(mod2)}$$

其中 $\overrightarrow{Z_n}(0)=\overrightarrow{X_n}$ 定為初始身分。

2. **在本文中** $z_{n+i}(m)=z_i(m)$；$x_{n+i}=x_i$

3. **特殊方陣符號定義：**

一個 n 階方陣所有的元素都是 0，我們以 $\mathbf{O}_n$ 表示，即 $\mathbf{O}_n=\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}_{n\times n}$

而 n 階的單位方陣，我們以 $\mathbf{I_n}$ 表示，即 $\mathbf{I}_n=\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$

首先，我們來證明一下，如果繼承身分向量收斂，必然收斂到全好人

【定理六】

1. **若繼承身分收斂，則必然收斂到『全好人』。**

2. **若** $\overrightarrow{Z_n}(m)$ **收斂⇔存在正整數** $\boldsymbol{r}$ **使得** $(\mathbf{A_n})^{\mathbf{m}} \equiv \mathbf{O_n}$ $\mathbf{(mod2)}$ $,\ if\ \ m\geq r$

證明：

第 1 部分：

假設 $\overrightarrow{Z_n}(m)$ 收斂到 $[z_1,z_2,\ldots,z_n]^T$，則 $\mathbf{A_n}[z_1,z_2,\ldots,z_n]^T \equiv [z_1,z_2,\ldots,z_n]^T$ $\mathbf{(mod2)}$

$\Rightarrow [z_1+z_2, z_2+z_3,\ldots,z_n+z_1]^T \equiv [z_1,z_2,\ldots,z_n]^T$ $\mathbf{(mod2)}$

所以對於 $i=1,\ldots,n$，$\because z_i \in \{0,1\}$ 且 $z_i+z_{i+1} \equiv z_i$ $\mathbf{(mod2)}$ $\therefore z_{i+1}=0$，其中 $z_{n+1}=z_1$

所以 $[z_1,z_2,\ldots,z_n]^T=[0,0,\ldots,0]^T$ $\mathbf{(mod2)}$

得證第 1 部分。

第 2 部分：

(1) 證明 『若 $\overrightarrow{Z_n}(m)$ 收斂 則 存在正整數 r 使得 $(\mathbf{A_n})^{\mathbf{m}} \equiv \mathbf{O_n}\quad if\ m \ge r$ 』

承第 1 部分，我們知道，若 $\overrightarrow{Z_n}(m)$ 收斂則必然收斂到 $[0,0,...,0]^T$

因此，當 $\overrightarrow{Z_n}(m)$ 收斂時 則必然存在正整數 r 使得 $\overrightarrow{Z_n}(r) \equiv [0,0,...,0]^T$ **(mod2)**

所以，對於任意的初始身分向量 $\overrightarrow{X_n}$ ， 恆有 $(\mathbf{A_n})^{\mathbf{r}} \cdot \overrightarrow{X_n} \equiv \overrightarrow{Z_n}(\mathbf{r}) = [0,0,...,0]^T$ **(mod2)**

假設 $(\mathbf{A_n})^{\mathbf{r}} = [a_{ij}]_{n\times n}$

若取 $\overrightarrow{X_n} = [1,0,0,...,0]^T$ 可得 $(\mathbf{A_n})^{\mathbf{r}} \cdot \overrightarrow{X_n} = [a_{11}, a_{21}, ..., a_{n1}]^T \equiv [0,0,...,0]^T$ **(mod2)**

若取 $\overrightarrow{X_n} = [0,1,0,...,0]^T$ 可得 $(\mathbf{A_n})^{\mathbf{r}} \cdot \overrightarrow{X_n} = [a_{12}, a_{22}, ..., a_{n2}]^T \equiv [0,0,...,0]^T$ **(mod2)**

同理 若取 $\overrightarrow{X_n} = [0,...,0,1,0,...,0]^T$ 第 j 個位置是 1，其他位置是 0

可得 $(\mathbf{A_n})^{\mathbf{r}} \cdot \overrightarrow{X_n} = [a_{1j}, a_{2j}, ..., a_{nj}]^T \equiv [0,0,...,0]^T$ **(mod2)**

所以 $(\mathbf{A_n})^{\mathbf{r}} \equiv \mathbf{O_n}$ **(mod2)**，從而 $(\mathbf{A_n})^{\mathbf{m}} \equiv \mathbf{O_n}$ **(mod2)** $,if\ m \ge r$ 。

(2) 證明 『若存在正整數 r 使得 $(\mathbf{A_n})^{\mathbf{m}} \equiv \mathbf{O_n}\quad if\ m \ge r$ 則 $\overrightarrow{Z_n}(m)$ 收斂』

明顯的，$\overrightarrow{Z_n}(r) \equiv (\mathbf{A_n})^{\mathbf{r}} \cdot \overrightarrow{X_n} \equiv \mathbf{O_n} \cdot \overrightarrow{X_n} = [0,0,...,0]^T$ **(mod2)**，故 $\overrightarrow{Z_n}(m)$ 收斂。

由(1)(2)得證第 **2** 部分。

證明完畢。

接著，關於 $\overrightarrow{Z_n}(m) = [z_1(m), z_2(m), ..., z_n(m)]^T$ ，我們找到底下的性質以及公式。

【性質 1】對於所有非負整數 k，恆有 $z_i(m+2^k) \equiv z_i(m) + z_{i+2^k}(m)$ **(mod2)**，

其中 $z_{n+i}(j) = z_i(j)$ ，$i, j \in N$ ，$m \in N \cup \{0\}$

【性質 2】對於 $a = 0,1$ ，$z_i(m + a\cdot 2^k) \equiv z_i(m) + a \cdot z_{i+a\cdot 2^k}(m)$ **(mod2)**

證明：

(1) 當 $k=0$ 時 ，$z_i(m+2^0)=z_i(m+1)\equiv z_i(m)+z_{i+1}(m)\pmod 2$ ，成立

假設 $k=h$ 時成立($h\ge 0$)，即 $z_i(m+2^h)\equiv z_i(m)+z_{i+2^h}(m)\pmod 2$

則，當 $k=h+1$ 時，

$$
\begin{aligned}
z_i(m+2^{h+1}) &= z_i(m+2^h+2^h)\\
&\equiv z_i(m+2^h)+z_{i+2^h}(m+2^h) \ \textbf{(mod2)}\\
&\equiv z_i(m)+z_{i+2^h}(m)+z_{i+2^h}(m)+z_{i+2^h+2^h}(m) \ \textbf{(mod2)}\\
&\equiv z_i(m)+2z_{i+2^h}(m)+z_{i+2^{h+1}}(m) \ \textbf{(mod2)}\\
&\equiv z_i(m)+z_{i+2^{h+1}}(m) \ \textbf{(mod2)}
\end{aligned}
$$

也成立，由數學歸納法得證【性質 1】。

(2) 當 $a=0$ 時，明顯成立。 當 $a=1$ 時，由【性質 1】可知成立。

證明完畢。

【公式一】

有 n 個人，若初始身分向量為 $\overrightarrow{X_n}=[x_1,x_2,...,x_n]^T$ ，

而答題 m 次後的繼承身分向量為 $\overrightarrow{Z_n}(m)=[z_1(m),z_2(m),...,z_n(m)]^T$

則 $z_i(m)\equiv x_i+\sum_{j=0}^{k}a_j\cdot x_{i+b_j}+\sum_{0\le j<l\le k}a_j\cdot a_l\cdot x_{i+b_j+b_l}+....+a_0\cdot a_1\cdots\cdots a_k\cdot x_{i+m}$ **(mod2)**

其中 m 的二進位型態為 $m=\sum_{j=0}^{k}a_j2^j$ ，$b_j=a_j2^j$

證明：

運用【性質 2】重複疊代可得

$$z_i(m)=z_i(\sum_{j=0}^{k}a_j2^j)=z_i(\sum_{j=0}^{k-1}a_j2^j+a_k\cdot 2^k)$$

$$\equiv z_i(\sum_{j=0}^{k-1}a_j2^j)+a_k\cdot z_{i+b_k}(\sum_{j=0}^{k-1}a_j2^j) \ \textbf{(mod2)}$$

$$\equiv\left(z_i(\sum_{j=0}^{k-2} a_j 2^j + a_{k-1}\cdot 2^{k-1})\right) + a_k \cdot \left(z_{i+b_k}(\sum_{j=0}^{k-2} a_j 2^j + a_{k-1}\cdot 2^{k-1})\right) \textbf{ (mod2)}$$

$$\equiv z_i(\sum_{j=0}^{k-2} a_j 2^j) + a_k \cdot z_{i+b_k}(\sum_{j=0}^{k-2} a_j 2^j) + a_{k-1}\cdot z_{i+b_{k-1}}(\sum_{j=0}^{k-2} a_j 2^j) + a_k \cdot a_{k-1}\cdot z_{i+b_k+b_{k-1}}(\sum_{j=0}^{k-2} a_j 2^j) \textbf{ (mod2)}$$

$$\equiv z_i(\sum_{j=0}^{k-3} a_j 2^j)$$

$$+ a_k \cdot z_{i+b_k}(\sum_{j=0}^{k-3} a_j 2^j) + a_{k-1}\cdot z_{i+b_{k-1}}(\sum_{j=0}^{k-3} a_j 2^j) + a_{k-2}\cdot z_{i+b_{k-2}}(\sum_{j=0}^{k-3} a_j 2^j)$$

$$+ a_k \cdot a_{k-1}\cdot z_{i+b_k+b_{k-1}}(\sum_{j=0}^{k-3} a_j 2^j) + a_k \cdot a_{k-2} z_{i+b_k+b_{k-2}}(\sum_{j=0}^{k-3} a_j 2^j) + a_{k-1}\cdot a_{k-2}\cdot z_{i+b_{k-1}+b_{k-2}}(\sum_{j=0}^{k-3} a_j 2^j)$$

$$+ a_k \cdot a_{k-1}\cdot a_{k-2}\cdot z_{i+b_k+b_{k-1}+b_{k-2}}(\sum_{j=0}^{k-3} a_j 2^j) \textbf{ (mod2)}$$

$$\equiv .....$$

$$\equiv z_i(0) + \sum_{j=0}^{k} a_j \cdot z_{i+b_j}(0) + \sum_{0\le j<l\le k} a_j \cdot a_l \cdot z_{i+b_j+b_l}(0) + ... + a_0 \cdots\cdot a_k \cdot z_{i+m}(0) \textbf{ (mod2)}$$

$$\equiv x_i + \sum_{j=0}^{k} a_j \cdot x_{i+b_j} + \sum_{0\le j<l\le k} a_j \cdot a_l \cdot x_{i+b_j+b_l} + ... + a_0 \cdots\cdot a_k \cdot x_{i+m} \textbf{ (mod2)}$$

證明完畢。'

【定理七】

若總人數 $n = 2^k$，則繼承身分會在第 ***n*** 次答後能確保收斂。

換句話說，當 $n = 2^k$ 則 $(\mathbf{A_n})^{\mathbf{x}} \equiv \mathbf{O_n}$ **(mod2)** 有解，且最小正整數解為 $x = n$

證明：

1. 首先證明第 ***n*** 次會收斂：

由【性質 1】知，

$$z_i(n) = z_i(0+2^k) \equiv z_i(0) + z_{i+2^k}(0) = z_i(0) + z_{i+n}(0) = z_i(0) + z_i(0) \equiv 0 \textbf{ (mod2)}$$

所以 $\overrightarrow{Z_n}(n) = [0,0,...,0]^T$，因此在第 n 次的時候必然收斂。

2. 接著證明前 **(*n*-1)** 次不能保證收斂：

而【定理六】又告訴我們，若收斂必然收斂到全好人，也就是說，若要收斂，則每位客人的初始身分必須被計算偶數次。然而，從【公式一】

$$z_i(m) \equiv x_i + \sum_{j=0}^{k} a_j \cdot x_{i+b_j} + \sum_{0 \le j < l \le k} a_j \cdot a_l \cdot x_{i+b_j+b_l} + ... + a_0 \cdot a_1 \cdots \cdot a_k \cdot x_{i+m} \quad \textbf{(mod2)}$$

其中 m 的二進位型態為 $m = \sum_{j=0}^{k} a_j 2^j$ ，$b_j = a_j 2^j$

可以看出，當 $m < n$ 時，x_i 必然存在，也就是說，每一位客人前 $(n\text{-}1)$ 次答題，其初始身分 x_i 都只計算過一次，這也說明了，前 $(n\text{-}1)$ 次不能保證收斂

證明完畢。

接著，對於 $n \neq 2^k$ 時 $\overrightarrow{Z_n}(m)$ 的情況，我們來進行分析。

由於【公式一】過於複雜難以從中找出訊息，而由【定理六】我們知道，

$$\overrightarrow{Z_n}(m) \text{ 收斂} \Leftrightarrow \text{存在正整數 } r \text{ 使得} (\mathbf{A_n})^{\mathbf{r}} \equiv \mathbf{O_n} \quad \textbf{(mod2)}, \; if \;\; m \ge r$$

因此，我們分析答題運算矩陣 $\mathbf{A_n}$，試著找出 $(\mathbf{A_n})^{\mathbf{m}}$ 的規律，從而解出 $\overrightarrow{Z_n}(m)$ 收斂的條件。

【定理八】若總人數 $n \ge 3$，且 n 不是 4 的倍數，則 $\overrightarrow{Z_n}(m)$ 不會收斂。

證明：

從【定理六】知道，若 $\overrightarrow{Z_n}(m)$ 收斂必然收斂到 $[0,...,0]^T$，再從【定理一】與【定理五】可知，若收斂則必然由交錯身分演變過來。

而 n 必須為偶數才有可能成為交錯身分，再者【定理二】告訴我們，答後的身分裡的騙子總數必然是偶數個，而繼承身分都是答後身份。

因此，n 必須為 4 的倍數，才有可能做到交錯身分且騙子數為偶數，

證明完畢。

至此，我們只剩下總人數 n 是 4 的倍數但不是 2^k 的形式需要討論其是否收斂。

【公式二】

若 $$\mathbf{A_{2n}}=\underbrace{\begin{bmatrix}1&1&0&\cdots&0\\0&1&1&\ddots&\vdots\\\vdots&\ddots&\ddots&\ddots&0\\0&\cdots&0&1&1\\1&0&\cdots&0&1\end{bmatrix}}_{\text{2n 行}}$$ 則 $$(\mathbf{A_{2n}})^2\equiv\underbrace{\begin{bmatrix}\mathbf{I_2}&\mathbf{I_2}&\mathbf{O_2}&\cdots&\mathbf{O_2}\\\mathbf{O_2}&\mathbf{I_2}&\mathbf{I_2}&\ddots&\vdots\\\vdots&\ddots&\ddots&\ddots&\mathbf{O_2}\\\mathbf{O_2}&\dots&\mathbf{O_2}&\mathbf{I_2}&\mathbf{I_2}\\\mathbf{I_2}&\mathbf{O_2}&\dots&\mathbf{O_2}&\mathbf{I_2}\end{bmatrix}}_{\text{n行}}\mathbf{(mod2)}$$

證明：

$$(\mathbf{A_{2n}})^2=\underbrace{\begin{bmatrix}1&2&1&0&\cdots&0\\0&1&2&1&\ddots&\vdots\\\vdots&\ddots&\ddots&\ddots&\ddots&0\\0&\cdots&0&1&2&1\\1&0&\dots&0&1&2\\2&1&0&\cdots&0&1\end{bmatrix}}_{\text{2n行}}\equiv\underbrace{\begin{bmatrix}1&0&1&0&\cdots&0\\0&1&0&1&\ddots&\vdots\\\vdots&\ddots&\ddots&\ddots&\ddots&0\\0&\cdots&0&1&0&1\\1&0&\dots&0&1&0\\0&1&0&\cdots&0&1\end{bmatrix}}_{\text{2n行}}\ \mathbf{(mod2)}$$

$$\equiv\underbrace{\begin{bmatrix}\mathbf{I_2}&\mathbf{I_2}&\mathbf{O_2}&\cdots&\mathbf{O_2}\\\mathbf{O_2}&\mathbf{I_2}&\mathbf{I_2}&\ddots&\vdots\\\vdots&\ddots&\ddots&\ddots&\mathbf{O_2}\\\mathbf{O_2}&\dots&\mathbf{O_2}&\mathbf{I_2}&\mathbf{I_2}\\\mathbf{I_2}&\mathbf{O_2}&\dots&\mathbf{O_2}&\mathbf{I_2}\end{bmatrix}}_{\text{n行}}\mathbf{(mod2)}$$

證明完畢。

【定理九】若總人數 $n\geq 3$，且 n 是 **4** 的倍數但不是 2^k 的形式，則 $\overrightarrow{Z_n}(m)$ 不會收斂。

證明：因為 $n\geq 3$，且 n 是 4 的倍數但不是 2^k 的形式

所以，n 必然可以寫成 $n=2^h\times(2p+1)$ 的形態，其中 $h\geq 2$ 且 $h,p\in N$。

考慮答題矩陣運算矩陣 $\mathbf{A_n}$ 的 2^h 次方，根據【公式二】有

$$(\mathbf{A_n})^2 \equiv \underbrace{\begin{bmatrix} \mathbf{I_2} & \mathbf{I_2} & \mathbf{O_2} & \cdots & \mathbf{O_2} \\ \mathbf{O_2} & \mathbf{I_2} & \mathbf{I_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \mathbf{O_2} \\ \mathbf{O_2} & \ldots & \mathbf{O_2} & \mathbf{I_2} & \mathbf{I_2} \\ \mathbf{I_2} & \mathbf{O_2} & \ldots & \mathbf{O_2} & \mathbf{I_2} \end{bmatrix}}_{\mathbf{2^{h-1}\times(2p+1)}\text{行}} \ (\mathbf{mod2})$$

$$\Rightarrow (\mathbf{A_n})^4 \equiv \underbrace{\begin{bmatrix} \mathbf{I_4} & \mathbf{I_4} & \mathbf{O_4} & \cdots & \mathbf{O_4} \\ \mathbf{O_4} & \mathbf{I_4} & \mathbf{I_4} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \mathbf{O_4} \\ \mathbf{O_4} & \ldots & \mathbf{O_4} & \mathbf{I_4} & \mathbf{I_4} \\ \mathbf{I_4} & \mathbf{O_4} & \ldots & \mathbf{O_4} & \mathbf{I_4} \end{bmatrix}}_{\mathbf{2^{h-2}\times(2p+1)}\text{行}} \ (\mathbf{mod2})$$

.....

$$\Rightarrow (\mathbf{A_n})^s \equiv \underbrace{\begin{bmatrix} \mathbf{I_s} & \mathbf{I_s} & \mathbf{O_s} & \cdots & \mathbf{O_s} \\ \mathbf{O_s} & \mathbf{I_s} & \mathbf{I_s} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \mathbf{O_s} \\ \mathbf{O_s} & \ldots & \mathbf{O_s} & \mathbf{I_s} & \mathbf{I_s} \\ \mathbf{I_s} & \mathbf{O_s} & \ldots & \mathbf{O_s} & \mathbf{I_s} \end{bmatrix}}_{\mathbf{(2p+1)}\text{行}} \ (\mathbf{mod2}) \text{，其中 } s = 2^h$$

因此，我們可以將 $\left((\mathbf{A_n})^s\right)^{\mathbf{m}}$ 視為 $\left(\mathbf{A_{2p+1}}\right)^{\mathbf{m}}$，其中 $\mathbf{A_{2p+1}} = \underbrace{\begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & 1 & 1 \\ 1 & 0 & \ldots & 0 & 1 \end{bmatrix}}_{\mathbf{(2p+1)}\text{行}}$

由【定理八】知，$\overrightarrow{Z_{2p+1}}(m)$ 不會收斂，

再【定理六】知，不存在正整數 m 使得 $\left(\mathbf{A_{2p+1}}\right)^{\mathbf{m}} \equiv \mathbf{O_{2p+1}}\ (\mathbf{mod2})$

從而，不存在正整數 m 使得 $\left((\mathbf{A_n})^s\right)^{\mathbf{m}} \equiv \mathbf{O_n}\ (\mathbf{mod2})$

因此，不存在正整數 m 使得 $(\mathbf{A_n})^{\mathbf{m}} \equiv \mathbf{O_n}\ (\mathbf{mod2})$，這說明了 $\overrightarrow{Z_n}(m)$ 不會收斂。

證明完畢。

至此，我們證明出了，若 $n = 2^k$，$\overrightarrow{Z_n}(m)$ 都會在第 n 次收斂到全好人，其他情況不收斂。

最後來討論一下，當 $n \neq 2^k$ 不收斂的行為，假設顧客有 n 人，每個人答題就 2 種可能，再者答後身分裡的騙子總數必為偶數，因此最多就 2^{n-1} 種不同的答後身分。所以，第 $2^{n-1}+1$ 次答後身分，必然與前 2^{n-1} 次答後身分的某一次重複，我們稱為『**循環**』。也就是說，當 $\overrightarrow{Z_n}(m)$ 不收斂時會在某次答題後開始循環，此時必然存在最大正整數 k，$1 \leq k \leq 2^{n-1}$ 使得 $\overrightarrow{Z_n}(2^{n-1}+1) = \overrightarrow{Z_n}(k)$，這裡我們把 $(2^{n-1}+1-k)$ 稱為『**循環節長**』。

名詞與符號定義 3：

當 $n \neq 2^k$ 時，我們定義符號「$s(n)$」、「$q(n)$」與「$l(n)$」分別為「開始循環答題次數」、「首次重複身分答題次數」與「循環節長度」。

其中 $1 \leq s(n) < q(n) \leq 2^{n-1}+1$ 為滿足 $\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(s(n))$ 的最小正整數數對，$l(n) = q(n) - s(n)$。

接著，透過列舉觀察 $n \neq 2^k$ 時的 $\overrightarrow{Z_n}(m)$，我們發現

1. 當 n 是奇數時 $\overrightarrow{Z_n}(m)$ **會全部循環**，即 $s(n) = 1$。
2. 當 n 是偶數時 $\overrightarrow{Z_n}(m)$ **會部分循環**，即 $s(n) > 1$。

我們在下表給出了 $n = 3 \sim 17$ 且非 2 的冪次方時滿足 $\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(s(n))$ 的最小整數數對。

其中 $1 \leq s(n) < q(n) \leq 2^{n-1}+1$；循環節長 $l(n) = q(n) - s(n)$

n	3	5	6=2*3	7	9	10=2*5	11	12=4*3	13	14=2*7	15	17
$q(n)$	2^2			2^3							2^4	
		4^2			8^2							16^2
			2*4			2*16		4*4		2*8		
							342		820			
$s(n)$	1	1	2	1	1	2	1	4	1	2	1	1
$l(n)$	3	15	6	7	63	30	341	12	819	14	15	255

表格為本團隊自製

由上表我們有底下的猜測：

(1) $n=2^k+1$ 時 則 $q(n)=(n-1)^2$，$s(n)=1$　　(2) $n=2^k-1$ 時 則 $q(n)=n+1$，$s(n)=1$

(3) n 是奇數，$n\neq 2^k\pm 1$ 時 則 $q(n)=n\cdot(2^{\frac{n-1}{2}}-1)+1$，$s(n)=1$

(4) $n\neq 2^k$ 且是偶數，此時 n 可寫成 $n=2^h\times(2p+1)$，則 $q(n)=s(n)\cdot q(2p+1)$，$s(n)=2^h$

【定理十】若總人數 $n\geq 3$

(1) $n=2^k+1$，$k\geq 2$，則 $\overrightarrow{Z_n}((n-1)^2)=\overrightarrow{Z_n}(1)$

(2) $n=2^k-1$，$k\geq 2$，則 $\overrightarrow{Z_n}(n+1)=\overrightarrow{Z_n}(1)$

證明：

(1) $n=2^k-1$ 時，由【性質 1】可知，

$z_i(n+1)=z_i(2^k)\equiv z_i(0)+z_{i+2^k}(0)=z_i(0)+z_{i+n+1}(0)=z_i(0)+z_{i+1}(0)\equiv z_i(1)$ **(mod2)**，

所以 $\overrightarrow{Z_n}(n+1)\equiv\overrightarrow{Z_n}(1)$ **(mod2)**

(2) $n=2^k+1$ 時，由【性質 1】可知，

$z_i((n-1)^2)=z_i(2^{2k})\equiv z_i(0)+z_{i+2^{2k}}(0)$ **(mod2)**，

而 $z_{i+2^{2k}}(0)=z_{i+(n-1)^2}(0)=z_{i+n(n-2)+1}(0)=z_{i+1}(0)$ 帶入上式

得 $z_i((n-1)^2)\equiv z_i(0)+z_{i+1}(0)=z_i(1)$ **(mod2)**，所以 $\overrightarrow{Z_n}((n-1)^2)\equiv\overrightarrow{Z_n}(1)$ **(mod2)**

證明完畢。

【定理十一】

1. 『若 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n}(s)$ 則 $\overrightarrow{Z_n}(q-1)=\overrightarrow{Z_n}(s-1)$ 或 $\overrightarrow{Z_n}(q-1)=\overrightarrow{Z_n}^c(s-1)$，其中 $1\leq s<q$』

也就是說，『答後身分若相同，則答題身分必為相同或是互補。』

2. 『已知 n 是奇數，若 $\overrightarrow{Z_n}(q+1)=\overrightarrow{Z_n}(s+1)$ 則 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n}(s)$，其中 $1\leq s<q$』

也就是說，『若總人數 n 是奇數，且答後身分若相同，則答題身分必相同。』

證明：

1. 證明第一部分：

令 $\overrightarrow{Z_n}(q-1)=[q_1,q_2,...,q_n]^T$ ， $\overrightarrow{Z_n}(s-1)=[s_1,s_2,...,s_n]^T$

而 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n}(s)$ ，所以 $A_n\cdot\overrightarrow{Z_n}(q-1)\equiv A_n\cdot\overrightarrow{Z_n}(s-1)$ **(mod2)**

所以對於 $i=1,2,...,n$ 有 $q_i+q_{i+1}\equiv s_i+s_{i+1}$ **(mod2)**

若 $q_i=0,q_{i+1}=0$ 則 $s_i+s_{i+1}\equiv 0$ **(mod2)** $\Rightarrow s_i=0,s_{i+1}=0$ 或 $s_i=1,s_{i+1}=1$

若 $q_i=0,q_{i+1}=1$ 則 $s_i+s_{i+1}\equiv 1$ **(mod2)** $\Rightarrow s_i=0,s_{i+1}=1$ 或 $s_i=1,s_{i+1}=0$

若 $q_i=1,q_{i+1}=0$ 則 $s_i+s_{i+1}\equiv 1$ **(mod2)** $\Rightarrow s_i=1,s_{i+1}=0$ 或 $s_i=0,s_{i+1}=1$

若 $q_i=1,q_{i+1}=1$ 則 $s_i+s_{i+1}\equiv 0$ **(mod2)** $\Rightarrow s_i=1,s_{i+1}=1$ 或 $s_i=0,s_{i+1}=0$

因此 $q_i=s_i$ 或 $q_i=1-s_i$

換句話說，$\overrightarrow{Z_n}(q-1)=\overrightarrow{Z_n}(s-1)$ 或是 $\overrightarrow{Z_n}(q-1)=\overrightarrow{Z_n^c}(s-1)$ 。**得證第一部分。**

2. 證明第二部分：

已知 n 是奇數，當 $\overrightarrow{Z_n}(q+1)=\overrightarrow{Z_n}(s+1)$ 時，由第一部分可知 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n}(s)$ 或是 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n^c}(s)$ ，然而，$\overrightarrow{Z_n}(q)$ 與 $\overrightarrow{Z_n}(s)$ 都是答後身分向量，從【定理二】可知，答後身分的騙子總數必為偶數，也就是說 $\overrightarrow{Z_n}(q)$ 與 $\overrightarrow{Z_n}(s)$ 裡都會有偶數個 1。而 n 是奇數，所以 $\overrightarrow{Z_n}(s)$ 的互補身分 $\overrightarrow{Z_n^c}(s)$ 裡的 1 有奇數個。

因此 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n^c}(s)$ 不合理，所以 $\overrightarrow{Z_n}(q)=\overrightarrow{Z_n}(s)$ 。**得證第二部分。**

證明完畢。

從【定理十一】的結果可知，雖然運算矩陣 **An** 在"mod 2"之下 是不可逆的運算，

但若是 n 為奇數，對於繼承身分 $\overrightarrow{Z_n}(m+1)$ 而言卻存在唯一的繼承身分 $\overrightarrow{Z_n}(m)$ 使得

$$\overrightarrow{Z_n}(m+1)\equiv \mathbf{A_n}\,\overrightarrow{Z_n}(m)\ \ \textbf{(mod2)}$$

這說明了，當 n 為奇數時，**An** 在"mod 2"之下在應該有著類似於逆矩陣的反運算。
即，當 n 是奇數時，存在矩陣 **Bn** 使得

$$\mathbf{B_n}\overrightarrow{Z_n}(m+1)\equiv\mathbf{B_n}(\mathbf{A_n})^{\mathbf{m}}\overrightarrow{Z_n}(1)\equiv(\mathbf{A_n})^{\mathbf{m-1}}\overrightarrow{Z_n}(1)\ \equiv\overrightarrow{Z_n}(m)\ \ \mathbf{(mod2)}\text{，}m\in N\text{。}$$

參考廣義逆矩陣的定義[6]，將我們將這樣的矩陣 **Bn** 稱為 **An** 的『**廣義(模 2)逆矩陣**』。

名詞與符號定義 4：

1. 若矩陣 $\mathbf{A_n},\mathbf{B_n}$，滿足下列兩個條件，我們 **Bn** 稱為 **An** 的『**廣義(模 2)逆矩陣**』。

   $\mathbf{(1)\ A_nB_n\equiv B_nA_n\ \ (mod2)}$ $\qquad$ $\mathbf{(2)\ \ A_nB_nA_n\equiv A_n\ \ (mod2)}$

   ★ 特別說明，$\mathbf{A_nB_n\not\equiv I_n\ \ (mod2)}$ 且『**廣義(模 2)逆矩陣**』**並非唯一的**。

   另外，當條件(1)、(2)都滿足時，不難得知 $\mathbf{B_n}\left(\mathbf{A_n}\right)^{\mathbf{m+1}}\equiv\left(\mathbf{A_n}\right)^{\mathbf{m}}\ \ \mathbf{(mod2)}$

2. 一個 n 階方陣所有的元素都是 1，我們以 $\mathbf{1_n}$ 表示，即 $\mathbf{1_n}=\begin{bmatrix}1&\cdots&1\\ \vdots&\ddots&\vdots\\ 1&\cdots&1\end{bmatrix}_{n\times n}$

接著尋找，**An** 的『**廣義(模 2)逆矩陣**』，其中 n 是奇數。首先考慮 n=3,5,7,9 的情況

因為 $\mathbf{A_3(A_3)^2(A_3)=(A_3)^4\equiv A_3\ \ (mod2)}$，$\mathbf{A_5(A_5)^{14}(A_5)=(A_5)^{16}\equiv A_5\ \ (mod2)}$，

$\mathbf{A_7(A_7)^6A_7=(A_7)^8\equiv A_7\ \ (mod2)}$，$\mathbf{A_9(A_9)^{62}A_9=(A_9)^{64}\equiv A_9\ \ (mod2)}$

因此，『**廣義(模 2)逆矩陣**』的訊息，應該就在 $\mathbf{(A_3)^2}$、$\mathbf{(A_5)^{14}}$、$\mathbf{(A_7)^6}$ 與 $\mathbf{(A_9)^{62}}$ 的形態裡。

定義 $\mathbf{B_n}=[b_{ij}]_{n\times n}$，其中 $b_{i,j}=\begin{cases}1,\ if\ \ (i\le j)\wedge(i+j\ is\ \text{even})\\ 1,\ if\ \ (i>j)\wedge(i+j\ is\ \text{odd})\\ 0,\ \text{otherwise}\end{cases}$

我們有 $\mathbf{(A_3)^2\equiv B_3\ \ (mod2)}$，$\mathbf{(A_5)^{14}\equiv 1_5+B_5\ \ (mod2)}$，

$\mathbf{(A_7)^6\equiv B_7\ \ (mod2)}$，$\mathbf{(A_9)^{62}\equiv 1_9+B_9\ \ (mod2)}$

而對於一個答後身分向量$\overrightarrow{Z_n}(m)$而言，從【定理二】可知，$\overrightarrow{Z_n}(m)$裡有偶數個 1

因此我們有 $(\mathbf{1_n}+\mathbf{B_n})\overrightarrow{Z_n}(m)=\mathbf{1_n}\overrightarrow{Z_n}(m)+\mathbf{B_n}\overrightarrow{Z_n}(m)\equiv\mathbf{B_n}\overrightarrow{Z_n}(m)$ **(mod2)**

現在我們來證明，當 n 是奇數時，這樣的 $\mathbf{B_n}$ 確實是 $\mathbf{A_n}$ 的一個『**廣義(模 2)逆矩陣**』

【定理十二】

已知 n 為奇數，且 $\mathbf{A_n}=\left[a_{i,j}\right]_{n\times n}$，其中 $a_{i,j}=\begin{cases}1\ ,\ if\ j=i\ \vee\ j=i+1\\0\ ,\ otherwise\end{cases}$

則 $\mathbf{B_n}=[b_{i,j}]_{n\times n}$，其中 $b_{i,j}=\begin{cases}1,\ if\ \ (i\le j)\wedge(i+j\ is\ \text{even})\\1,\ if\ \ (i>j)\wedge(i+j\ is\ \text{odd})\\0,\ \text{otherwise}\end{cases}$ 為 $\mathbf{A_n}$ 的『**廣義(模 2)逆矩陣**』。

證明：

第一部分：證明 $\mathbf{A_nB_n}\equiv\mathbf{B_nA_n}$ (mod2)

令 $\mathbf{A_nB_n}=\left[c_{i,j}\right]_{n\times n}$，其中 $c_{i,j}=\sum_{k=1}^{n}a_{i,k}\cdot b_{k,j}=b_{i,j}+b_{i+1,j}$，其中 $b_{n+i,j}=b_{i,j}$

(1) 當 $1\le i<j\le n$ 時，可知 $(i+1)\le j$，因為 $(i+j)$ 與 $(i+1+j)$ 為一奇與一偶，

因此 $b_{i,j}$ 與 $b_{i+1,j}$ 為一個 0 與一個 1，故 $c_{i,j}=1$

(2) 當 $1\le i=j\le n$ 時，$c_{i,j}=c_{i,i}=b_{i,i}+b_{i+1,i}=1+1=2\equiv 0$ **(mod2)**，

(3) 當 $1\le j<i\le n-1$ 時，可知 $i+1>j$，因為 $(i+j)$ 與 $(i+1+j)$ 為一奇與一偶，

因此 $b_{i,j}$ 與 $b_{i+1,j}$ 為一個 0 與一個 1，故 $c_{i,j}=1$

(4) 當 $i=n$ 時，因為 n 是奇數，

(I) 當 $j=1,2,....,(n-1)$ 時，

有 $b_{n,j}=\begin{cases}1\ ,\ if\ j\ is\ even\\0\ ,\ if\ j\ \text{odd}\end{cases}$，$b_{1,j}=\begin{cases}0\ ,\ if\ j\ is\ even\\1\ ,\ if\ j\ is\ \text{odd}\end{cases}$，此時 $c_{i,j}=1$

(II) 當 $j=n$，此時 $c_{i,j}=c_{n,n}=b_{n,n}+b_{n+1,n}=b_{n,n}+b_{1,n}=1+1\equiv 0$ **(mod2)**

得 $\mathbf{A_nB_n}=\left[c_{i,j}\right]_{n\times n}$，其中 $c_{i,j}\equiv\begin{cases}1\ ,if\ \ i\ne j\\0\ ,if\ \ i=j\end{cases}$ **(mod2)**

接著令$\mathbf{B_n A_n}=\left[c*_{i,j}\right]_{n\times n}$，其中$c*_{i,j}=\sum_{k=1}^{n} b_{i,k}\cdot a_{k,j}=b_{i,j-1}\cdot a_{j-1,j}+b_{i,j}\cdot a_{j,j}=b_{i,j-1}+b_{i,j}$，

其中$a_{0,j}=a_{n,j}$ 且 $b_{i,0}=b_{i,n}$

(5) 當$1\le i=j\le n$時，$c*_{i,j}=c*_{i,i}=b_{i,i-1}+b_{i,i}=1+1=2\equiv 0$ **(mod2)**

(6) 當$1\le i<j\le n$時，$c*_{i,j}=b_{i,j-1}+b_{i,j}$，因為$(i+j-1)$與$(i+j)$為一奇與一偶，

因此 $b_{i,j-1}$與$b_{i,j}$為一個 0 與一個 1，故$c*_{i,j}=1$

(7) 當$2\le j<i\le n$時，$c*_{i,j}=b_{i,j-1}+b_{i,j}$，因為$(i+j-1)$與$(i+j)$為一奇與一偶，

因此 $b_{i,j-1}$與$b_{i,j}$為一個 0 與一個 1，故$c*_{i,j}=1$

(8) 當$j=1$時，$c*_{i,j}=c*_{i,1}=b_{i,0}+b_{i,1}=b_{i,n}+b_{i,1}$

(I) 當$i=1$時，$c*_{1,1}=b_{1,n}+b_{1,1}=1+1=2\equiv 0$ **(mod2)**

(II) 當$i=2,3,....,n$時，因為n是奇數

所以$b_{i,n}=\begin{cases}0, & if\ \ i\ is\ even\\ 1, & if\ \ i\ is\ \text{odd}\end{cases}$，而 $b_{i,1}=\begin{cases}1, & if\ \ i\ is\ even\\ 0, & if\ \ i\ is\ \text{odd}\end{cases}$，此時 $c*_{i,j}=1$

$$\text{得}\ \mathbf{B_n A_n}=\left[c*_{i,j}\right]_{n\times n}，\text{其中}\ c*_{i,j}\equiv\begin{cases}1\ ,if\ \ i\ne j\\ 0\ ,if\ \ i=j\end{cases}\ \textbf{(mod2)}$$

所以有 $\mathbf{A_n B_n}\equiv\mathbf{B_n A_n}$ **(mod2)**，得證第一部分。

第二部分：證明 $\mathbf{A_n B_n A_n}\equiv\mathbf{A_n}$ (mod2)

令$\mathbf{A_n B_n A_n}=\left[d_{i,j}\right]_{n\times n}$，其中$d_{i,j}=\sum_{k=1}^{n} c_{i,k}\cdot a_{k,j}=c_{i,j-1}+c_{i,j}$，而$c_{i,0}=c_{i,n}$，

(1) 當$1\le i<j-1\le n$時，$d_{i,j}=c_{i,j-1}+c_{i,j}=1+1\equiv 0$ **(mod2)**

(2) 當$1\le i=j-1\le n$時，$d_{i,j}=d_{i,i+1}=c_{i,i}+c_{i,i+1}=0+1=1$

(3) 當$1\le i=j\le n$時，$d_{i,j}=d_{i,i}=c_{i,i-1}+c_{i,i}=1+0=1$

(4) 當$1 \le j < i \le n-1$時，$d_{i,j} = c_{i,j-1} + c_{i,j} = 1+1 \equiv 0$ **(mod2)**

(5) 當$1 \le j < i = n$時，

(I) 當 $j=1$時，$d_{i,j} = d_{n,1} = c_{n,0} + c_{n,1} = c_{n,n} + c_{1,1} = 1+0 = 1$

(II) 當 $j = 2,...,(n-1)$時，$d_{i,j} = d_{n,j} = c_{n,j-1} + c_{n,j} = 1+1 \equiv 0$ **(mod2)**

(III) 當 $j = n$時，$d_{i,j} = d_{n,n} = c_{n,n-1} + c_{n,n} = 1+0 = 1$

所以有$d_{i,j} \equiv a_{i,j}$ **(mod2)**，從而得知 $\mathbf{A_n B_n A_n} \equiv \mathbf{A_n}$ **(mod2)**，得證第二部分。

證明完畢。

【定理十三】

『若 n 是奇數，**則存在最小正整數**$q(n) > 1$**使得** $\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(1)$ 。』

即，『當 n 是奇數時 則 $s(n) = 1$ 。**此時**$\overrightarrow{Z_n}(m)$ **會全部循環。』**

證明：因為 n 為奇數，所以$\overrightarrow{Z_n}(m)$不會收斂。

因此，必然存在最小正整數數對$1 \le s(n) < q(n) \le 2^{n-1} + 1$ 使得 $\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(s(n))$ ，

也就是 $(\mathbf{A_n})^{\mathbf{q(n)}} \overrightarrow{X_n} \equiv (\mathbf{A_n})^{\mathbf{s(n)}} \overrightarrow{X_n}$ **(mod2)**

若$s(n) > 1$，因為 n 是奇數，所以 $\mathbf{A_n}$ 的『**廣義(模 2)逆矩陣**』$\mathbf{B_n}$ 存在，

因此，$\mathbf{B_n}(\mathbf{A_n})^{\mathbf{q(n)}} \overrightarrow{X_n} \equiv \mathbf{B_n}(\mathbf{A_n})^{\mathbf{s(n)}} \overrightarrow{X_n}$ **(mod2)**

$\Rightarrow (\mathbf{A_n})^{\mathbf{q(n)-1}} \overrightarrow{X_n} \equiv (\mathbf{A_n})^{\mathbf{s(n)-1}} \overrightarrow{X_n}$ **(mod2)**

$\Rightarrow \overrightarrow{Z_n}(q(n-1)) = \overrightarrow{Z_n}(s(n-1))$

所以$s(n), q(n)$不是滿足$\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(s(n))$的最小整數數對，矛盾。

所以$s(n) = 1$。

證明完畢。

最後我們討論，當$n=2^h\times p$時，其中 p 是正奇數，$\overrightarrow{Z_n}(m)$ 又會從甚麼時候開始循環。

【定理十四】

『若$n=2^h\times p$，則存在正整數$q^*(n)$使得$\overrightarrow{Z_n}(q^*(n))=\overrightarrow{Z_n}(2^h)$』，其中$h\in N$，$p$ 是正奇數。

證明：

令$\mathbf{s}=2^h\ge 2$， 考慮$\mathbf{A_n}$的 s 次方，根據【公式一】有

$$(\mathbf{A_n})^{\mathbf{s}}\equiv\underbrace{\begin{bmatrix}\mathbf{I_s} & \mathbf{I_s} & \mathbf{O_s} & \cdots & \mathbf{O_s}\\ \mathbf{O_s} & \mathbf{I_s} & \mathbf{I_s} & \ddots & \vdots\\ \vdots & \ddots & \ddots & \ddots & \mathbf{O_s}\\ \mathbf{O_s} & \dots & \mathbf{O_s} & \mathbf{I_s} & \mathbf{I_s}\\ \mathbf{I_s} & \mathbf{O_s} & \dots & \mathbf{O_s} & \mathbf{I_s}\end{bmatrix}}_{\mathbf{p}\text{行}}\ (\mathbf{mod2})\text{， 比對 }\mathbf{A_p}=\underbrace{\begin{bmatrix}1 & 1 & 0 & \cdots & 0\\ 0 & 1 & 1 & \ddots & \vdots\\ \vdots & \ddots & \ddots & \ddots & 0\\ 0 & \dots & 0 & 1 & 1\\ 1 & 0 & \dots & 0 & 1\end{bmatrix}}_{\mathbf{p}\text{行}}$$

因為p是奇數，所以$\mathbf{A_p}$存在著『廣義(模 2)逆矩陣』$\mathbf{B_p}$，使得$\mathbf{B_p}\left(\mathbf{A_p}\right)^{\mathbf{2}}\equiv\mathbf{A_p}$ $(\mathbf{mod2})$

從而$(\mathbf{A_n})^{\mathbf{s}}$存在著『廣義(模 2)逆矩陣』$\mathbf{B_n}$，使得$\mathbf{B_n}\left((\mathbf{A_n})^{\mathbf{s}}\right)^{\mathbf{2}}\equiv(\mathbf{A_n})^{\mathbf{s}}$ $(\mathbf{mod2})$。

然後我們考慮每 s 次答題後的繼承身分向量，$\overrightarrow{Z_n}(s),\overrightarrow{Z_n}(2s),\overrightarrow{Z_n}(3s),....$，

因為$\overrightarrow{Z_n}(m)$最多就2^{n-1}種不同的身分，所以$\overrightarrow{Z_n}\left((2^{n-1}+1)\cdot s\right)$必然與之前的某一項重複。

也就是說存在整數 k，其中$1\le k\le 2^{n-1}$，使得$\overrightarrow{Z_n}\left((2^{n-1}+1)\cdot s\right)=\overrightarrow{Z_n}\left(k\cdot s\right)$

令$r=2^{n-1}+1>k$，則有$(\mathbf{A_n})^{\mathbf{r\cdot s}}\overrightarrow{X_n}\equiv(\mathbf{A_n})^{\mathbf{k\cdot s}}\overrightarrow{X_n}$ $(\mathbf{mod2})$

$$\Rightarrow\left((\mathbf{A_n})^{\mathbf{s}}\right)^{\mathbf{r}}\overrightarrow{X_n}\equiv\left((\mathbf{A_n})^{\mathbf{s}}\right)^{\mathbf{k}}\overrightarrow{X_n}\quad(\mathbf{mod2})$$

$$\Rightarrow(\mathbf{B_n})^{\mathbf{k-1}}\left((\mathbf{A_n})^{\mathbf{s}}\right)^{\mathbf{r}}\overrightarrow{X_n}\equiv(\mathbf{B_n})^{\mathbf{k-1}}\left((\mathbf{A_n})^{\mathbf{s}}\right)^{\mathbf{k}}\overrightarrow{X_n}\quad(\mathbf{mod2})$$

$$\Rightarrow\left((\mathbf{A_n})^{\mathbf{s}}\right)^{\mathbf{r-k+1}}\overrightarrow{X_n}\equiv(\mathbf{A_n})^{\mathbf{s}}\overrightarrow{X_n}\quad(\mathbf{mod2})$$

$$\Rightarrow\overrightarrow{Z_n}\left((r-k+1)\cdot s\right)=\overrightarrow{Z_n}\left(s\right)$$

證明完畢。

伍、研究結果：

對於全好人、全壞人的初始身分，答題後就會是全好人，從而繼承身分收斂，而交錯身分再答題後就變成全壞人，同樣會使得繼承身分在下一次繼承時就收斂。我們分析的是對於一般的初始身分，都能夠有的性質。

1. 關於答後身分，我們證明出底下的結果：

   甲、若答後身分是全老實人，則初始身分是全老實人或全騙子。

   乙、答後身分的騙子總數必然為偶數。

   丙、若答後身分等於初始身分，則初始身分為全老實人。

   丁、若初始身分互補，則答後身分相同。

   戊、若答後身分是全騙子，則初始身分為交錯身分。

2. 關於繼承身分 $\overrightarrow{Z_n}(m)$ ，我們證明出底下的結果：

   甲、當 $n=2^k$ ，$\overrightarrow{Z_n}(m)$ 都會在第 n 次收斂到全好人。

   乙、當 $n\neq 2^k$ ，$\overrightarrow{Z_n}(m)$ 不會收斂，會進入循環。

   i. 當 n 是奇數時，則存在最小整數 $q(n)$ 使得 $\overrightarrow{Z_n}(q(n))=\overrightarrow{Z_n}(1)$

      1. $n=2^k+1$ ，$k\geq 2$ ，則 $\overrightarrow{Z_n}((n-1)^2)=\overrightarrow{Z_n}(1)$

      2. $n=2^k-1$ ，$k\geq 2$ ，則 $\overrightarrow{Z_n}(n+1)=\overrightarrow{Z_n}(1)$

   ii. 當 n 是偶數時，可將 n 表示成為 $n=2^h\times p$ ，$h\in N$ 且 p 是正奇數

   則存在整數 $q^*(n)$ 使得 $\overrightarrow{Z_n}(q^*(n))=\overrightarrow{Z_n}(2^h)$

陸、未來展望：

當 $n \neq 2^k$ 時 $\overrightarrow{Z_n}(m)$ 不收斂會進入循環，也就是，存在最小正整數對$(q(n), s(n))$，

使得 $\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(s(n))$，其中 $1 \leq s(n) < q(n) \leq 2^{n-1} + 1$，循環節長 $l(n) = q(n) - s(n)$。

這說明了，答後身分向量會從第 $s(n)$ 次答題開始，每隔 $l(n)$次答題循環一次。雖然在【定理十】到【定理十四】有證明出我們所猜測出的部分結果，但仍有很大的努力空間，我們將持續朝著完善這個部分而努力。

柒、參考文獻與資料：

[1]. 游森棚(2024.4)。騙子或老實人，科學研習期刊 NO.63-02

https://www.ntsec.gov.tw/article/detail.aspx?a=5420

[2]. 南一書局，高中數學課本第四冊 A (P.169-P.217)

[3]. 中山大學雙週一題網路數學問題徵答 113 學年度第 1 學期第五題

https://www-math.nsysu.edu.tw/~problem/

[4]. 維基百科-分塊矩陣的乘法

https://zh.wikipedia.org/zh-tw/%E5%88%86%E5%A1%8A%E7%9F%A9%E9%99%A3

[5]. 周志成(2013.07.15)，線代啟示錄-有限體與模算術

https://ccjou.wordpress.com/2013/07/15/%E6%9C%89%E9%99%90%E9%AB%94%E8%88%87%E6%A8%A1%E7%AE%97%E8%A1%93/

[6]. 維基百科-廣逆矩陣

https://zh.wikipedia.org/wiki/%E5%B9%BF%E4%B9%89%E9%80%86%E9%98%B5

【評語】050418

本作品討論"老實人和騙子"的遊戲，窮舉了人數少的情形，也討論了一些以 0，1 為係數的轉移矩陣。不過其實本質上是一個特殊形式的轉移矩陣問題。作者最終證明，一定能收斂到所有人都是老實人若且唯若 n 是 2 的乘冪,並且證明不收斂的情形下會產生循環。作者並未發現本題蘊含許多抽象代數的結構，略為可惜. 結果不多，但整體而言是個認真的作品。

作品海報

負負得正

研究摘要

一群彼此熟識的朋友在小吃店圍桌而坐，每個人可能是老實人(只說實話)，也有可能是騙子(只說謊話)。由老闆的提問「坐在你右邊的是騙子還是老實人？」，之後由每位顧客進行回答。

那我們延伸問題，**如果讓答題者繼承所答的身分呢？**

舉例來說：如果小明的回答是老實人，那麼小明的身分在答題後就會變成老實人。(繼承身分後進行第二輪答題、第三輪答題、......)。在文中我們解出當顧客人數是 2^k 時繼承身分會收斂，並在第 2^k 次必然收斂到全好人；若顧客人數不是 2^k 時，則會產生循環。

壹、研究動機

在科學研習期刊第63卷第二期的特約專欄中「森棚教官數學題─騙子或老實人」，看到了這個有趣的題目：『五位熟識的朋友在小吃店圍著圓桌而坐，但是每個人可能是騙子(永遠說謊)，也可能是老實人(永遠誠實)。老闆問每一個人坐在他右邊的人是騙子還是老實人，然後統計答案』。在解題過程當中，我們發現了些有趣的現象以及可以延伸討論，因此有了本文的討論。

貳、研究目的

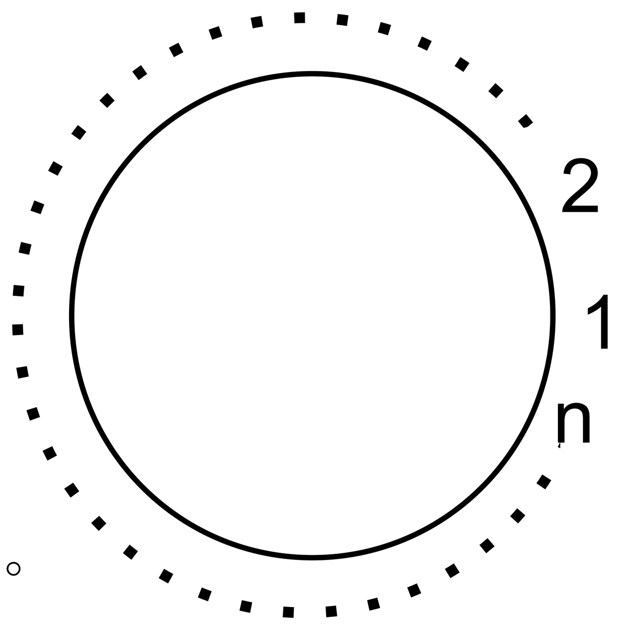
1. 找出n位顧客答題後有規律的部分並加以證明。
2. 延伸問題，假設答題者會繼承所答的身分，進行第二次答題，第三次答題、...，我們想了解的是，對於任意的初始身分，需要何種的條件才能保證答後身分收斂，以及幾次後能保證收斂。若不收斂，則找出循環規則並加以證明。

參、研究設備

紙、筆、電腦。

肆、研究方法

我們將圓周上n位置給予逆時針編號 1,2,...,n ，如右圖



一、名詞與符號定義1

1. **初始身分向量 $\overrightarrow{X_n}=[x_1,x_2,...,x_n]^T$**

   將這n人的身分以 $\overrightarrow{X_n}=[x_1,x_2,...,x_n]^T$ 來表示，稱為『初始身分向量』。

   其中，如果第i個位置是老實人，則 $x_i = 0$，否則 $x_i = 1$。

2. **答後身分向量 $\overrightarrow{Y_n}=[y_1,y_2,...,y_n]^T$**

   將回答的結果以$\overrightarrow{Y_n}=[y_1,y_2,...,y_n]^T$表示，稱為『答後身分向量』。

   也就是，如果第i個位置的回答是騙子，則 $y_i=1$，否則 $y_i= 0$。

3. **互補身分向量 $\overrightarrow{X_n}^c=[1-x_1,1-x_2,...,1-x_n]^T$**

   將每個位置的身分變換後，老實人換成騙子，騙子換成老實人，所得到的身分向量，稱為『互補身分向量』。

4. **交錯身分向量 $\overrightarrow{X_{2m}}=[1,0,1,0,...,1,0]^T$或是 $\overrightarrow{X_{2m}}=[0,1,0,1,...,0,1]^T$**

   有2m個人圍桌而坐，騙子與老實人各半，且2m個人的身分圓桌上形成騙子與老實人的交錯排列，則稱這樣向量為交錯身分向量。

二、列舉顧客人數，並觀察其共同現象

1. 顧客2人:初始身分 $\overrightarrow{X_2}=[x_1,x_2]^T$，答後身分 $\overrightarrow{Y_2}=[y_1,y_2]^T$

x_1	0	0	1	1
x_2	0	1	0	1

⟶

y_1	0	1	1	0
y_2	0	1	1	0

2. 顧客3人:初始身分 $\overrightarrow{X_3}=[x_1,x_2,x_3]^T$，答後身分 $\overrightarrow{Y_3}=[y_1,y_2,y_3]^T$

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1

⟶

y_1	0	0	1	1	1	1	0	0
y_2	0	1	1	0	0	1	1	0
y_3	0	1	0	1	1	0	1	0

三、定義答題運算

考慮 $\overrightarrow{X_n}=[x_1,x_2,\ldots,x_n]^T$ 與 $\overrightarrow{Y_n}=[y_1,y_2,\ldots,y_n]^T$ 之間的對應關係

令 $x_{n+1}=x_1$ ，則對於 i=1,2,...,n 我們有

(1) 若 $x_i=0$ 且 $x_{i+1}=0$ 則 $y_i=0=x_i+x_{i+1}$

(2) 若 $x_i=0$ 且 $x_{i+1}=1$ 則 $y_i=1=x_i+x_{i+1}$

(3) 若 $x_i=1$ 且 $x_{i+1}=0$ 則 $y_i=1=x_i+x_{i+1}$

(4) 若 $x_i=1$ 且 $x_{i+1}=1$ 則 $y_i=0\equiv x_i+x_{i+1}$ **(mod2)**

綜合以上 (1)~(4) 可知 $y_i\equiv x_i+x_{i+1}$ **(mod2)**

我們定義一個答題運算矩陣 $\mathbf{A_n}$ ，來表示 $\overrightarrow{X_n}$ 與 $\overrightarrow{Y_n}$ 之間的轉換關係，如下

$$\mathbf{A_n}=\begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$$

也就是 $\mathbf{A_n}=[a_{i,j}]_{n\times n}$ ，其中 $a_{i,j}=\begin{cases}1, \text{ if } j=i \vee j=i+1 \\ 0, \text{ otherwise}\end{cases}$ ，另外 $a_{n,n+1}=a_{n,1}$

於是有 $\overrightarrow{Y_n}\equiv \mathbf{A_n}\overrightarrow{X_n}$ **(mod2)**

四、分析答後身分

【定理一】若答後身分為全老實人，則初始身分是全老實人或全騙子

【定理二】答後的騙子總數必然為偶數

【定理三】若答後身分等於初始身分，則初始身分為全老實人

【定理四】若初始身分互補，則答後身分相同

【定理五】若答後身分為全騙子，則初始身分為交錯身分

五、延伸討論

接下來討論讓答題者繼承所答身分的玩法。如果怎麼回答身分都一樣，就稱為「**收斂**」。如果繼承身分不收斂，則會發生「**循環**」。

六、名詞與符號定義2

1. **繼承身分向量** $\overrightarrow{\mathbf{Z}_n}\mathbf{(m)=[z_1(m),z_2(m),z_3(m),\ldots\ldots,z_n(m)]^T}$，其中 m≧0 ，且m∈$Z$，代表繼承 m 次身分。其中$\overrightarrow{\mathbf{Z}_n}\mathbf{(0)}$ 是初始身分。
2. **在本文中** $\mathbf{z_{n+i}(m)=z_i(m)}$**，**$\mathbf{x_{n+i}=x_i}$**。**
3. **特殊方陣**

一個 n 階的方陣所有元素都是0，則以 $\mathbf{O_n}$ 表示。

一個 n 階的單位方陣，則以 $\mathbf{I_n}$ 表示。

【定理六】1.若繼承身分收斂，則必然收斂到全好人。

2.若 $\overrightarrow{Z_n}(m)$ 收斂，則存在正整數 r 使得 $(\mathbf{A}_n)^m\equiv\mathbf{O}_n$ **(mod2)**。其中m≧r，r≧0 ，r∈Z。

【定理七】若總人數 $n=2^k$，則繼承身分在第n次保證收斂，即 $(\mathbf{A}_n)^n\equiv\mathbf{O}_n$ **(mod2)** 。

【定理八】若總人數 n≧3，n 不是4的倍數，則 $\overrightarrow{Z_n}(m)$ 不會收斂。即不存在 r 使得 $(\mathbf{A}_n)^r\equiv\mathbf{O}_n$ **(mod2)** 。

【定理九】若總人數 n≧3，n 是4的倍數，但不屬於 2^k的形式，則 $\overrightarrow{Z_n}(m)$ 不會收斂。

【性質一】對於所有非負整數 k，恆有 $z_i(m+2^k)\equiv z_i(m)+z_{i+2^k}(m)$ **(mod2)**

【性質二】對於 a= 0,1， $z_i(m+a\cdot 2^k)\equiv z_i(m)+a\cdot z_{i+a\,2^k}(m)$ **(mod2)**

【公式一】$z_i(m)\equiv x_i+\sum_{j=0}^{k}a_j\cdot x_{i+b_j}+\sum_{0\le j<l\le k}a_j\cdot a_l\cdot x_{i+b_j+b_l}+\ldots+a_0\cdot a_1\cdot\ldots\cdot a_k\cdot x_{i+m}$ **(mod2)**

其中 m 的二進位型態為 $m=\sum_{j=0}^{k}a_j2^j$ ，$b_j=a_j2^j$

【公式二】如下圖

若 $A_{2n}=\begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix}_{2n\times 2n}$ 則 $(A_{2n})^2\equiv\begin{bmatrix} I_2 & I_2 & O_2 & \cdots & O_2 \\ O_2 & I_2 & I_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & O_2 \\ O_2 & \cdots & O_2 & I_2 & I_2 \\ I_2 & O_2 & \cdots & O_2 & I_2 \end{bmatrix}_{n\times n}$ **(mod2)**

七、名詞與符號定義3

如果繼承身分不收斂，並與前面某次的答題結果相同，我們稱為**「循環」**。

所以，若 $\overrightarrow{Z_n}(m)$ 不收斂則存在最小數對(s(n) , q(n))，使得 $\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(s(n))$，其中$1 \leqq s(n) < q(n) \leqq 2^{n-1}+1$，從而循環節長 $l(n) = q(n) - s(n)$。

【定理十】若總人數 $n \geqq 3$

(1) $n = 2^k+1$，$k \geqq 2$，則 $\overrightarrow{Z_n}((n-1)^2) = \overrightarrow{Z_n}(1)$　　(2) $n = 2^k-1$，$k \geqq 2$，則 $\overrightarrow{Z_n}(n+1) = \overrightarrow{Z_n}(1)$

【定理十一】

1. 若$\overrightarrow{Z_n}(q) = \overrightarrow{Z_n}(s)$ 則 $\overrightarrow{Z_n}(q-1) = \overrightarrow{Z_n}(s-1)$ 或 $\overrightarrow{Z_n}(q-1) = \overrightarrow{Z_n}^c(s-1)$，其中$1 \leqq s < q$
2. 已知n是奇數，若$\overrightarrow{Z_n}(q+1) = \overrightarrow{Z_n}(s+1)$ 則 $\overrightarrow{Z_n}(q) = \overrightarrow{Z_n}(s)$ 其中$1 \leqq s < q$

八、名詞與符號定義4

1. 若矩陣B_n滿足下列兩條件，則我們將B_n稱為 A_n的『廣義(模 2)逆矩陣』。

　(1) $A_n B_n \equiv B_n A_n \pmod 2$　　(2) $A_n B_n A_n \equiv A_n \pmod 2$

2. 若一個n階方陣所有的元素都是 1，我們以1_n表示，即$1_n = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}$

【定理十二】令$B_n=[b_{ij}]_{nxn}$，其中 $b_{i,j} = \begin{cases} 1, \text{ if } (i \le j) \wedge (i+j \text{ is even}) \\ 1, \text{ if } (i > j) \wedge (i+j \text{ is odd}) \\ 0, \text{ otherwise} \end{cases}$，則$B_n$確實為$A_n$的『廣義(模 2)逆矩陣』。

【定理十三】當n是奇數時，則 s(n)=1。此時$\overrightarrow{Z_n}(m)$會全部循環。

【定理十四】若$n = 2^h \times p$，則存在正整數$q^*(n)$使得$\overrightarrow{Z_n}(q^*(n)) = \overrightarrow{Z_n}(2^h)$，$h \in N$，p是正奇數。

伍、研究結果

關於答後身分，我們證明出以下的結果

甲、若答後身分是全老實人，則初始身分是全老實人或全騙子。

乙、答後身分的騙子總數必然為偶數。

丙、若答後身分等於初始身分，則初始身分為全老實人。

丁、若初始身分互補，則答後身分相同。

戊、若答後身分是全騙子，則初始身分為交錯身分。

關於繼承身分$\overrightarrow{Z_n}(m)$，得到以下結果：

甲、當$n = 2^k$，則 $\overrightarrow{Z_n}(m)$會在第 n 次收斂到全好人。

乙、當$n \neq 2^k$，則 $\overrightarrow{Z_n}(m)$不會收斂，而會循環。

i. 當n是奇數，則存在最小整數q(n)使得$\overrightarrow{Z_n}(q(n)) = \overrightarrow{Z_n}(1)$

1. $n = 2^k+1$，$k \geqq 2$，$\overrightarrow{Z_n}((n-1)^2) = \overrightarrow{Z_n}(1)$
2. $n = 2^k-1$，$k \geqq 2$，$\overrightarrow{Z_n}(n+1) = \overrightarrow{Z_n}(1)$

ii. 當n是偶數時，可將n表示成為$n = 2^h \times p$，$h \in N$ 且 p是正奇數

則存在整數$q^*(n)$使得$\overrightarrow{Z_n}(q^*(n)) = \overrightarrow{Z_n}(2^h)$

陸、未來展望

當$n \neq 2^k$ 時$\overrightarrow{Z_n}(m)$不收斂會進入循環，也就是，存在最小正整數對(q(n),s(n))，使得$\overrightarrow{Z}_n(q(n)) = \overrightarrow{Z}_n(s(n))$，其中$1 \le s(n) < q(n) \le 2^{n-1}+1$，循環節長$l(n)=q(n)-s(n)$。這說明了，答後身分向量會從第 s(n) 次答題開始，每隔$l(n)$次答題循環一次。雖然在【定理十】到【定理十四】有證明出我們所猜測出的部分結果，但我們仍有很大的努力空間，我們將持續朝著完善這個部分而努力。

柒、參考文獻與資料

[1]. 游森棚(2024.4)。騙子或老實人，科學研習期刊 NO.63-02
ntsec.gov.tw/article/detail.aspx?a=5420

[2]. 南一書局，高中數學課本第四冊A(P.169-P.217)

[3]. 中山大學雙週一題網路數學問題徵答113學年度第1學期第五題
www-math.nsysu.edu.tw/~problem/

[4]. 維基百科，分塊矩陣的乘法
zh.wikipedia.org/zh-tw/%E5%88%86%E5%A1%8A%E7%9F%A9%E9%99%A3

[5]. 周志成(2013.07.15)，線代啟示錄-有限體與模算術
ccjou.wordpress.com/2013/07/15/%E6%9C%89%E9%99%90%E9%AB%94%E8%88%87%E6%A8%A1%E7%AE%97%E8%A1%93/

[6]. 維基百科-廣逆矩陣
zh.wikipedia.org/wiki/%E5%B9%BF%E4%B9%89%E9%80%86%E9%98%B5