# 中華民國第 57 屆中小學科學展覽會

# 作品說明書

---

高級中等學校組　數學科

## 第三名

050411

## 巴斯卡三角形對質數同餘性質探討

學校名稱：國立嘉義高級中學

| 作者： | 指導老師： |
| --- | --- |
| 高二 劉奇聖<br>高二 詹凱傑 | 謝孟恭 |


關鍵詞：組合數、質數、矩陣

# 壹、 摘要

我們利用進位分解的方法，將組合數對一質數做同餘。並探討巴斯卡三角形其中一列對一質數同餘後，各個餘數數量的關係。

# 貳、 研究動機

我們曾經看過一個數奧問題:

> $n$是一個正整數，$n+1$個正整數$C_0^n, C_1^n, C_2^n, \cdots, C_{n-1}^n, C_n^n$中，除以 5 餘$j(1 \le j \le 4)$的個數用$r_j$表示，求證$r_1 + r_4 \ge r_2 + r_3$。
>
> 這題的答案用數學歸納法證明。(數學奧林匹亞大集新編)

但我們好奇是否能將$r_1, r_2, r_3, r_4$分別的數值求出，於是開始對類似的問題進行探討。

# 參、 研究目的

本文主要探討組合數對一質數$p$同餘的性質:

一、給定一組合數$C_m^n$對$p$同餘，若不整除，餘數為多少?若整除，含有幾次的質因數?

二、探討同餘後的巴斯卡三角形的特性。

三、$n$是一個正整數，第$n$列巴斯卡三角形$C_0^n, C_1^n, \cdots, C_{n-1}^n, C_n^n$中，除以$p$餘j $(0 \le \mathrm{j} < p)$的個數用$r_j$表示，$r_j$各別的數值為何?

四、探討在比 5 更大的質數中，是否亦存在與原題目類似的$r_j$數量大小關係。

# 肆、 研究設備或器材

紙、筆、電腦。

# 伍、 研究過程與方法

在這一章節，我們將推導及介紹我們會用到的數學定理，本章節的數學定理都是已經經過大家證明過的性質。此外在這一章節我們給出巴斯卡三角形對前幾個較小的質數同餘後的圖形，並稍加探討其中的性質。

一、Lucas 定理的推導

Lucas 定理有助於我們計算給定一組合數$C_m^n$對$p$同餘若不整除餘數為多少，下文中將會頻繁使用 Lucas 定理，以下給出證明。

[定理 5-1.1] 給定一個正整數$m$與質數$p$ ,其中$1 \le m \le p-1$ ,

則$\boxed{C_m^p = \frac{p!}{m!(p-m)!} = p \cdot \frac{(p-1)!}{m!(p-m)!} \equiv 0 \pmod p}$

[引理 5-1.2] 給定一個質數$p$，由二項式定理:

$$(1+x)^p = C_0^p + C_1^p x + C_2^p x^2 + \cdots + C_{p-1}^p x^{p-1} + C_p^p x^p$$

我們引用定理 5-1.1 的結果

則$\boxed{(1+x)^p \equiv 1 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^{p-1} + x^p \equiv 1 + x^p \pmod p}$

[引理 5-1.3] 給定非負整數$n = n_1 p + n_0$ 、$m = m_1 p + m_0$

，其中$\mathrm{m_1} \le n_1 \le \mathrm{p-1}$ , $\mathrm{m_0} \le \mathrm{n_0} \le \mathrm{p-1}$，則：$\boxed{C_m^n \equiv C_{m_1}^{n_1} C_{m_0}^{n_0} \pmod p}$

[證明]$(1+x)^n \equiv (1+x)^{n_1 p + n_0} \equiv [(1+x)^p]^{n_1} (1+x)^{n_0} \pmod p$

我們引用引理 5-1.2 的結果$\boxed{(1+x)^p \equiv 1 + x^p \pmod p}$

得$(1+x)^n \equiv [(1+x)^p]^{n_1} (1+x)^{n_0} \equiv (1+x^p)^{n_1} (1+x)^{n_0}$

$$\equiv (C_0^{n_1} + C_1^n x^p + \cdots + \boxed{C_{m_1}^{n_1} x^{m_1 p}} + \cdots + C_{n_1}^{n_1} x^{n_1 p})$$

$$\cdot (C_0^{n_0} + C_1^{n_0} x + \cdots + \boxed{C_{m_0}^{n_0} x^{m_0}} + \cdots + C_{n_0}^{n_0} x^{n_0})$$

又由二項式定理得$(1+x)^n \equiv (C_0^n + C_1^n x + \cdots + \boxed{C_m^n x^{m_1 p + m_0}} + \cdots + C_n^n x^n) \pmod p$

$\because \mathrm{m_0} \le \mathrm{n_0} \le \mathrm{p-1}$ $\therefore$只有$x^{m_1 p}$與$x^{m_0}$能夠乘出$x^{m_1 p + m_0}$ ，

又$x^{m_1 p + m_0}$項的係數應相同，因此由比較係數得$C_m^n \equiv C_{m_1}^{n_1} C_{m_0}^{n_0} \pmod p$，故得證。

[定理 5-1.4] 給定非負整數$n$、$m$，將其各自化為$p$進位，$p$為質數，即

$$\begin{cases} n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 \text{，記作} (n_k n_{k-1} \cdots n_0)_p \\ m = m_k p^k + m_{k-1} p^{k-1} + \cdots m_1 p + m_0 \text{，記作} (m_k m_{k-1} \cdots m_0)_p \end{cases}$$

其中$k$為非負整數，$n_k, \mathrm{n_{k-1}}, \cdots n_0, m_k, \cdots, m_0 \in \{0, 1, \cdots, p-1\}$

，且$n_k \neq 0$，$m_l \le n_l (0 \le l \le k)$

則$\boxed{C_m^n \equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0} (mod\ p)}$(此即 Lucas 定理)

[證明]$C_m^n \equiv C_{m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0}^{n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0}$

我們引用引理 5-1.3 的結論，即

$$C_m^n \equiv C_{(m_k p^{k-1} + \cdots + m_1) p + m_0}^{(n_k p^{k-1} + \cdots + n_1) p + n_0} \equiv C_{m_k p^{k-1} + \cdots + m_1}^{n_k p^{k-1} + \cdots + n_1} C_{m_0}^{n_0} \equiv C_{(m_k p^{k-2} + \cdots + m_2) p + m_1}^{(n_k p^{k-2} + \cdots + n_2) p + n_1} C_{m_0}^{n_0}$$

$$\equiv C_{(m_k p^{k-2} + \cdots + m_2)}^{(n_k p^{k-2} + \cdots + n_2)} C_{m_1}^{n_1} C_{m_0}^{n_0} \equiv \cdots$$

$\equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} C_{m_{k-2}}^{n_{k-2}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0}$，故得證。

[例子]$n = 2017 = (5611)_7$，$m = 1618 = (4501)_7$

，則$C_{1618}^{2017} \equiv C_4^5 C_5^6 C_0^1 C_1^1 \equiv 30 \equiv 2\ (mod\ 7)$

二、費馬小定理的推導

費馬小定理是一個很漂亮的同餘式子，下文中亦會多次使用。

[引理 5-2.1] $(x+1)^p \equiv x+1$

[證明]我們引用引理 5-1.2 的結果$\boxed{(1+x)^p \equiv 1 + x^p \ (\mathrm{mod}\ p)}$

$$(x+1)^p \equiv x^p + 1 \equiv (x-1)^p + 1 + 1 \equiv (x-2)^p + 1 + 1 + 1$$

$$\equiv (x-3)^p + 1 + 1 + 1 + 1 \equiv \cdots \equiv 1 + 1 + \cdots + 1 \ (x+1 \text{ 個 } 1)$$

$\equiv x+1$，得證。

[定理 5-2.2] $\boxed{\text{若}\alpha\text{不為質數}p\text{的倍數，則}\alpha^{p-1} \equiv 1(\mathrm{mod}\ p)}$，此即費馬小定理。

[證明] 我們引用引理 5-2.1 的結果$(x+1)^p \equiv x+1$，令$x = \alpha - 1$，

則$\alpha^p \equiv \alpha(\mathrm{mod}\ p)$，若$\alpha$與$p$互質，則可左右兩邊同除以$\alpha$，即得證。

三、Lucas 定理的變形

Lucas 定理可幫助我們有效的計算一組合數$C_m^n$對$p$同餘若不整除餘數為多少，但我們在證明的過程中，有假設$m_l \le n_l$ 這個條件，本小節將探討若存在$m_i > n_i$會發生甚麼事。

[定理 5-3.1] 在 Lucas 定理中，若存在$m_i > n_i$，則$C_m^n \equiv 0(\mathrm{mod}\ p)$ 。

[證明]先將問題簡化，設$n = n_1p + n_0$ , $m = m_1p + m_0$，類似引理 5-1.3 的推導過程，

但其中$m_1 < n_1$ , $n_0 \le m_0 \le\ p - 1$，則：

$(1 + x)^n \equiv (1 + x)^{n_1p+n_0} \equiv [(1 + x)^p]^{n_1}(1 + x)^{n_0} \equiv\ (1 + x^p)^{n_1}(1 + x)^{n_0}$

$\equiv \left(C_0^{n_1} + C_1^n x^p + \cdots + \boxed{C_{m_1}^{n_1} x^{m_1 p}} + \cdots + C_{n_1}^{n_1} x^{n_1 p}\right) \cdot (C_0^{n_0} + C_1^{n_0} x + \cdots + \boxed{C_{n_0}^{n_0} x^{n_0}})$

又由二項式定理得$(1 + x)^n \equiv (C_0^n + C_1^n x + \cdots + \boxed{C_m^n x^{m_1 p+m_0}} + \cdots + C_n^n x^n)\ (mod\ p)$

比較兩式，$\because\ m_1p + n_0 < m_1p + m_0$

為了乘出$x^{m_1p+m_0}$項，我們必須找$x^{m_1p}$之下一項$x^{(m_1+1)p}$才有機會。

上面取$x^{(m_1+1)p}$這項，下面假設取$x^{\alpha}$項，$0 \le \alpha \le \mathrm{n}_0$

則$(\mathrm{m}_1 + 1)\mathrm{p} + \alpha = \mathrm{m}_1\mathrm{p} + m_0$，整理後得到$p + \alpha = m_0$

$\therefore p < m_0$ 且$p >\ p - 1 \ge m_0$(矛盾)

因此找不到相乘能得到$x^{m_1p+m_0}$之兩項$\therefore\ C_m^n \equiv 0\ (mod\ p)$，得證。

這個結果可推廣至$\begin{cases} n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0 \\ m = m_k p^k + m_{k-1}p^{k-1} + \cdots m_1 p + m_0 \end{cases}$，即定理 5-3.1。

[例子]$n = 2017 = (5611)_7, m = 1632 = (4521)_7$

，則$\mathrm{n}_3 = 5, n_2 = 6, n_1 = 1, n_0 = 1$

，$\mathrm{m}_3 = 4, m_2 = 5, m_1 = 2, m_0 = 1$

∵當中$m_1 > n_1\ \therefore\ C_{1632}^{2017} \equiv 0\ (\mathrm{mod}\ 7)$

[定理 5-3.2] 給定非負整數$n$、$m$，將其各自化為$p$進位，$p$為質數，即

$\begin{cases} n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0 \text{，記作} (n_k n_{k-1} \cdots n_0)_p \\ m = m_k p^k + m_{k-1}p^{k-1} + \cdots m_1 p + m_0 \text{，記作 } (m_k m_{k-1} \cdots m_0)_p \end{cases}$

其中$k$為非負整數，$n_k, \mathrm{n}_{\mathrm{k}-1}, \cdots n_0, m_k, \cdots, m_0 \in \{0, 1, \cdots, p - 1\}$

令$\mathrm{h}_l = \begin{cases} 0\text{，當}(n_l n_{l-1} \cdots n_0)_{\mathrm{p}} \ge (m_l m_{l-1} \cdots m_0)_{\mathrm{p}} \\ 1\text{，當}(n_l n_{l-1} \cdots n_0)_{\mathrm{p}} < (m_l m_{l-1} \cdots m_0)_{\mathrm{p}} \end{cases}$，$0 \le l \le k$

則若把$C_m^n$表為$C_m^n = p^h \cdot t$時(即$C_m^n$含有 $h$ 次的質因數)，$h = \sum_{l=0}^{k} h_l$

，此即 Lucas 定理的變形，有助於我們計算給定一組合數$C_m^n$對$p$同餘若整除含有幾次的質因數。

[證明] 為了證明定理 5-3.2，我們同樣先將問題簡化，

設$n = n_1p + n_0$ , $m = m_1p + m_0$,$C_m^n = p^h \cdot t$

由$C_m^n = \frac{n!}{m!(n-m)!}$可知

$$h = (\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \left[\frac{n}{p^4}\right] + \cdots) - (\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + \left[\frac{m}{p^4}\right] + \cdots)$$
$$-(\left[\frac{n-m}{p}\right] + \left[\frac{n-m}{p^2}\right] + \left[\frac{n-m}{p^3}\right] + \left[\frac{n-m}{p^4}\right] + \cdots)$$

從這三個括號的第一項可得

$$\left[\frac{n}{p}\right] - \left[\frac{m}{p}\right] - \left[\frac{n-m}{p}\right]$$
$$= \left[\frac{n_1\mathrm{p} + n_0}{p}\right] - \left[\frac{m_1\mathrm{p} + m_0}{p}\right] - \left[\frac{n_1\mathrm{p} + n_0 - m_1\mathrm{p} - m_0}{p}\right]$$
$$= \left[n_1 + \frac{n_0}{p}\right] - \left[m_1 + \frac{m_0}{p}\right] - \left[n_1 - m_1 + \frac{n_0 - m_0}{p}\right]$$

(1)$n_0 \geq m_0$,則$\left[\frac{n}{p}\right] - \left[\frac{m}{p}\right] - \left[\frac{n-m}{p}\right] = n_1 - m_1 - (n_1 - m_1) = 0$

(2)$n_0 < m_0$則$\left[\frac{n}{p}\right] - \left[\frac{m}{p}\right] - \left[\frac{n-m}{p}\right] = n_1 - m_1 - (n_1 - m_1 - 1) = 1$

此結果可推廣至定理 5-3.2，當$n = (n_k n_{k-1} \cdots n_0)_p, m = (m_k m_{k-1} \cdots m_0)_p$時，當有一個$(n_l n_{l-1} \cdots n_0)_{\mathrm{p}} < (m_l m_{l-1} \cdots m_0)_{\mathrm{p}}, 0 \leq l \leq k$時，就表示$C_m^n$有一個質因數$p$，所以我們只要知道有幾個$(n_l n_{l-1} \cdots n_0)_p < (m_l m_{l-1} \cdots m_0)_p$就可知$h$的值，由於此一性質與下文較為無關，故證明略為簡略。

[例子] $n = 2017 = (5611)_7$,$m = 1632 = (4521)_7$

$\because (1)_7 \geq (1)_7 \therefore h_0 = 0$

$\because (11)_7 < (21)_7 \therefore h_1 = 1$

$\because (611)_7 \geq (521)_7 \therefore h_2 = 0$

$\because (5611)_7 \geq (4521)_7 \therefore h_3 = 0$

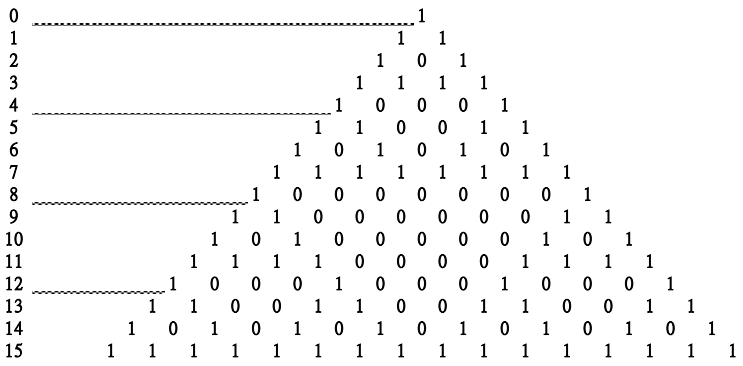
因此 $h = \sum_{l=0}^{3} h_l = 0 + 1 + 0 + 0 = 1$

$\therefore C_{1632}^{2017}$質因數分解後有 1 個質因數 7，即$C_{1632}^{2017} = 7^1 \cdot$

$t$，$t$為與 7 互質的一個正整數。

四、巴斯卡三角形對前幾個較小的質數同餘後的圖形

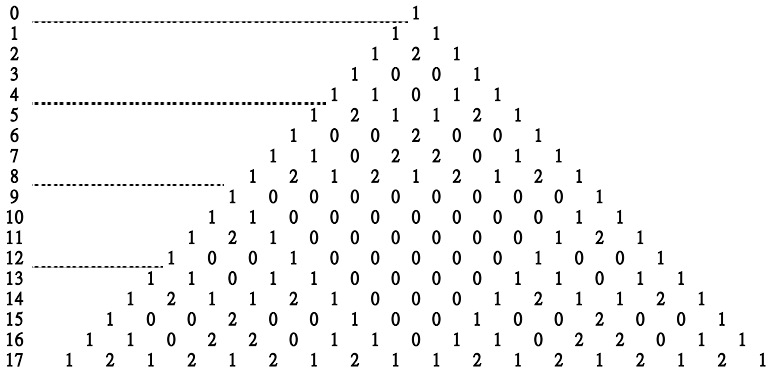
將巴斯卡三角形對$p$做同餘，得到一個新三角形(如圖一,圖二,圖三)，觀察這些新三角形可以發現有些列全不為 0，在定理 5-4.1 將討論符合這種情形的條件。



(圖一)巴斯卡三角形對 2 做同餘的0~16列

| 第n列 | n化為二進位 | 0的個數 | 1的個數 |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 2 |
| 2 | 10 | 1 | 2 |
| 3 | 11 | 0 | 4 |
| 4 | 100 | 3 | 2 |
| 5 | 101 | 2 | 4 |
| 6 | 110 | 3 | 4 |
| 7 | 111 | 0 | 8 |
| 8 | 1000 | 7 | 2 |
| 9 | 1001 | 6 | 4 |
| 10 | 1010 | 7 | 4 |
| 11 | 1011 | 4 | 8 |
| 12 | 1100 | 9 | 4 |
| 13 | 1101 | 6 | 8 |
| 14 | 1110 | 7 | 8 |
| 15 | 1111 | 0 | 16 |

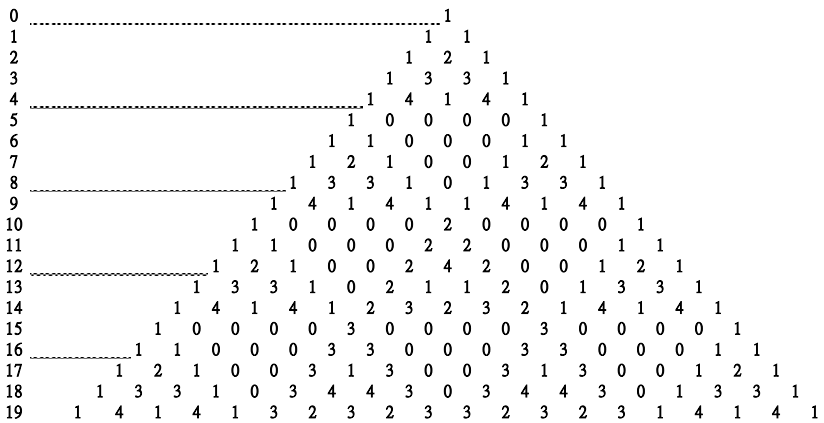
(表一)巴斯卡三角形對 2 做同餘後各列 0、1 的個數



(圖二)巴斯卡三角形對 3 做同餘的0~17列

| 第n列 | n化為三進位 | 0的個數 | 1的個數 | 2的個數 |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 2 | 0 |
| 2 | 2 | 0 | 2 | 1 |
| 3 | 10 | 2 | 2 | 0 |
| 4 | 11 | 0 | 4 | 1 |
| 5 | 12 | 0 | 4 | 2 |
| 6 | 20 | 4 | 2 | 1 |
| 7 | 21 | 2 | 4 | 2 |
| 8 | 22 | 0 | 5 | 4 |
| 9 | 100 | 8 | 2 | 0 |
| 10 | 101 | 7 | 4 | 0 |
| 11 | 102 | 6 | 4 | 2 |
| 12 | 110 | 9 | 4 | 0 |
| 13 | 111 | 6 | 8 | 0 |
| 14 | 112 | 3 | 8 | 4 |
| 15 | 120 | 10 | 4 | 2 |
| 16 | 121 | 5 | 8 | 4 |
| 17 | 122 | 0 | 10 | 8 |

(表二)巴斯卡三角形對 3 做同餘後各列 0、1、2 的個數



(圖三)巴斯卡三角形對 5 做同餘的0~19列

| 第n列 | n化為五進位 | 0的個數 | 1的個數 | 2的個數 | 3的個數 | 4的個數 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 2 | 0 | 0 | 0 |
| 2 | 2 | 0 | 2 | 1 | 0 | 0 |
| 3 | 3 | 0 | 2 | 0 | 2 | 0 |
| 4 | 4 | 0 | 3 | 0 | 0 | 2 |
| 5 | 10 | 4 | 2 | 0 | 0 | 0 |
| 6 | 11 | 3 | 4 | 0 | 0 | 0 |
| 7 | 12 | 2 | 4 | 2 | 0 | 0 |
| 8 | 13 | 1 | 4 | 0 | 4 | 0 |
| 9 | 14 | 0 | 6 | 0 | 0 | 4 |
| 10 | 20 | 8 | 2 | 1 | 0 | 0 |
| 11 | 21 | 6 | 4 | 2 | 0 | 0 |
| 12 | 22 | 4 | 4 | 4 | 0 | 1 |
| 13 | 23 | 2 | 6 | 2 | 4 | 0 |
| 14 | 24 | 0 | 6 | 3 | 2 | 4 |
| 15 | 30 | 12 | 2 | 0 | 2 | 0 |
| 16 | 31 | 9 | 4 | 0 | 4 | 0 |
| 17 | 32 | 6 | 6 | 2 | 4 | 0 |
| 18 | 33 | 3 | 4 | 0 | 8 | 4 |
| 19 | 34 | 0 | 6 | 4 | 6 | 4 |

(表三)巴斯卡三角形對 5 做同餘後各列 0、1、2、3、4 的個數

[定理 5-4.1] 巴斯卡三角形第$n$列中，$C_0^n, C_1^n, \cdots, C_n^n$皆不為質數$p$的倍數，即巴斯卡三角形對$p$做同餘後新三角形中全不為 0 的列，其充要條件為$n = ap^k - 1,\ k \in N$ ,$1 \le a \le p-1$ 。

[證明] 當$n = ap^k - 1$時，$n$化為$p$進位後， $n_k = a-1, n_{k-1} = \cdots = n_0 = p-1$，

則對於所有的$m = 0,1,2,\cdots,n$，$n_l \ge m_l$，$0 \le l \le k$，

$n_l = p-1 \ge m_l$皆成立，($l = 1,2,3,\cdots,k-1$，$n_k \ge m_k$)，

由 Lucas 定理，若對於所有的$m_l$皆滿足$m_l \le n_l (0 \le l \le k)$，

則$C_m^n \equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0} \ne 0 (\mathrm{mod}\ p)$，因此$C_m^n$皆不為 0。

# 陸、 研究結果

本章節將定義一些函數，利用排列組合、遞迴式、矩陣等方式將$r_j$的數值一一求出。

一、$r_j$的一般化定義

研究動機的題目中$r_j$定義為:$n$是一個正整數，$n+1$個正整數$C_0^n, C_1^n, C_2^n, \cdots, C_{n-1}^n, C_n^n$中除以 5 餘$j(1 \le j \le 4)$的個數用$r_j$表示。為了探討一般質數$p$，我們必須重新對$r_j$定義。

[定義 6-1.1] $n$是一個正整數，巴斯卡三角形第$n$列中的$n+1$個正整數

$C_0^n, C_1^n, C_2^n, \cdots, C_{n-1}^n, C_n^n$中除以一質數$p$餘$j(1 \le j \le p-1)$的個數用$r_j$表示。

二、定義新函數與$r_0$的公式推導

[定義 6-2.1] $n$是一個正整數，巴斯卡三角形第$n$列中同餘$p$餘$j(1 \le j \le p-1)$的個數用函數$F(n,p,j)$表示，即將$r_j$用函數$F(n,p,j)$表示。

[說明]此定義純粹是將$r_j$的資訊表示完整，將$n$與$p$都標示出來可以避免我們在討論不同的質數$p$時或同一個質數不同列時混淆。

[命題 6-2.2] $\boxed{r_0 = F(n,p,0) = n+1-2^{a_1}3^{a_2}4^{a_3}5^{a_4}\cdots p^{a_{p-1}}}$，其中的$a_1$、$a_2 \cdots$、$a_{p-1}$代表$n$化為$p$進位後，$n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$，

在集合$\{n_k, n_{k-1}, \cdots n_1, n_0\}$裡有$a_1$個 1、$a_2$個 2、…、$a_{p-1}$個$(p-1)$

[證明]運用 Lucas 定理 $C_m^n \equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0} (\mathrm{mod}\ p)$，可將$C_m^n$分為

$a_1$個$C_l^1$,$a_2$個$C_l^2 \cdots$,$a_{p-1}$個$C_l^{p-1}$相乘，當中$l$可為$0,1,\cdots,\mathrm{p}-1$。

而$F(n,p,0)$表$C_m^n$為$p$的倍數，所以我們以全部扣掉不是$p$的倍數來證明，要使$C_m^n$不

為$p$的倍數須滿足 Lucas 定理中$m_l \le n_l (0 \le l \le k)$的條件，所以$a_1$個$C_l^1$中的$l$有 0,1 兩種選擇，$a_2$個$C_l^2$中的$l$有 0,1,2 三種選擇，$a_3$個$C_l^3$中的$l$有 0,1,2,3 四種選擇，…，依此類推，可得不為$p$的倍數有$2^{a_1}3^{a_2}4^{a_3}5^{a_4}\cdots p^{a_{p-1}}$個，又巴斯卡三角形第$n$列共有$n+1$個數，因此$r_0 = F(n,p,0) = n+1-2^{a_1}3^{a_2}4^{a_3}5^{a_4}\cdots p^{a_{p-1}}$ 。

[例子] mod 5時，巴斯卡三角形第 12 列$C_0^{12}, C_1^{12}, C_2^{12}, \cdots, C_{11}^{12}, C_{12}^{12}$中，除以 5 餘 0 的個數為?

(解法)因為 12 化為 5 進位: $12 = (22)_5$，因此$a_1 = 0$，$a_2 = 2$，$a_3 = 0$，$a_4 = 0$，

因此$F(12,5,0) = 12+1-2^0 \cdot 3^2 \cdot 4^0 \cdot 5^0 = 4$，因此有 4 個。

[定義 6-2.3] 將$F(n,p,j)$中的$n$化為$p$進位後，即$n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$，

在集合$\{n_k, n_{k-1}, \cdots n_1, n_0\}$裡有$a_1$個 1、$a_2$個 2…$a_{p-1}$個$(p-1)$時，

則定義$F(n,p,j)$的另一種表法:$F(n,p,j) = f(a_1, a_2, \cdots, a_{p-1}, j)$ 。

[說明]由剛才的推導命題 6-2.2 的過程，我們得到不為$p$的倍數有$2^{a_1}3^{a_2}4^{a_3}5^{a_4}\cdots p^{a_{p-1}}$個，

因此除了$F(n,p,0)$之外，其他的$F(n,p,j)$中$j \neq 0$的公式便僅與$a_1, a_2, \cdots, a_{p-1}$的個數有關，而與$n$的數值無關了，因此我們如此定義。

再來我們即將討論$F(n,p,j)$中$j \neq 0$的情形。由於$j \neq 0$的情形較複雜，因此我們先從$p = 2$開始討論。

三、mod 2中$r_j (j \neq 0)$的公式推導

[命題 6-3.1] $r_1 = f(a_1, 1) = 2^{a_1}$

[證明]運用 Lucas 定理 $C_m^n \equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0} (\mathrm{mod}\ p)$，可將$C_m^n$分為$a_0$個$C_l^0$,$a_1$個$C_l^1$相乘，$l = 0,1$，因為$f(a_1,1)$表$C_m^n$不為 2 的倍數的個數，要使得$C_m^n$不為 2 的倍數，必須滿足 Lucas 定理中$m_l \le n_l (0 \le l \le k)$的條件，所以$a_0$個$C_l^0$中的$l$有 0 一種選擇，$a_1$個$C_l^1$中的$l$有 0,1 兩種選擇，由此可知$f(a_1,1) = 1^{a_0}2^{a_1} = 2^{a_1}$。

四、mod 3中$r_j (j \neq 0)$的公式推導

[命題 6-4.1]考慮巴斯卡三角形某一列對三同餘餘1,2的個數，則:

$$r_1 = f(a_1, a_2, 1) = \frac{2^{a_1}3^{a_2} + 2^{a_1}}{2} \text{ ，} r_2 = f(a_1, a_2, 2) = \frac{2^{a_1}3^{a_2} - 2^{a_1}}{2}$$

[證明] 首先，由推導命題 6-2.2 的過程，我們得到不為$p$的倍數有$2^{a_1}3^{a_2}4^{a_3}5^{a_4}\cdots p^{a_{p-1}}$個

因此$f(a_1,a_2,1)+f(a_1,a_2,2)=2^{a_1}3^{a_2}$

再來我們先算$f(a_1,a_2,2)$。由$C_1^2\equiv 2$，$C_0^0,C_0^1,C_1^1,C_1^2,C_2^2$皆同餘 1 (mod 3)，可知化為 Lucas 定理型式$C_m^n\equiv C_{m_k}^{n_k}C_{m_{k-1}}^{n_{k-1}}\cdots C_{m_1}^{n_1}C_{m_0}^{n_0}$時，當$C_{m_l}^{n_l}(0\le l\le k)$中有奇數個$C_1^2$時才能使得$C_m^n\equiv 2\ (\mathrm{mod}\ 3)$，($\because 2^t=\begin{cases}2,t\text{為奇數}\\1,t\text{為偶數}\end{cases}$)

所以若要使得$C_m^n\equiv 2\ (\mathrm{mod}\ 3)$，則$a_0$個$C_l^0$中的$l$有 0 一種選擇，$a_1$個$C_l^1$中的$l$有 0,1 兩種選擇，而$a_2$個$C_l^2$中的要有奇數個$l$為 1，其餘的$l$可為 0,2 兩種選擇。

$$f(a_1,a_2,2)=C_1^{a_2}\cdot 2^{a_1+a_2-1}+C_3^{a_2}\cdot 2^{a_1+a_2-3}+\cdots=2^{a_1+a_2-1}\left[C_1^{a_2}+(\frac{1}{2})^2C_3^{a_2}+\cdots\right]$$

為了求出$f(a_1,a_2,2)$需要運用下列兩式

$$(1+\tfrac{1}{2})^{a_2}=C_0^{a_2}+C_1^{a_2}\cdot\tfrac{1}{2}+C_2^{a_2}\cdot\left(\tfrac{1}{2}\right)^2+C_3^{a_2}\cdot\left(\tfrac{1}{2}\right)^3+\cdots\cdots(1)$$

$$\left(1-\tfrac{1}{2}\right)^{a_2}=C_0^{a_2}-C_1^{a_2}\cdot\tfrac{1}{2}+C_2^{a_2}\cdot\left(\tfrac{1}{2}\right)^2-C_3^{a_2}\cdot\left(\tfrac{1}{2}\right)^3+\cdots\cdots(2)$$

$(1)-(2)$可得 $\left(\tfrac{3}{2}\right)^{a_2}-\left(\tfrac{1}{2}\right)^{a_2}=C_1^{a_2}+C_3^{a_2}\cdot\left(\tfrac{1}{2}\right)^2+\cdots$

因此$f(a_1,a_2,2)=2^{a_1+a_2-1}\left[C_1^{a_2}+\left(\frac{1}{2}\right)^2C_3^{a_2}+\cdots\right]$

$$=2^{a_1+a_2-1}\left[\left(\tfrac{3}{2}\right)^{a_2}-\left(\tfrac{1}{2}\right)^{a_2}\right]=\frac{2^{a_1}3^{a_2}-2^{a_1}}{2}$$

將$f(a_1,a_2,2)=\frac{2^{a_1}3^{a_2}-2^{a_1}}{2}$代回$f(a_1,a_2,1)+f(a_1,a_2,2)=2^{a_1}3^{a_2}$

可得$f(a_1,a_2,1)=\frac{2^{a_1}3^{a_2}+2^{a_1}}{2}$。

[命題 6-4.2]以遞迴及矩陣的方式，同樣可推導出$\boxed{\begin{bmatrix}r_1\\r_2\end{bmatrix}=\begin{bmatrix}f(a_1,a_2,1)\\f(a_1,a_2,2)\end{bmatrix}=\frac{2^{a_1}}{2}\begin{bmatrix}(3^{a_2}+1)\\(3^{a_2}-1)\end{bmatrix}}$

[說明]理論上，我們應該繼續推導mod 5的公式，但因使用排列組合的觀點已無法應付如此複雜的情形，因此我們必須利用別的方法來推導公式。

STEP1:利用遞迴的觀念，我們來推想若$a_1+1$會發生什麼情形?

$a_1+1$代表將原本已用Lucas定理將$C_m^n$分成$a_0$個$C_l^0$、$a_1$個$C_l^1$、$a_2$個$C_l^2$後，再加乘一個$C_l^1$，根據剛才的推導我們知道$a_0$個$C_l^0$其實對公式無影響，因為$l$只有 0 一種選擇。因此我們

來想下面這 2 個式子:

$f(a_1+1,a_2,1)$ =? $f(a_1,a_2,1)$+? $f(a_1,a_2,2)$

$f(a_1+1,a_2,2)$ =? $f(a_1,a_2,1)$+? $f(a_1,a_2,2)$

剛才說過$a_1+1$代表將原來的數多乘一個一個$C_l^1$，即乘以$C_0^1$或$C_1^1$，因此原本有$f(a_1,a_2,1)$個1，無論是乘以$C_0^1$還是$C_1^1$都還是1，但數量變為 2 倍。

有$f(a_1,a_2,2)$個2，無論是乘以$C_0^1$還是$C_1^1$都還是2，但數量變為 2 倍。

因此$f(a_1+1,a_2,1)=2\,f(a_1,a_2,1)+0\,f(a_1,a_2,2)$

$f(a_1+1,a_2,2)=0\,f(a_1,a_2,1)+2\,f(a_1,a_2,2)$

寫成矩陣即為$\begin{bmatrix}f(a_1+1,a_2,1)\\f(a_1+1,a_2,2)\end{bmatrix}=\begin{bmatrix}2&0\\0&2\end{bmatrix}\begin{bmatrix}f(a_1,a_2,1)\\f(a_1,a_2,2)\end{bmatrix}\cdots(1)$

STEP2: 同樣的概念，$a_2+1$代表將原來的數多乘一個一個$C_l^2$，即乘以$C_0^2$、$C_1^2$或$C_2^2$，乘以$C_0^2$或$C_2^2$就代表乘以2，數量變 2 倍；乘以$C_1^2$就代表乘以1，數量變 1 倍，因此原本有$f(a_1,a_2,1)$個1，乘以1就變1，乘以2就變2

有$f(a_1,a_2,2)$個2，乘以1就變2，乘以2就變1

因此數量發生了改變，即$f(a_1,a_2+1,1)=2\,f(a_1,a_2,1)+1\,f(a_1,a_2,1)$

$f(a_1,a_2+1,2)=1\,f(a_1,a_2,2)+2\,f(a_1,a_2,2)$

寫成矩陣即為$\begin{bmatrix}f(a_1,a_2+1,1)\\f(a_1,a_2+1,2)\end{bmatrix}=\begin{bmatrix}2&1\\1&2\end{bmatrix}\begin{bmatrix}f(a_1,a_2,1)\\f(a_1,a_2,2)\end{bmatrix}\cdots(2)$

STEP3: 利用(1)、(2)這兩個遞迴矩陣將$a_1$及$a_2$的個數降至0。

$$\begin{bmatrix}f(a_1,a_2,1)\\f(a_1,a_2,2)\end{bmatrix}=\begin{bmatrix}2&0\\0&2\end{bmatrix}^{a_1}\begin{bmatrix}2&1\\1&2\end{bmatrix}^{a_2}\begin{bmatrix}f(0,0,1)\\f(0,0,2)\end{bmatrix}=\begin{bmatrix}2&0\\0&2\end{bmatrix}^{a_1}\begin{bmatrix}2&1\\1&2\end{bmatrix}^{a_2}\begin{bmatrix}1\\0\end{bmatrix}$$

STEP4:設 I 為單位矩陣，$\begin{bmatrix}2&0\\0&2\end{bmatrix}=A_1,\begin{bmatrix}2&1\\1&2\end{bmatrix}=A_2$，再令$\begin{bmatrix}0&1\\1&0\end{bmatrix}=P$，

則$A_2=2I+P$，又$(P)^2=I$，

因此$\begin{bmatrix}f(a_1,a_2,1)\\f(a_1,a_2,2)\end{bmatrix}=(2I)^{a_1}(2I+P)^{a_2}\begin{bmatrix}1\\0\end{bmatrix}$

$(2I+P)^{a_2}=C_0^{a_2}\cdot(2I)^{a_2}+C_1^{a_2}\cdot(2I)^{a_2-1}P+C_2^{a_2}\cdot(2I)^{a_2-2}(P)^2+\cdots$

利用$(2+1)^{a_2}$及$(2-1)^{a_2}$二式的二項式展開，我們可以求得

$$(2I+P)^{a_2}=\frac{(2+1)^{a_2}+(2-1)^{a_2}}{2}\cdot I+\frac{(2+1)^{a_2}-(2-1)^{a_2}}{2}\cdot P$$

因此 $\begin{bmatrix} f(a_1,a_2,1) \\ f(a_1,a_2,2) \end{bmatrix} = (2I)^{a_1}(2I+P)^{a_2}\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$$= \begin{bmatrix} 2^{a_1} & 0 \\ 0 & 2^{a_1} \end{bmatrix} \begin{bmatrix} \frac{3^{a_2}+1^{a_2}}{2} & \frac{3^{a_2}-1^{a_2}}{2} \\ \frac{3^{a_2}-1^{a_2}}{2} & \frac{3^{a_2}+1^{a_2}}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{2^{a_1}3^{a_2}+2^{a_1}}{2} \\ \frac{2^{a_1}3^{a_2}-2^{a_1}}{2} \end{bmatrix} = \frac{2^{a_1}}{2}\begin{bmatrix} (3^{a_2}+1) \\ (3^{a_2}-1) \end{bmatrix}$$

五、mod 5中$r_j(j \neq 0)$的公式推導

[命題 6-5.1] 考慮巴斯卡三角形某一列對五同餘餘1,2,3,4的個數，則:

$$\begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix}$$

$$= \frac{2^{a_1}}{4}\begin{bmatrix} 3^{a_2}4^{a_3}5^{a_4} + (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} + 1^{a_2}0^{a_3}5^{a_4} + (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} - i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4} - 1^{a_2}0^{a_3}5^{a_4} + i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} + i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4} - 1^{a_2}0^{a_3}5^{a_4} - i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} - (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} + 1^{a_2}0^{a_3}5^{a_4} - (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \end{bmatrix}$$

，其中$i = \sqrt{-1}$

[推導] 根據前面的方法我們可以寫出遞迴式，用矩陣的方式表達，

$$\begin{bmatrix} f(a_1+1,a_2,a_3,a_4,1) \\ f(a_1+1,a_2,a_3,a_4,2) \\ f(a_1+1,a_2,a_3,a_4,3) \\ f(a_1+1,a_2,a_3,a_4,4) \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix}$$

$$\begin{bmatrix} f(a_1,a_2+1,a_3,a_4,1) \\ f(a_1,a_2+1,a_3,a_4,2) \\ f(a_1,a_2+1,a_3,a_4,3) \\ f(a_1,a_2+1,a_3,a_4,4) \end{bmatrix} = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix}$$

$$\begin{bmatrix} f(a_1,a_2,a_3+1,a_4,1) \\ f(a_1,a_2,a_3+1,a_4,2) \\ f(a_1,a_2,a_3+1,a_4,3) \\ f(a_1,a_2,a_3+1,a_4,4) \end{bmatrix} = \begin{bmatrix} 2 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix}$$

$$\begin{bmatrix} f(a_1,a_2,a_3,a_4+1,1) \\ f(a_1,a_2,a_3,a_4+1,2) \\ f(a_1,a_2,a_3,a_4+1,3) \\ f(a_1,a_2,a_3,a_4+1,4) \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 & 2 \\ 0 & 3 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 2 & 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix}$$

根據上面 4 個矩陣可將$a_1$、$a_2$、$a_3$、$a_4$的個數降至0。

$$\begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}^{a_1} \begin{bmatrix} 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 \end{bmatrix}^{a_2} \begin{bmatrix} 2 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{bmatrix}^{a_3} \begin{bmatrix} 3 & 0 & 0 & 2 \\ 0 & 3 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 2 & 0 & 0 & 3 \end{bmatrix}^{a_4} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

設$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} = A_1$，$\begin{bmatrix} 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 \end{bmatrix} = A_2$，$\begin{bmatrix} 2 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{bmatrix} = A_3$，$\begin{bmatrix} 3 & 0 & 0 & 2 \\ 0 & 3 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 2 & 0 & 0 & 3 \end{bmatrix} = A_4$

，再令$P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$，計算出$P^2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$, $P^3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$, $P^4 = I$

$\therefore A_1 = 2I$ , $A_2 = 2I + P$ , $A_3 = 2I + 2P^3$ , $A_4 = 3I + 2P^2$

因此$\begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix} = (2I)^{a_1}(2I+P)^{a_2}(2I+2P^3)^{a_3}(3I+2P^2)^{a_4} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

為了方便算出$P^n$我們要將$P$對角化，寫成$P = CDC^{-1}$的形式，我們先算$P$的特徵值

$$\begin{vmatrix} 0-\lambda & 0 & 1 & 0 \\ 1 & 0-\lambda & 0 & 0 \\ 0 & 0 & 0-\lambda & 1 \\ 0 & 1 & 0 & 0-\lambda \end{vmatrix} = \lambda^4 - 1 = 0$$

得到特徵值$\lambda_1 = 1, \lambda_2 = i, \lambda_3 = -1, \lambda_4 = -i$

$(\lambda_1 I - P)x = O$的解為$x = t\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$,所以$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$為$\lambda_1 = 1$對應的特徵向量

同理$\lambda_2 = i, \lambda_3 = -1, \lambda_4 = -i$對應的特徵向量分別為$\begin{bmatrix} -1 \\ i \\ -i \\ 1 \end{bmatrix}$、$\begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}$、$\begin{bmatrix} -1 \\ -i \\ i \\ 1 \end{bmatrix}$

取$C = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \\ 1 & 1 & 1 & 1 \end{bmatrix}$,則$D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{bmatrix}$, $C^{-1} = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -i & i & 1 \\ 1 & -1 & -1 & 1 \\ -1 & i & -i & 1 \end{bmatrix}$

可得 $P$= $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \\ 1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{bmatrix}\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -i & i & 1 \\ 1 & -1 & -1 & 1 \\ -1 & i & -i & 1 \end{bmatrix}$=CD$C^{-1}$

將$P$對角化後，我們就要來算$\begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix}$,

$\because P = CDC^{-1}$　　$\therefore A_1 = 2I = C(2I)C^{-1}$，$A_2 = 2I + P = C(2I + D)C^{-1}$，

$A_3 = 2I + 2P^3 = C(2I + 2D^3)C^{-1}$，　$A_4 = 3I + 2P^2 = C(3I + 2D^2)C^{-1}$，

因此$\begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix} = (A_1)^{a_1}(A_2)^{a_2}(A_3)^{a_3}(A_4)^{a_4}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$= \mathrm{C}(2I)^{a_1}(2I + D)^{a_2}(2I + 2D^3)^{a_3}(3I + 2D^2)^{a_4}C^{-1}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$= \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \\ 1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}^{a_1}\begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 2+i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2-i \end{bmatrix}^{a_2}\begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 2-2i & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2+2i \end{bmatrix}^{a_3}\begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}^{a_4}\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -i & i & 1 \\ 1 & -1 & -1 & 1 \\ -1 & i & -i & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$= \frac{2^{a_1}}{4}\begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \\ 1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 3^{a_2}4^{a_3}5^{a_4} & 0 & 0 & 0 \\ 0 & (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} & 0 & 0 \\ 0 & 0 & 1^{a_2}0^{a_3}5^{a_4} & 0 \\ 0 & 0 & 0 & (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \end{bmatrix}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$

$= \frac{2^{a_1}}{4}\begin{bmatrix} 3^{a_2}4^{a_3}5^{a_4} + (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} + 1^{a_2}0^{a_3}5^{a_4} + (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} - i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4} - 1^{a_2}0^{a_3}5^{a_4} + i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} + i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4} - 1^{a_2}0^{a_3}5^{a_4} - i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} - (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} + 1^{a_2}0^{a_3}5^{a_4} - (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \end{bmatrix}$

[定義 6-5.2] 定義$0^0 = 1$，$0^n = 0(n\epsilon N)$

[說明]剛才計算中出現了 0 的$a_3$次方，$a_3 = 0$代表是$A_3$矩陣消失，可視為${A_3}^0 = I$，$0^0 = 1$

六、mod 7中$r_j(j \neq 0)$的公式推導

從對 5 做同餘中我們可以看出對 7 做同餘需要用到$6 \times 6$的方陣，這讓我們不方便表示，

所以我們先定義一些符號，使我們表示起來更方便。

[定義 6-6.1]定義$V_{n,p} = \begin{bmatrix} r_0 \\ r_1 \\ \vdots \\ r_{p-1} \end{bmatrix} = \begin{bmatrix} f(a_1,a_2,\cdots,a_{p-1},1) \\ f(a_1,a_2,\cdots,a_{p-1},2) \\ \vdots \\ f(a_1,a_2,\cdots,a_{p-1},p-1) \end{bmatrix}$

[定義 6-6.2]對於$u,v \in \{1,2,3\cdots p-1\}$必存在唯一 j 使得$u \equiv v$ j (mod p)，即j $\equiv \frac{u}{v}$(mod p)。

為了計算與呈現的方便，下面我們將j記作$\frac{u}{v}$。

定義$A_{k,p} = \begin{bmatrix} f(k,p,\frac{1}{1}) & f(k,p,\frac{1}{2}) & \cdots & f(k,p,\frac{1}{p-1}) \\ f(k,p,\frac{2}{1}) & f(k,p,\frac{2}{2}) & \cdots & f(k,p,\frac{2}{p-1}) \\ \cdots & \cdots & \cdots & \cdots \\ f(k,p,\frac{p-1}{1}) & f(k,p,\frac{p-1}{2}) & \cdots & f(k,p,\frac{p-1}{p-1}) \end{bmatrix}$

[定義 6-6.3]定義$P_{k,p}$表一個$(\mathrm{p}-1)\times(\mathrm{p}-1)$的方陣，

$$\text{其第}i\text{列與第}j\text{行的元素有}\left[P_{k,p}\right]_{ij}=\begin{cases}0,\text{其他情形}\\1,\text{當}i\equiv kj\ (mod\ p)\end{cases}\text{的關係}$$

有了上面的定義後我們開始分析巴斯卡三角形對 7 同餘的情形，至於為何如此定義，

則在後面對任意質數$p$做同餘時作說明。

[命題 6-6.4] 考慮巴斯卡三角形某一列對七同餘餘1,2,3,4,5,6的個數，由於 mod 7的公式太過龐大，我們直接寫在計算中。

$$\begin{bmatrix}f(a_1+1,a_2,a_3,a_4,a_5,a_6,1)\\f(a_1+1,a_2,a_3,a_4,a_5,a_6,2)\\f(a_1+1,a_2,a_3,a_4,a_5,a_6,3)\\f(a_1+1,a_2,a_3,a_4,a_5,a_6,4)\\f(a_1+1,a_2,a_3,a_4,a_5,a_6,5)\\f(a_1+1,a_2,a_3,a_4,a_5,a_6,6)\end{bmatrix}=\begin{bmatrix}2&0&0&0&0&0\\0&2&0&0&0&0\\0&0&2&0&0&0\\0&0&0&2&0&0\\0&0&0&0&2&0\\0&0&0&0&0&2\end{bmatrix}\begin{bmatrix}f(a_1,a_2,a_3,a_4,a_5,a_6,1)\\f(a_1,a_2,a_3,a_4,a_5,a_6,2)\\f(a_1,a_2,a_3,a_4,a_5,a_6,3)\\f(a_1,a_2,a_3,a_4,a_5,a_6,4)\\f(a_1,a_2,a_3,a_4,a_5,a_6,5)\\f(a_1,a_2,a_3,a_4,a_5,a_6,6)\end{bmatrix}$$

此即$A_{1,7}=2I$

同理$A_{2,7}=\begin{bmatrix}2&0&0&1&0&0\\1&2&0&0&0&0\\0&0&2&0&1&0\\0&1&0&2&0&0\\0&0&0&0&2&1\\0&0&1&0&0&2\end{bmatrix}$, $A_{3,7}=\begin{bmatrix}2&0&0&0&2&0\\0&2&2&0&0&0\\2&0&2&0&0&0\\0&0&0&2&0&2\\0&0&0&2&2&0\\0&2&0&0&0&2\end{bmatrix}$,

$A_{4,7}$ , $A_{5,7}$ , $A_{6,7}$分別為

$$\begin{bmatrix}2&2&0&0&0&1\\0&2&0&2&1&0\\0&0&2&1&0&2\\2&0&1&2&0&0\\0&1&2&0&2&0\\1&0&0&0&2&2\end{bmatrix},\begin{bmatrix}2&0&2&0&2&0\\0&2&2&0&0&2\\2&2&2&0&0&0\\0&0&0&2&2&2\\2&0&0&2&2&0\\0&2&0&2&0&2\end{bmatrix},\begin{bmatrix}4&0&0&0&0&3\\0&4&0&0&3&0\\0&0&4&3&0&0\\0&0&3&4&0&0\\0&3&0&0&4&0\\3&0&0&0&0&4\end{bmatrix}$$

即$V_{n,7}=(A_{1,7})^{a_1}(A_{2,7})^{a_2}(A_{3,7})^{a_3}(A_{4,7})^{a_4}(A_{5,7})^{a_5}(A_{6,7})^{a_6}V_{0,7}$

根據$P_{k,p}$的定義，

$$P_{1,7}=I, P_{2,7}=\begin{bmatrix}0&0&0&1&0&0\\1&0&0&0&0&0\\0&0&0&0&1&0\\0&1&0&0&0&0\\0&0&0&0&0&1\\0&0&1&0&0&0\end{bmatrix}, P_{3,7}=\begin{bmatrix}0&0&0&0&1&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&0&0&1&0&0\\0&1&0&0&0&0\end{bmatrix}$$

$$P_{4,7}=\begin{bmatrix}0&1&0&0&0&0\\0&0&0&1&0&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\end{bmatrix}, P_{5,7}=\begin{bmatrix}0&0&1&0&0&0\\0&0&0&0&0&1\\0&1&0&0&0&0\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&0&0&1&0&0\end{bmatrix}, P_{6,7}=\begin{bmatrix}0&0&0&0&0&1\\0&0&0&0&1&0\\0&0&0&1&0&0\\0&0&1&0&0&0\\0&1&0&0&0&0\\1&0&0&0&0&0\end{bmatrix}$$

選定$P=P_{3,7}$，$(P_{3,7})^2=P_{2,7}$，$(P_{3,7})^6=P_{6,7}$，$(P_{3,7})^4=P_{4,7}$，$(P_{3,7})^5=P_{5,7}$，$(P_{3,7})^6=I$

我們發現可以用$P_{3,7}$將其他$P_{n,7}$表示出來，我們將$P_{3,7}$對角化:

$$\begin{vmatrix}0-\lambda&0&0&0&1&0\\0&0-\lambda&1&0&0&0\\1&0&0-\lambda&0&0&0\\0&0&0&0-\lambda&0&1\\0&0&0&1&0-\lambda&0\\0&1&0&0&0&0-\lambda\end{vmatrix}=\lambda^6-1=0$$

得到特徵值 $\lambda_1=1,\ \lambda_2=\omega,\ \lambda_3=\omega^2,\ \lambda_4=\omega^3,\ \lambda_5=\omega^4,\ \lambda_6=\omega^5\ \ (\omega=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3})$

$(\lambda_1 I-P_{3,7})x=O$的解為$x=t[1\quad 1\quad 1\quad 1\quad 1\quad 1]^T$,即為 $\lambda_1=1$所對應的特徵向量，

同理 $\lambda_2=\omega$所對應的特徵值為$[\omega^6\quad \omega^4\quad \omega^5\quad \omega^2\quad \omega^1\quad \omega^3]^T$，

值得注意的是在ω的運算裡，$\omega_1=\omega^1$、$\omega_2=\omega^2$、$\omega_3=\omega^3\cdots\cdots\omega_k=\omega^k$的運算性質均同

因此$C=\begin{bmatrix}1^6&\omega^6&(\omega^2)^6&(\omega^3)^6&(\omega^4)^6&(\omega^5)^6\\1^4&\omega^4&(\omega^2)^4&(\omega^3)^4&(\omega^4)^4&(\omega^5)^4\\1^5&\omega^5&(\omega^2)^5&(\omega^3)^5&(\omega^4)^5&(\omega^5)^5\\1^2&\omega^2&(\omega^2)^2&(\omega^3)^2&(\omega^4)^2&(\omega^5)^2\\1^1&\omega^1&(\omega^2)^1&(\omega^3)^1&(\omega^4)^1&(\omega^5)^1\\1^3&\omega^3&(\omega^2)^3&(\omega^3)^3&(\omega^4)^3&(\omega^5)^3\end{bmatrix}$

則$D=\begin{bmatrix}1&0&0&0&0&0\\0&\omega&0&0&0&0\\0&0&\omega^2&0&0&0\\0&0&0&\omega^3&0&0\\0&0&0&0&\omega^4&0\\0&0&0&0&0&\omega^5\end{bmatrix}, C^{-1}=\frac{1}{6}\begin{bmatrix}1\\1\\1\\1\cdots\\1\\1\end{bmatrix}$($C^{-1}$不用詳細寫出，因為$C^{-1}V_{0,7}=\frac{1}{6}\begin{bmatrix}1\\1\\1\\1\\1\\1\end{bmatrix}$)

因此$V_{n,7} = (A_{1,7})^{a_1}(A_{2,7})^{a_2}(A_{3,7})^{a_3}(A_{4,7})^{a_4}(A_{5,7})^{a_5}(A_{6,7})^{a_6}V_{0,7}$

$= \left[(2I)^{a_1}(2I + {P_{3,7}}^2)^{a_2}(2I + 2P_{3,7})^{a_3}(2I + 2{P_{3,7}}^4 + {P_{3,7}}^3)^{a_4}\left(2I + 2P_{3,7} + {P_{3,7}}^5\right)^{a_5}\left(4I + 3{P_{3,7}}^3\right)^{a_6}\right]$

$= \left[C(2I)^{a_1}(2I + D^2)^{a_2}(2I + 2D)^{a_3}(2I + 2D^4 + D^3)^{a_4}(2I + 2D + D^5)^{a_5}(4I + 3D^3)^{a_6}\frac{1}{6}C^{-1}\right]$

$$= \frac{2^{a_1}}{6}\begin{bmatrix} 1^6 & \omega^6 & (\omega^2)^6 & (\omega^3)^6 & (\omega^4)^6 & (\omega^5)^6 \\ 1^4 & \omega^4 & (\omega^2)^4 & (\omega^3)^4 & (\omega^4)^4 & (\omega^5)^4 \\ 1^5 & \omega^5 & (\omega^2)^5 & (\omega^3)^5 & (\omega^4)^5 & (\omega^5)^5 \\ 1^2 & \omega^2 & (\omega^2)^2 & (\omega^3)^2 & (\omega^4)^2 & (\omega^5)^2 \\ 1^1 & \omega^1 & (\omega^2)^1 & (\omega^3)^1 & (\omega^4)^1 & (\omega^5)^1 \\ 1^3 & \omega^3 & (\omega^2)^3 & (\omega^3)^3 & (\omega^4)^3 & (\omega^5)^3 \end{bmatrix}\begin{bmatrix} 3^{a_2}\cdot 4^{a_3}\cdot 5^{a_4}\cdot 6^{a_5}\cdot 7^{a_6} \\ (2+\omega^2)^{a_2}(2+2\omega)^{a_3}(1-2\omega)^{a_4}(2+2\omega-2\omega^2)^{a_5}1^{a_6} \\ (2-\omega^2)^{a_2}(2+2\omega^2)^{a_3}(3+2\omega^2)^{a_4}(2-2\omega+2\omega^2)^{a_5}7^{a_6} \\ 3^{a_2}0^{a_3}3^{a_4}(-2)^{a_5}1^{a_6} \\ (2+\omega^2)^{a_2}(2-2\omega)^{a_3}(3-2\omega)^{a_4}(2-2\omega+2\omega^2)^{a_5}7^{a_6} \\ (2-\omega)^{a_2}(2-2\omega^2)^{a_3}(1+2\omega^2)^{a_4}(1+2\omega-2\omega^2)^{a_5}1^{a_6} \end{bmatrix}$$

此即mod 7的公式其中$\omega = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$，由於乘開過於龐大，用兩個矩陣相乘表示。

七、mod $p$中$r_j(j \neq 0)$的公式推導步驟歸納

STEP1: 寫出遞迴矩陣$A_k$。

STEP2: 選取一個$P$矩陣將遞迴矩陣$A_k$分解。

STEP3: 將$P$矩陣對角化。

STEP4: 將原式改寫後乘開。

(一)$P$矩陣

先前在定義 6-6.3 時我們定義$P_{k,p}$表一個$(\mathrm{p}-1)\times(\mathrm{p}-1)$的方陣，

其第$i$列與第$j$行的元素有$\left[P_{k,p}\right]_{ij} = \begin{cases} 0, \text{其他情形} \\ 1, \text{當} i \equiv kj\ (mod\ p) \end{cases}$ 的關係

事實上，我們所定義的$P_{k,p}$是一個「置換矩陣」(Permutation Matrix)，擁有以下性質:

(1) $P_{x,p}P_{y,p} = P_{z,p}$，其充要條件為$xy = z(\mathrm{mod}\ p)$

(2) ${P_{x,p}}^n = P_{y,p}$，其充要條件為$x^n = y(mod\ p)$

(3) ${P_{x,p}}^{-1} = P_{y,p}$，其充要條件為$\frac{1}{x} = y(mod\ p)$

(4) ${P_{x,p}}^{-1} = {P_{x,p}}^T$

(二) 分解遞迴矩陣$A_k$

(1)若選了某個$P = P_{\alpha,p}(1 \leq \alpha \leq p-1)$，可以將所有$P_{j,p}(1 \leq j \leq p-1)$表示為 $P$的次方，就能將遞迴矩陣$\mathrm{A_{k,p}}$完全分解成 P 與 I，我們稱這個$P_{\alpha,p}$為「可用」，檢驗$P_{\alpha,p}$是否為可用可以藉由上述$P$矩陣性質的第 2 點來實現。

若選了某個$\alpha$，可以將所有的$j(1 \le j \le p-1)$ 表示為$\alpha$的次方，我們便稱這個$\alpha$為「可用」。

若$\alpha$可用，則$P_{\alpha,p}$亦為可用。

(2)∵ 對於$u, v \in \{1,2,3 \cdots p-1\}$必存在唯一$j$ 使得$u \equiv v\, j \pmod p$，即 j $\equiv \frac{u}{v} \pmod p$

我們在寫遞迴式時$f(a_1, a_2, \cdots, a_k+1, \cdots, j)$

$= f(0, \cdots, 1, \cdots, j) \times f(a_1, a_2, \cdots, a_k, \cdots, 1) + f\left(0, \cdots, 1, \cdots, \frac{j}{2}\right) \times f(a_1, a_2, \cdots, a_k, \cdots, 2) + \cdots$

$$+ f\left(0, \cdots, 1, \cdots, \frac{j}{p-1}\right) \times f(a_1, a_2, \cdots, a_k, \cdots, p-1)$$

因此$A_{k,p} = \begin{bmatrix} f(k,p,\frac{1}{1}) & f(k,p,\frac{1}{2}) & \cdots & f(k,p,\frac{1}{p-1}) \\ f(k,p,\frac{2}{1}) & f(k,p,\frac{2}{2}) & \cdots & f(k,p,\frac{2}{p-1}) \\ \cdots & \cdots & \cdots & \cdots \\ f(k,p,\frac{p-1}{1}) & f(k,p,\frac{p-1}{2}) & \cdots & f(k,p,\frac{p-1}{p-1}) \end{bmatrix} = \sum_{j=1}^{p-1} f(k,p,j)\, P_{j,p}$

因此我們將$A_k$的分解做了公式化的呈現。

# 柒、 討論

在這一章節，我們將探討研究動機中的數奧問題，並加以推廣。

***n 是一個正整數，n+1 個正整數$C_0^n, C_1^n, C_2^n, \cdots, C_{n-1}^n, C_n^n$中除以 5 餘 j$(1 \le j \le 4)$的個數用$r_j$表示，求證$r_1 + r_4 \ge r_2 + r_3$***

一、質數 3、5、7 的數奧問題探討

(一)mod 3 中，$r_1 > r_2$

回憶一下我們算出來的 mod 3 公式$\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \frac{2^{a_1}}{2} \begin{bmatrix} (3^{a_2}+1) \\ (3^{a_2}-1) \end{bmatrix}$

∴ $r_1 - r_2 = 2^{a_1} > 0$，因此$r_1 > r_2$

(二)mod 5 中，$r_1 + r_4 \ge r_2 + r_3$

$$\begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \frac{2^{a_1}}{4} \begin{bmatrix} 3^{a_2}4^{a_3}5^{a_4} + (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} + 1^{a_2}0^{a_3}5^{a_4} + (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} - i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4} - 1^{a_2}0^{a_3}5^{a_4} + i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} + i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4} - 1^{a_2}0^{a_3}5^{a_4} - i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4} - (2+i)^{a_2}(2-2i)^{a_3}1^{a_4} + 1^{a_2}0^{a_3}5^{a_4} - (2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \end{bmatrix}$$

得$(r_1 + r_4) - (r_2 + r_3) = 2^{a_1} \cdot 1^{a_2} \cdot 0^{a_3} \cdot 5^{a_4} \ge 0$，其中等號成立的條件為$a_3 \ne 0$，且根據先前計算時的定義$0^0 = 1$可知當$a_3 = 0$時，$r_1 + r_4 > r_2 + r_3$

(三) mod 7 中，$(r_1+r_2+r_4)-(r_3+r_5+r_6)=2^{a_1}\cdot 3^{a_2}\cdot 0^{a_3}\cdot 3^{a_4}\cdot(-2)^{a_5}\cdot 1^{a_6}$

現在我們要來討論 mod 7，但現在出現了一個問題，我們雖然已算出 mod 7 的公式，但在$r_1,r_2,r_3,r_4,r_5,r_6$這六個數中，我們不知道要選取哪三個數去減掉另外三數，因此我們必須先回到 mod 5 中進行觀察。

[觀察]$(r_1+r_4)-(r_2+r_3)=(1)\cdot r_1+(-1)\cdot r_2+(-1)\cdot r_3+(1)\cdot r_4$

又mod 5中特徵根$(-1)$對應的特徵向量$w=[1\quad -1\quad -1\quad 1]^T$

[驗證]把$w^T$分別乘在 mod 5 的各個遞迴矩陣前，得

$w^TA_{1,5}=2\cdot w^T$

$w^TA_{2,5}=1\cdot w^T$

$w^TA_{3,5}=0\cdot w^T$

$w^TA_{4,5}=5\cdot w^T$

接著把$w^T$乘在$V_{n,5}=(A_{1,5})^{a_1}(A_{2,5})^{a_2}(A_{3,5})^{a_3}(A_{4,5})^{a_4}V_{0,5}$的前面

利用以上 4 式得$w^TV_{n,5}=2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}w^TV_{0,5}$，又$w^TV_{0,5}=[1]$

左式$=w^TV_{n,5}=[r_1-r_2-r_3+r_4]=[(r_1+r_4)-(r_2+r_3)]$

右式$=2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}\cdot w^TV_{0,5}=[2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}]$

由左、右式相等得$(r_1+r_4)-(r_2+r_3)=2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}$，與先前的計算相同。

[計算]在 mod 7 中，有了$(-1)$對應的特徵向量，我們就可以進行計算。

mod 7中$(-1)$所對應的特徵向量$w=[1\quad 1\quad -1\quad 1\quad -1\quad -1]^T$

把$w^T$分別乘在 mod 7 的各個遞迴矩陣前，得

$w^TA_{1,7}=2\cdot w^T$

$w^TA_{2,7}=3\cdot w^T$

$w^TA_{3,7}=0\cdot w^T$

$w^TA_{4,7}=3\cdot w^T$

$w^TA_{5,7}=(-2)\cdot w^T$

$w^TA_{6,7}=1\cdot w^T$

接著把$w^T$乘在$V_{n,7}=(A_{1,7})^{a_1}(A_{2,7})^{a_2}(A_{3,7})^{a_3}(A_{4,7})^{a_4}(A_{5,7})^{a_5}(A_{6,7})^{a_6}V_{0,7}$的前面，經過與 mod 5 類似的計算得$(r_1+r_2+r_4)-(r_3+r_5+r_6)=2^{a_1}\cdot 3^{a_2}\cdot 0^{a_3}\cdot 3^{a_4}\cdot(-2)^{a_5}\cdot 1^{a_6}$

我們可發現這已不是純粹的數量大小關係了，究竟是$r_1+r_2+r_4$還是$r_3+r_5+r_6$比較大是由$a_5$這個變數所控制，而等號則是由$a_3$這個變數所控制。

二、一般質數 $p$ 中$(-1)$的特徵向量

在這一小節，我們將藉由觀察mod 7來推廣至mod$p$，首要目標是找出$(-1)$的特徵向量。根據先前的定義，若選了某個$\alpha$，可以將所有的$j(1 \le j \le p-1)$ 表示為$\alpha$的次方，我們便稱這個$\alpha$為「可用」。在mod 7裡，可用的$\alpha$有 3、5，我們先以$P_{3,7}$為例。

(一)觀察$P_{3,7}$寫出$(-1)$的特徵向量

$P_{3,7}=\begin{bmatrix}0&0&0&0&1&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&0&0&1&0&0\\0&1&0&0&0&0\end{bmatrix}$，將$P_{3,7}$對角化，即$P_{3,7}x=\lambda x=\lambda Ix$，所以$(\lambda-P_{3,7})x=O$

將$\lambda$以$\omega$代入($\omega=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}$，$\omega^6=1$)，得$(\omega-P_{3,7})x=O$，

令$x=[x_1\quad x_2\quad x_3\quad x_4\quad x_5\quad x_6]^T$，則

$$\begin{bmatrix}\omega&0&0&0&-1&0\\0&\omega&-1&0&0&0\\-1&0&\omega&0&0&0\\0&0&0&\omega&0&-1\\0&0&0&-1&\omega&0\\0&-1&0&0&0&\omega\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\0\\0\end{bmatrix}$$，得$\begin{cases}x_1\omega=x_5\\x_2\omega=x_3\\x_3\omega=x_1\\x_4\omega=x_6\\x_5\omega=x_4\\x_6\omega=x_2\end{cases}$

也就是說若令$x_1=\omega^1$，則$x_5=\omega x_1$，$x_4=\omega x_5$……依此類推，排成一列即為

$$x_1\longrightarrow x_5\longrightarrow x_4\longrightarrow x_6\longrightarrow x_2\longrightarrow x_3$$

$$\omega^1\longrightarrow\omega^2\longrightarrow\omega^3\longrightarrow\omega^4\longrightarrow\omega^5\longrightarrow\omega^6$$

因此$\omega$對應特徵向量$x=[x_1\quad x_2\quad x_3\quad x_4\quad x_5\quad x_6]^T=[\omega^1\quad\omega^5\quad\omega^6\quad\omega^3\quad\omega^2\quad\omega^4]^T$

又在$\omega$的運算裡，$\omega_1=\omega^1$、$\omega_2=\omega^2$、$\omega_3=\omega^3\cdots\cdots\omega_k=\omega^k$的運算性質均相同，因此將$\omega$用$\omega_3=\omega^3=-1$代入即得到$(-1)$所對應的特徵向量$w$，即

$w=[(-1)^1\quad(-1)^5\quad(-1)^6\quad(-1)^3\quad(-1)^2\quad(-1)^4]^T=[-1\quad-1\quad1\quad-1\quad1\quad1]^T$

，又因為向量可以乘以任意倍數，因此乘以(-1)後便得到$w=[1\quad1\quad-1\quad1\quad-1\quad-1]^T$

[註]為了與$\omega$對應的特徵向量$x=[x_1\quad x_2\quad\cdots\quad\cdots\quad x_{p-1}]^T$作區別，

我們令$(-1)$對應的特徵向量$w=[t_1\quad t_2\quad\cdots\quad\cdots\quad t_{p-1}]^T$

(二)簡化計算過程

回到剛才的式子$(\omega - P_{3,7})x = O$，將左右兩邊同時轉置，得$x^T(\omega - P_{3,7})^T = O$，即

$$[x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6]\begin{bmatrix} \omega & 0 & -1 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & -1 \\ 0 & -1 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & -1 & 0 \\ -1 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & -1 & 0 & \omega \end{bmatrix} = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$$

有沒有發現中間那個矩陣是$(\omega - P_{5,7})$，其實這是因為$P_{5,7} = {P_{3,7}}^T$

($P$矩陣的計算性質 4:$\because 3 \times 5 \equiv 1 (\mathrm{mod}\ 7)$)

配合$P_{5,7}$的定義$\boxed{[P_{5,7}]_{ij} = \begin{cases} 1, i \equiv 5j\ (\mathrm{mod}\ 7) \\ 0, \text{其他} \end{cases}}$，以及矩陣的乘法規則，可發現$x_i = \omega t_j$，

即$x_{5j} = \omega x_j$，若令$x_1 = \omega^1$，則$x_5 = \omega x_1$，$x_{5^2} = \omega x_5$，$x_{5^3} = \omega x_{5^2}$…依此類推，如下

$$x_1 \rightarrow x_{5^1} \rightarrow x_{5^2} \rightarrow x_{5^3} \rightarrow x_{5^4} \rightarrow x_{5^5}$$
$$x_1 \rightarrow x_5 \rightarrow x_4 \rightarrow x_6 \rightarrow x_2 \rightarrow x_3$$
$$\omega^1 \rightarrow \omega^2 \rightarrow \omega^3 \rightarrow \omega^4 \rightarrow \omega^5 \rightarrow \omega^6$$

如果只要算(-1)的特徵向量，則只須標示正負號即可，例如令$x_1 = 1(+)$，則下一個數為-1(-)，再把$x$、$\omega$拿掉只留數字，則可進一步簡化符號，實際計算只需列出下面 2 列。

$$1 \rightarrow 5^1 \rightarrow 5^2 \rightarrow 5^3 \rightarrow 5^4 \rightarrow 5^5$$
$$1 \rightarrow 5 \rightarrow 4 \rightarrow 6 \rightarrow 2 \rightarrow 3$$
$$+ \quad - \quad + \quad - \quad + \quad -$$

(三)以簡化過程計算 mod 11 中(-1)所對應的特徵向量

STEP1:找出一個可用的$\alpha$，這裡使用 2

STEP2:找出 2 的乘法反元素: 6 $(2 \times 6 \equiv 1)$

STEP3:計算 6 的次方，由 0 次到 9 次排成一排，正負相間標上記號

$$1 \rightarrow 6 \rightarrow 3 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 5 \rightarrow 8 \rightarrow 4 \rightarrow 2$$
$$+ \quad - \quad + \quad - \quad + \quad - \quad + \quad - \quad + \quad -$$

依$t_1 = 1$、$t_6 = -1$、$t_3 = 1$…的順序得$w = [1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \quad -1]^T$

[研究]mod 11 中，可用的$\alpha$有 2、6、7、8，把這些$\alpha$用上面的方法計算，發現得到的w皆相同，顯示出這種關係在每個質數裡只會有 1 組。

(四)關於選取可用的$\alpha$

根據定義，我們知道若$\alpha$可用，則$\alpha$的次方可以將所有 $j(1 \le j \le p-1)$表示出來，又根據費馬小定理我們知道$\alpha^{p-1} \equiv 1 (\mathrm{mod}\, p)$，因此若$\alpha$不可用，則表示它在$(p-1)$次方之前「提早」變成了 1，以至於它無法將其他所有 $j$表示出來，即$\alpha^q \equiv 1$，又即使$\alpha$不可用，仍符合費馬小定理，將此二式聯立，即$\begin{cases}\alpha^q \equiv 1 \cdots\cdots (1)\\ \alpha^{p-1} \equiv 1 \cdots (2)\end{cases}$，(1)交集(2)得$q|(p-1)$，即$q$是$(p-1)$的因數，經過多次計算我們發現不可用的$\alpha$裡有很大一部分會在$q = \frac{(p-1)}{2}$時變為 1，也就是說**我們可以藉由檢驗$\alpha^{\frac{p-1}{2}}$是否為 1 來作為初步篩選的依據**，再以 $(p-1)$的其他因數次方做更精確的確認。

(五)mod $p$ 中(-1)所對應的特徵向量

依照上述作法，我們寫出了更多向量來進行觀察:

| mod $p$ | (-1)所對應的特徵向量$\mathrm{w} = [t_1 \quad t_2 \quad \cdots \quad \cdots \quad t_{p-1}]^T$ |
|---|---|
| mod 3 | $[1 \quad -1]^T$ |
| mod 5 | $[1 \quad -1 \quad -1 \quad 1]^T$ |
| mod 7 | $[1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1]^T$ |
| mod 11 | $[1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \quad -1]^T$ |
| mod 13 | $[1 \quad -1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad -1 \quad 1 \quad 1 \quad -1 \quad 1]^T$ |
| mod 17 | $[1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \quad -1 \quad 1 \quad 1]^T$ |
| mod 19 | $[1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad -1 \quad -1 \quad 1 \quad 1 \quad -1]^T$ |

觀察這個表可以得到一些規律:$w$中的第$k$個數$t_k \equiv k^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$ ，其中 $1 \le k \le p-1$

[例]:我們舉mod 11當例子，因為$\frac{11-1}{2} = 5$，

而$1^5 \equiv 1$，$3^5 \equiv 1$，$4^5 \equiv 1$，$5^5 \equiv 1$，$9^5 \equiv 1$

，$2^5 \equiv -1$，$6^5 \equiv -1$，$7^5 \equiv -1$，$8^5 \equiv -1$，$10^5 \equiv -1$

，因此在(-1)對應的特徵向量w裡第 1、3、4、5、9 個數為 1，第 2、6、7、8、10 個數為(-1)。

[證明]: 觀察的結果，我們給出證明，根據先前的計算:

$$1 \longrightarrow \alpha^1 \longrightarrow \alpha^2 \longrightarrow \cdots \longrightarrow \cdots \longrightarrow \alpha^{p-2}$$

$$+ \quad - \quad + \qquad\qquad -$$

我們可以知道第$\alpha$的偶次方個數為 1，第$\alpha$的奇次方個數為(-1)。

寫成數學式即為w 中的第$k(=\alpha^q)$個數$t_k \equiv \begin{cases} 1，若q = 2s \\ -1，若q = 2s-1 \end{cases}$，$s\epsilon N$

Ⅰ.若$q = 2s$，則$t_k \equiv 1$

而$k^{\frac{p-1}{2}} = (\alpha^q)^{\frac{p-1}{2}} = (\alpha^{2s})^{\frac{p-1}{2}} = (\alpha^s)^{p-1} \equiv 1$(由費馬小定理得證)

因此$t_k \equiv k^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$

Ⅱ.若$q = 2s-1$，則$t_k \equiv -1$

而$k^{\frac{p-1}{2}} = (\alpha^q)^{\frac{p-1}{2}} = (\alpha^{2s-1})^{\frac{p-1}{2}} = (\frac{\alpha^{2s}}{\alpha})^{\frac{p-1}{2}} = \frac{(\alpha^s)^{p-1}}{(\alpha)^{\frac{p-1}{2}}} \equiv \frac{1}{(\alpha)^{\frac{p-1}{2}}}$

又$\alpha$為「可用」，因此$(\alpha)^{\frac{p-1}{2}}$是一個不同餘 1 的整數，令$(\alpha)^{\frac{p-1}{2}} = z$，則

$\begin{cases} z\text{不同餘 } 1 \cdots (\text{第 1 式}) \\ z^2 = \alpha^{p-1} \equiv 1 \cdots (\text{第 2 式}) \end{cases}$，由第 2 式得$(z-1)(z+1) \equiv 0$，

於是得$z \equiv (-1)$或$1 \cdots$(第 3 式)

，把第 1 式交集第 3 式得$z = (\alpha)^{\frac{p-1}{2}} \equiv (-1)$，因此$k^{\frac{p-1}{2}} \equiv \frac{1}{(\alpha)^{\frac{p-1}{2}}} \equiv (-1)$

故$t_k \equiv k^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$，綜合Ⅰ、Ⅱ得證。

[註]在我們發現了這些規律後，赫然發現這竟然與「勒讓德符號」(Legendre symbol)的原始定義完全相同，但由於時間問題，我們無法解釋這兩者間的關聯並做更深入的探討，我們只能將(-1)所對應的特徵向量 w 用勒讓德符號表示。

[原始定義]勒讓德符號$\left(\frac{k}{p}\right) = \pm 1 \equiv k^{\frac{p-1}{2}}$

而$(-1)$所對應的特徵向量可表示為:

$w = [t_1 \quad t_2 \quad \cdots \quad \cdots \quad t_{p-1}]^T = \left[\left(\frac{1}{p}\right) \quad \left(\frac{2}{p}\right) \quad \cdots \quad \cdots \quad \left(\frac{\mathrm{p}-1}{p}\right)\right]^T$，即$t_k = \left(\frac{k}{p}\right)$

三、一般質數 $p$ 的數奧問題探討

有了(-1)的特徵向量後，本小節將探討一般質數 $p$ 中的數奧問題。

(一)一般質數 $p$ 中的數奧問題

暫且不管勒讓德符號的運算性質，我們先借用它來表示我們的計算式子，

$w=\left[\left(\frac{1}{p}\right)\ \ \left(\frac{2}{p}\right)\ \ \cdots\ \ \cdots\ \ \left(\frac{p-1}{p}\right)\right]^{T}$，其中的$\left(\frac{k}{p}\right)$，$1\le k\le p-1$，為勒讓德符號。

先將$\mathrm{w}^{\mathrm{T}}$乘在$P_{j,p}$前，得$\boxed{\mathrm{w}^{\mathrm{T}}P_{j,p}=\left(\frac{j}{p}\right)\mathrm{w}^{\mathrm{T}}}$

又$A_{k,p}=\sum_{j=1}^{p-1}f(k,p,j)\,P_{j,p}$，把$\mathrm{w}^{\mathrm{T}}$乘在$A_{k,p}$前，得

$$\boxed{\mathrm{w}^{\mathrm{T}}A_{k,p}=\sum_{j=1}^{p-1}f(k,p,j)\mathrm{w}^{\mathrm{T}}P_{j,p}=\sum_{j=1}^{p-1}f(k,p,j)\left(\frac{j}{p}\right)\mathrm{w}^{\mathrm{T}}}$$

又$V_{n,p}=(A_{1,p})^{a_1}(A_{2,p})^{a_2}\cdots(A_{k,p})^{a_k}\cdots(A_{p-1,p})^{a_{p-1}}V_{0,p}$，把$\mathrm{w}^{\mathrm{T}}$乘在$V_{n,p}$前，

得$\mathrm{w}^{\mathrm{T}}V_{n,p}=\left[\sum_{j=1}^{p-1}f(1,p,j)\left(\frac{j}{p}\right)\right]^{a_1}\left[\sum_{j=1}^{p-1}f(2,p,j)\left(\frac{j}{p}\right)\right]^{a_2}\cdots\left[\sum_{j=1}^{p-1}f(p-1,p,j)\left(\frac{j}{p}\right)\right]^{a_{p-1}}\mathrm{w}^{\mathrm{T}}V_{0,p}$

又 $\mathrm{w}^{\mathrm{T}}V_{0,p}=[1]$，因此左式$\mathrm{w}^{\mathrm{T}}V_{n,p}=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)r_i$

$$=\left[\sum_{j=1}^{p-1}f(1,p,j)\left(\frac{j}{p}\right)\right]^{a_1}\left[\sum_{j=1}^{p-1}f(2,p,j)\left(\frac{j}{p}\right)\right]^{a_2}\cdots\cdots\left[\sum_{j=1}^{p-1}f(p-1,p,j)\left(\frac{j}{p}\right)\right]^{a_{p-1}}$$

$$=\prod_{l=1}^{p-1}\left[\sum_{j=1}^{p-1}f(l,p,j)\left(\frac{j}{p}\right)\right]^{a_l}=\prod_{l=1}^{p-1}\left[\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)f(l,p,j)\right]^{a_l}$$

對於所有的正整數$n$，令$r_i$為巴斯卡三角形第$n$列$C_0^n,C_1^n,C_2^n,\cdots,C_n^n$除以$p$餘$i$的個數，則

$$\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)r_i=\prod_{l=1}^{p-1}\left[\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)f(l,p,j)\right]^{a_l}$$

，其中$\left(\frac{i}{p}\right)$和$\left(\frac{j}{p}\right)$為勒讓德符號，而$a_l$為$n$化為$p$進位後$l$的個數$(1\le l\le p-1)$，

且$f(l,p,j)$為$C_0^l,C_1^l,C_2^l,\cdots,C_l^l$除以$p$餘$j$的個數$(1\le j\le p-1)$

(二) mod 11 中的數奧問題

雖然有了公式，但這只是表示方便，計算時仍要算出各個∑的值。

STEP1:列出公式$\sum_{i=1}^{10}\left(\frac{i}{11}\right)r_i=\prod_{l=1}^{10}\left[\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(l,11,j)\right]^{a_l}$

STEP2:寫出向量$w=[1\quad -1\quad 1\quad 1\quad 1\quad -1\quad -1\quad -1\quad 1\quad -1]^{\mathrm{T}}$

$=\left[\left(\frac{1}{11}\right)\ \left(\frac{2}{11}\right)\ \left(\frac{3}{11}\right)\ \left(\frac{4}{11}\right)\ \left(\frac{5}{11}\right)\ \left(\frac{6}{11}\right)\ \left(\frac{7}{11}\right)\ \left(\frac{8}{11}\right)\ \left(\frac{9}{11}\right)\ \left(\frac{10}{11}\right)\right]^{\mathrm{T}}$

STEP3:計算左式$=\sum_{i=1}^{10}\left(\frac{i}{11}\right)r_i=(r_1+r_3+r_4+r_5+r_9)-(r_2+r_6+r_7+r_8+r_{10})$

STEP4:計算右式中的各個∑的值

$\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(1,11,j)=2\cdot\left(\frac{1}{11}\right)=2$(因為巴斯卡三角形第 1 列:1 1，只有 2 個 1)

$\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(2,11,j)=2\cdot\left(\frac{1}{11}\right)+1\cdot\left(\frac{2}{11}\right)=1$(因為巴斯卡三角形第 2 列:1 2 1，有 2 個 1、1 個 2)

$\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(3,11,j)=2\cdot\left(\frac{1}{11}\right)+2\cdot\left(\frac{3}{11}\right)=4$(因為巴斯卡三角形第 3 列:1 3 3 1，有 2 個 1、2 個 3)

$\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(4,11,j)=2\cdot\left(\frac{1}{11}\right)+2\cdot\left(\frac{4}{11}\right)+1\cdot\left(\frac{6}{11}\right)=3$(因為第 4 列:1 4 6 4 1)

$\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(5,11,j)=2\cdot\left(\frac{1}{11}\right)+2\cdot\left(\frac{5}{11}\right)+2\cdot\left(\frac{10}{11}\right)=2$(因為第 5 列:1 5 10 10 5 1)

⋮

依此類推，所以右式$=\prod_{l=1}^{10}\left[\sum_{j=1}^{10}\left(\frac{j}{11}\right)f(l,11,j)\right]^{a_l}=2^{a_1}\cdot 1^{a_2}\cdot 4^{a_3}\cdot 3^{a_4}\cdot 2^{a_5}\cdots\cdots$

STEP5:左式 = 右式，得

$$(\boldsymbol{r_1+r_3+r_4+r_5+r_9})-(\boldsymbol{r_2+r_6+r_7+r_8+r_{10}})$$
$$=\boldsymbol{2^{a_1}\cdot 1^{a_2}\cdot 4^{a_3}\cdot 3^{a_4}\cdot 2^{a_5}\cdot 3^{a_6}\cdot(-4)^{a_7}\cdot 1^{a_8}\cdot 6^{a_9}\cdot 1^{a_{10}}}$$

(三)質數中的數奧問題整理

(1)mod 3 時，$r_1 - r_2 = 2^{a_1}$，因此$r_1 > r_2$

[註]若用公式計算會算出$r_1 - r_2 = 2^{a_1} \cdot 1^{a_2}$

(2)mod 5 時，$(r_1 + r_4) - (r_2 + r_3) = 2^{a_1} \cdot 1^{a_2} \cdot 0^{a_3} \cdot 5^{a_4}$，因此$r_1 + r_4 \geq r_2 + r_3$

(3)mod 7 時，$(r_1 + r_2 + r_4) - (r_3 + r_5 + r_6) = 2^{a_1} \cdot 3^{a_2} \cdot 0^{a_3} \cdot 3^{a_4} \cdot (-2)^{a_5} \cdot 1^{a_6}$

(4)mod 11 時，$(r_1 + r_3 + r_4 + r_5 + r_9) - (r_2 + r_6 + r_7 + r_8 + r_{10})$

$$= 2^{a_1} \cdot 1^{a_2} \cdot 4^{a_3} \cdot 3^{a_4} \cdot 2^{a_5} \cdot 3^{a_6} \cdot (-4)^{a_7} \cdot 1^{a_8} \cdot 6^{a_9} \cdot 1^{a_{10}}$$

(5)mod 13 時，

$$(r_1 + r_3 + r_4 + r_9 + r_{10} + r_{12}) - (r_2 + r_5 + r_6 + r_7 + r_8 + r_{11})$$

$$= 2^{a_1} \cdot 1^{a_2} \cdot 4^{a_3} \cdot 3^{a_4} \cdot 2^{a_5} \cdot (-3)^{a_6} \cdot 0^{a_7} \cdot (-1)^{a_8} \cdot 6^{a_9} \cdot 1^{a_{10}} \cdot 0^{a_{11}} \cdot 13^{a_{12}}$$

(6)mod 17 時，

$$(r_1 + r_2 + r_4 + r_8 + r_9 + r_{13} + r_{15} + r_{16}) - (r_3 + r_5 + r_6 + r_7 + r_{10} + r_{11} + r_{12} + r_{14})$$

$$= 2^{a_1} \cdot 3^{a_2} \cdot 0^{a_3} \cdot 3^{a_4} \cdot (-2)^{a_5} \cdot 1^{a_6} \cdot 4^{a_7} \cdot 1^{a_8} \cdot 6^{a_9} \cdot (-3)^{a_{10}} \cdot (-4)^{a_{11}} \cdot 3^{a_{12}} \cdot 2^{a_{13}} \cdot (-1)^{a_{14}} \cdot 0^{a_{15}} \cdot 17^{a_{16}}$$

(6)mod 19 時，

$$(r_1 + r_4 + r_5 + r_6 + r_7 + r_9 + r_{11} + r_{16} + r_{17}) - (r_2 + r_3 + r_8 + r_{10} + r_{12} + r_{13} + r_{14} + r_{15} + r_{18})$$

$$= 2^{a_1} \cdot 1^{a_2} \cdot 0^{a_3} \cdot 5^{a_4} \cdot 2^{a_5} \cdot 3^{a_6} \cdot 4^{a_7} \cdot (-1)^{a_8} \cdot 2^{a_9} \cdot 7^{a_{10}} \cdot 8^{a_{11}} \cdot 3^{a_{12}} \cdot (-2)^{a_{13}} \cdot (-3)^{a_{14}} \cdot (-4)^{a_{15}} \cdot 9^{a_{16}} \cdot 6^{a_{17}} \cdot 1^{a_{18}}$$

# 捌、 結論

一、本篇文章主要用到了以下數學工具

(一)Lucas 定理:

[內容]若 $p$為質數，將$n$、$m$化成$p$進位$\begin{cases} n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 \\ m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0 \end{cases}$

，且$n_i \geq m_i$，則組合數$C_m^n \equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0} = \prod_{i=0}^{k} C_{m_i}^{n_i} \pmod p$

(二)費馬小定理:

[內容]若 $\alpha$ 不為質數$p$的倍數，則$\alpha^{p-1} \equiv 1 \pmod p$

(三)勒讓德符號(Legendre symbol):

[原始定義] $\left(\frac{k}{p}\right) = \pm 1 \equiv k^{\frac{p-1}{2}}$

[註]由於時間問題，本篇文章只借用勒讓德符號來表示公式，並未探討其運算性質。

(四)遞迴式及矩陣的對角化技巧。

二、利用 Lucas 定理，我們探討了以下性質

(一)Lucas 定理的變形

若 $p$為質數，將$n$、$m$化成$p$進位$\begin{cases} n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0 \\ m = m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0 \end{cases}$

若存在$m_i > n_i$，則$C_m^n \equiv 0 (\mathrm{mod}\, p)$

令$\mathrm{h}_l = \begin{cases} 0\text{，當}(n_l n_{l-1} \cdots n_0)_\mathrm{p} \geq (m_l m_{l-1} \cdots m_0)_\mathrm{p} \\ 1\text{，當}(n_l n_{l-1} \cdots n_0)_\mathrm{p} < (m_l m_{l-1} \cdots m_0)_\mathrm{p} \end{cases}$，$0 \leq l \leq k$

則若把$C_m^n$表為$C_m^n = p^h \cdot t$時，$h = \sum_{l=0}^{k} h_l$

即將$C_m^n$質因數分解後可提出$h$個$p$，$h$的值由末位往前一一比較後而得。

(二)關於巴斯卡三角形

巴斯卡三角形第$n$列中，$C_0^n, C_1^n, \cdots, C_n^n$皆不為質數$p$的倍數，即將巴斯卡三角形

對$p$做同餘後新三角形中全不為 0 的列，充要條件為$n = ap^k - 1,\ k \in N, 1 \leq a \leq p-1$

三、定義函數後，我們導出了以下公式

(一)[定義]函數$F(n,p,j)$表巴斯卡三角形第$n$列$C_0^n, C_1^n, C_2^n, \cdots, C_n^n$中除以$p$餘$j$的個數。$p$:質數。

[定義]將$F(n,p,j)$中的$n$化為$p$進位後，即$n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$，

在集合$\{n_k, n_{k-1}, \cdots n_1, n_0\}$裡有$a_1$個 1、$a_2$個 2$\cdots a_{p-1}$個$(p-1)$時，

則定義$F(n,p,j)$的另一種表法:$F(n,p,j) = f(a_1, a_2, \cdots, a_{p-1}, j)$

(二)藉由 Lucas 定理配合排列組合，我們可直接導出

$F(n,p,0) = n + 1 - 2^{a_1}3^{a_2}4^{a_3}5^{a_4} \cdots p^{a_{p-1}}$

(三)藉由 Lucas 定理配合排列組合，我們導出 mod 2 與 mod 3 的公式

(1) $f(a_1, 1) = 2^{a_1}$　　(2) $f(a_1, a_2, 1) = \frac{2^{a_1}3^{a_2} + 2^{a_1}}{2}$，$f(a_1, a_2, 2) = \frac{2^{a_1}3^{a_2} - 2^{a_1}}{2}$

(四)藉由遞迴式及矩陣，我們同樣可導出 mod 3 的公式，還導出了 mod 5 與 mod 7 的公式。

(1)$\begin{bmatrix} f(a_1,a_2,1) \\ f(a_1,a_2,2) \end{bmatrix} = \frac{2^{a_1}}{2}\begin{bmatrix} (3^{a_2}+1) \\ (3^{a_2}-1) \end{bmatrix}$

(2)$\begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix} = \frac{2^{a_1}}{4}\begin{bmatrix} 3^{a_2}4^{a_3}5^{a_4}+(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}+1^{a_2}0^{a_3}5^{a_4}+(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4}-i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}-1^{a_2}0^{a_3}5^{a_4}+i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4}+i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}-1^{a_2}0^{a_3}5^{a_4}-i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \\ 3^{a_2}4^{a_3}5^{a_4}-(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}+1^{a_2}0^{a_3}5^{a_4}-(2-i)^{a_2}(2+2i)^{a_3}1^{a_4} \end{bmatrix}$

(3)$\begin{bmatrix} f(a_1,a_2,a_3,a_4,a_5,a_6,1) \\ f(a_1,a_2,a_3,a_4,a_5,a_6,2) \\ f(a_1,a_2,a_3,a_4,a_5,a_6,3) \\ f(a_1,a_2,a_3,a_4,a_5,a_6,4) \\ f(a_1,a_2,a_3,a_4,a_5,a_6,5) \\ f(a_1,a_2,a_3,a_4,a_5,a_6,6) \end{bmatrix}$

$= \frac{2^{a_1}}{6}\begin{bmatrix} 1^6 & \omega^6 & (\omega^2)^6 & (\omega^3)^6 & (\omega^4)^6 & (\omega^5)^6 \\ 1^4 & \omega^4 & (\omega^2)^4 & (\omega^3)^4 & (\omega^4)^4 & (\omega^5)^4 \\ 1^5 & \omega^5 & (\omega^2)^5 & (\omega^3)^5 & (\omega^4)^5 & (\omega^5)^5 \\ 1^2 & \omega^2 & (\omega^2)^2 & (\omega^3)^2 & (\omega^4)^2 & (\omega^5)^2 \\ 1^1 & \omega^1 & (\omega^2)^1 & (\omega^3)^1 & (\omega^4)^1 & (\omega^5)^1 \\ 1^3 & \omega^3 & (\omega^2)^3 & (\omega^3)^3 & (\omega^4)^3 & (\omega^5)^3 \end{bmatrix}\begin{bmatrix} 3^{a_2}\cdot 4^{a_3}\cdot 5^{a_4}\cdot 6^{a_5}\cdot 7^{a_6} \\ (2+\omega^2)^{a_2}(2+2\omega)^{a_3}(1-2\omega)^{a_4}(2+2\omega-2\omega^2)^{a_5}1^{a_6} \\ (2-\omega^2)^{a_2}(2+2\omega^2)^{a_3}(3+2\omega^2)^{a_4}(2-2\omega+2\omega^2)^{a_5}7^{a_6} \\ 3^{a_2}0^{a_3}3^{a_4}(-2)^{a_5}1^{a_6} \\ (2+\omega^2)^{a_2}(2-2\omega)^{a_3}(3-2\omega)^{a_4}(2-2\omega+2\omega^2)^{a_5}7^{a_6} \\ (2-\omega)^{a_2}(2-2\omega^2)^{a_3}(1+2\omega^2)^{a_4}(1+2\omega-2\omega^2)^{a_5}1^{a_6} \end{bmatrix}$

(五)我們歸納出計算一般質數$p$的流程

①寫出遞迴矩陣$A_k$ →②選取一個 $P$矩陣將遞迴矩陣$A_k$分解→③將 $P$矩陣對角化→

④將原式改寫後乘開

四、藉由(-1)所對應的特徵向量，我們對研究動機中的數奧問題做了推廣

(一)研究動機中的數奧問題

[問題] $n$是一個正整數，$n+1$個正整數$C_0^n, C_1^n, C_2^n, \cdots, C_{n-1}^n, C_n^n$中除以 5 餘 $j(1 \le j \le 4)$ 的個數用$r_j$表示，求證$r_1 + r_4 \ge r_2 + r_3$

(二)我們把特徵根(-1)所對應的特徵向量，分別乘在各個遞迴矩陣前，算出了質數 3、5、7 中$r_j$的關係式。

(1)mod 3 中，$r_1 - r_2 = 2^{a_1}$，因此$r_1 > r_2$

(2)mod 5 中，$(r_1 + r_4) - (r_2 + r_3) = 2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}$，因此$r_1 + r_4 \ge r_2 + r_3$

(3)mod 7 中，$(r_1 + r_2 + r_4) - (r_3 + r_5 + r_6) = 2^{a_1}\cdot 3^{a_2}\cdot 0^{a_3}\cdot 3^{a_4}\cdot (-2)^{a_5}\cdot 1^{a_6}$

[註]配合計算過程，我們定義$0^0 = 1$

(三)我們從找 mod 7 中(-1)所對應的特徵向量中簡化計算過程，適時配合費馬小定理加以一般化，推廣至找 mod $p$ 中(-1)所對應的特徵向量。

mod $p$ 中，(-1)所對應的特徵向量$\mathrm{w} = [t_1 \quad t_2 \quad \cdots \quad \cdots \quad t_{p-1}]^T$

，其中$t_k = \left(\frac{k}{p}\right) \equiv k^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p)$ ，$1 \le k \le p-1$，$\left(\frac{k}{p}\right)$為勒讓德符號。

(四)有了 mod $p$ 中(-1)的特徵向量後，我們利用與算 3、5、7 相同的手法，導出了$r_j$一般式。

對於所有的正整數$n$，令$r_i$為巴斯卡三角形第$n$列$C_0^n, C_1^n, C_2^n, \cdots, C_n^n$除以$p$餘$i$的個數，則

$$\sum_{i=1}^{p-1}\left(\frac{i}{p}\right) r_i = \prod_{l=1}^{p-1}\left[\sum_{j=1}^{p-1}\left(\frac{j}{p}\right) f(l,p,j)\right]^{a_l}$$

，其中$\left(\frac{i}{p}\right)$和$\left(\frac{j}{p}\right)$為勒讓德符號，而$a_l$為$n$化為$p$進位後$l$的個數$(1 \le l \le p-1)$，

且$f(l,p,j)$為$C_0^l, C_1^l, C_2^l, \cdots, C_l^l$除以$p$餘$j$的個數$(1 \le j \le p-1)$

(五)利用公式，我們算出了更多個質數中$r_j$的關係式:

(1)mod 11 時，

$$(r_1 + r_3 + r_4 + r_5 + r_9) - (r_2 + r_6 + r_7 + r_8 + r_{10})$$

$$= 2^{a_1} \cdot 1^{a_2} \cdot 4^{a_3} \cdot 3^{a_4} \cdot 2^{a_5} \cdot 3^{a_6} \cdot (-4)^{a_7} \cdot 1^{a_8} \cdot 6^{a_9} \cdot 1^{a_{10}}$$

(2)mod 13 時，

$$(r_1 + r_3 + r_4 + r_9 + r_{10} + r_{12}) - (r_2 + r_5 + r_6 + r_7 + r_8 + r_{11})$$

$$= 2^{a_1} \cdot 1^{a_2} \cdot 4^{a_3} \cdot 3^{a_4} \cdot 2^{a_5} \cdot (-3)^{a_6} \cdot 0^{a_7} \cdot (-1)^{a_8} \cdot 6^{a_9} \cdot 1^{a_{10}} \cdot 0^{a_{11}} \cdot 13^{a_{12}}$$

(3)mod 17 時，

$$(r_1 + r_2 + r_4 + r_8 + r_9 + r_{13} + r_{15} + r_{16}) - (r_3 + r_5 + r_6 + r_7 + r_{10} + r_{11} + r_{12} + r_{14})$$

$$= 2^{a_1} \cdot 3^{a_2} \cdot 0^{a_3} \cdot 3^{a_4} \cdot (-2)^{a_5} \cdot 1^{a_6} \cdot 4^{a_7} \cdot 1^{a_8} \cdot 6^{a_9} \cdot (-3)^{a_{10}} \cdot (-4)^{a_{11}} \cdot 3^{a_{12}} \cdot 2^{a_{13}} \cdot (-1)^{a_{14}} \cdot 0^{a_{15}} \cdot 17^{a_{16}}$$

(4)mod 19 時，

$$(r_1 + r_4 + r_5 + r_6 + r_7 + r_9 + r_{11} + r_{16} + r_{17}) - (r_2 + r_3 + r_8 + r_{10} + r_{12} + r_{13} + r_{14} + r_{15} + r_{18})$$

$$= 2^{a_1} \cdot 1^{a_2} \cdot 0^{a_3} \cdot 5^{a_4} \cdot 2^{a_5} \cdot 3^{a_6} \cdot 4^{a_7} \cdot (-1)^{a_8} \cdot 2^{a_9} \cdot 7^{a_{10}} \cdot 8^{a_{11}} \cdot 3^{a_{12}} \cdot (-2)^{a_{13}} \cdot (-3)^{a_{14}} \cdot (-4)^{a_{15}} \cdot 9^{a_{16}} \cdot 6^{a_{17}} \cdot 1^{a_{18}}$$

# 玖、參考資料

一、數學奧林匹亞大集新編；黃宣國著，中國科學技術大學出版社。

二、Linear Algebra with Applications; W.Keith Nicholson 著,黃孟棟 編譯，東華書局。

三、費馬小定理；
https://zh.wikipedia.org/wiki/%E8%B4%B9%E9%A9%AC%E5%B0%8F%E5%AE%9A%E7%90%86
四、勒讓德符號；

https://zh.wikipedia.org/wiki/%E5%8B%92%E8%AE%A9%E5%BE%B7%E7%AC%A6%E5%8F%B7

## 【評語】050411

此研究解決了 IMO 的競賽題，並將其推廣到 p=2、3、5、7 的情形。結論不宜列入眾所皆知的結果，參考文獻的探討需加強。

## 作品海報

## 摘要

我們利用進位分解將組合數對一質數做同餘，並探討巴斯卡三角形其中一列對一質數同餘後，各個餘數數量的關係。


## 壹、研究動機

$n$是一個正整數，$n+1$個正整數$C_0^n, C_1^n, \cdots, C_n^n$中，除以 5 餘$j(1 \le j \le 4)$的個數用$r_j$表示，求證$r_1 + r_4 \ge r_2 + r_3$。

（數學奧林匹亞大集新編）

這題的答案用數學歸納法證明。但我們好奇是否能將$r_1, r_2, r_3, r_4$分別的數值求出，於是開始對類似的問題進行探討。

## 貳、研究目的

求出$r_j$的各別數值為何，並探討在比 5 更大的質數中，是否亦存在與原題目類似的$r_j$數量大小關係。

## 參、研究設備與器材

紙、筆、電腦。

## 肆、研究過程與方法

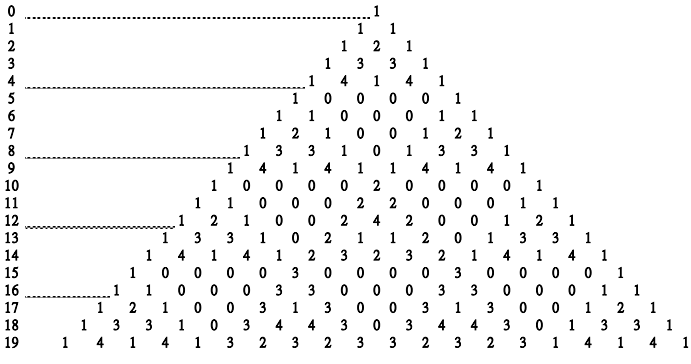
我們介紹 Lucas 定理。

〔定理〕令$p$為質數，非負整數$n$、$m$化為$p$進位：$\begin{cases} n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 = (n_k n_{k-1} \cdots n_0)_p \\ m = m_k p^k + m_{k-1} p^{k-1} + \cdots m_1 p + m_0 = (m_k m_{k-1} \cdots m_0)_p \end{cases}$。

若對於所有的 $0 \le l \le k$滿足$n_l \ge m_l$，則$C_m^n \equiv C_{m_k}^{n_k} C_{m_{k-1}}^{n_{k-1}} \cdots C_{m_1}^{n_1} C_{m_0}^{n_0} (\mathrm{mod}\ p)$，否則$C_m^n \equiv 0 (\mathrm{mod}\ p)$。

〔舉例〕滿足：$n = 2017 = (5611)_7$，$m = 1618 = (4501)_7$，所以$C_{1618}^{2017} \equiv C_4^5 C_5^6 C_0^1 C_1^1 \equiv 30 \equiv 2 \ (\mathrm{mod}\ 7)$

不滿足：$n = 2017 = (5611)_7$，$m = 1619 = (4502)_7$，因為$n_0 = 1 < m_0 = 2$，所以$C_{1619}^{2017} \equiv 0 \ (\mathrm{mod}\ 7)$



巴斯卡三角形對 5 同餘圖

| 第n列 | n化為五進位 | 0的個數 | 1的個數 | 2的個數 | 3的個數 | 4的個數 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 2 | 0 | 0 | 0 |
| 2 | 2 | 0 | 2 | 1 | 0 | 0 |
| 3 | 3 | 0 | 2 | 0 | 2 | 0 |
| 4 | 4 | 0 | 3 | 0 | 0 | 2 |
| 5 | 10 | 4 | 2 | 0 | 0 | 0 |
| 6 | 11 | 3 | 4 | 0 | 0 | 0 |
| 7 | 12 | 2 | 4 | 2 | 0 | 0 |
| 8 | 13 | 1 | 4 | 0 | 4 | 0 |
| 9 | 14 | 0 | 6 | 0 | 0 | 4 |
| 10 | 20 | 8 | 2 | 1 | 0 | 0 |
| 11 | 21 | 6 | 4 | 2 | 0 | 0 |
| 12 | 22 | 4 | 4 | 4 | 0 | 1 |
| 13 | 23 | 2 | 6 | 2 | 4 | 0 |
| 14 | 24 | 0 | 6 | 3 | 2 | 4 |
| 15 | 30 | 12 | 2 | 0 | 2 | 0 |
| 16 | 31 | 9 | 4 | 0 | 4 | 0 |
| 17 | 32 | 6 | 6 | 2 | 4 | 0 |
| 18 | 33 | 3 | 4 | 0 | 8 | 4 |
| 19 | 34 | 0 | 6 | 4 | 6 | 4 |

巴斯卡三角形對 5 同餘表

## 伍、研究結果

本章節將定義一些函數，利用排列組合、遞迴式、矩陣等方式將$r_j$的數值求出。

### 一、$r_j$、$F(n,p,j)$、$f(a_1, a_2, \cdots, a_{p-1}, j)$的定義

〔定義〕巴斯卡三角形第$n$列$C_0^n, C_1^n, \cdots, C_n^n$除以質數$p$餘$j(0 \le j \le p-1)$的個數用$r_j = F(n,p,j)$表示。

〔命題〕$n$化為$p$進位，$n = (n_k n_{k-1} \cdots n_0)_p$，若$n_k, n_{k-1}, \cdots n_1, n_0$裡有$a_1$個 1、$a_2$個 2、…、$a_{p-1}$個$(p-1)$，

則 $r_0 = F(n,p,0) = n + 1 - 2^{a_1} 3^{a_2} 4^{a_3} 5^{a_4} \cdots p^{a_{p-1}}$。

〔證明〕根據 Lucas 定理，若所有的$n_l \ge m_l$時，則$C_m^n$不同餘 0。若$n_l = j$，則$m_l = 0, 1, \cdots, j$共$j+1$種選擇$(1 \le j \le p-1)$。

因此巴斯卡三角形第$n$列中不為$p$的倍數有$2^{a_1} 3^{a_2} 4^{a_3} 5^{a_4} \cdots p^{a_{p-1}}$個。

〔說明〕更進一步，$F(n,p,j)$中的值只與$a_1, a_2, \cdots, a_{p-1}$有關$(1 \le j \le p-1)$，所以我們定義以下函數。

〔定義〕$r_j = f(a_1, a_2, \cdots, a_{p-1}, j)$，其中$a_l$為$n$化為$p$進位後$l$的個數$(1 \le l, j \le p-1)$。

〔例〕取$8 = (13)_5$，$16 = (31)_5$，則$a_1 = a_3 = 1$，$a_2 = a_4 = 0$，且$F(8,5,j) = F(16,5,j) = f(1,0,1,0,j)$，$(1 \le j \le 4)$。

〔例〕取$13 = (23)_5$，$17 = (32)_5$，則$a_2 = a_3 = 1$，$a_1 = a_4 = 0$，且$F(13,5,j) = F(17,5,j) = f(0,1,1,0,j)$，$(1 \le j \le 4)$。

### 二、質數 2、3、5、7 及 $p$的$r_j$公式

〔mod2〕$r_1 = f(a_1, 1) = 2^{a_1}$

〔mod3〕$\begin{bmatrix} f(a_1,a_2,1) \\ f(a_1,a_2,2) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}^{a_1} \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^{a_2} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$，$\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \frac{2^{a_1}}{2} \begin{bmatrix} (3^{a_2}+1) \\ (3^{a_2}-1) \end{bmatrix}$

〔mod5〕我們寫出若干遞迴式後併為矩陣。考慮$f(a_1, a_2, a_3+1, a_4, 2)$與$f(a_1, a_2, a_3, a_4, j)$之間的關係。

$a_3 + 1$代表$n = (n_k n_{k-1} \cdots n_0)_p$多插入個 3 得到$n'$，則$C_{m'}^{n'} \equiv C_k^3 C_m^n \equiv 2 (\mathrm{mod}\ p)$。

所以$(C_k^3, C_m^n) \equiv (2,1), (1,2), (4,3), (3,4)$，且 $C_0^3, C_1^3, C_2^3, C_3^3 = 1,3,3,1$，可得遞迴式：

$f(a_1, a_2, a_3+1, a_4, 2)$

$= F(3,5,2) \times f(a_1,a_2,a_3,a_4,1) + F(3,5,1) \times f(a_1,a_2,a_3,a_4,2) + F(3,5,4) \times f(a_1,a_2,a_3,a_4,3) + F(3,5,3) \times f(a_1,a_2,a_3,a_4,4)$

$= 0 f(a_1,a_2,a_3,a_4,1) + 2 f(a_1,a_2,a_3,a_4,2) + 0 f(a_1,a_2,a_3,a_4,3) + 2 f(a_1,a_2,a_3,a_4,4)$

分別以$a_1+1$、$a_2+1$、$a_3+1$、$a_4+1$與餘1,2,3,4寫出 16 個遞迴式，併為 4 個遞迴矩陣，就可以將$a_1, a_2, a_3, a_4$都遞降為 0。

$$\begin{bmatrix} f(a_1,a_2,a_3,a_4,1) \\ f(a_1,a_2,a_3,a_4,2) \\ f(a_1,a_2,a_3,a_4,3) \\ f(a_1,a_2,a_3,a_4,4) \end{bmatrix} = \underbrace{\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}^{a_1}}_{\text{設為} A_{1,5}} \underbrace{\begin{bmatrix} 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 \end{bmatrix}^{a_2}}_{\text{設為} A_{2,5}} \underbrace{\begin{bmatrix} 2 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{bmatrix}^{a_3}}_{\text{設為} A_{3,5}} \underbrace{\begin{bmatrix} 2 & 0 & 0 & 3 \\ 0 & 2 & 3 & 0 \\ 0 & 3 & 2 & 0 \\ 3 & 0 & 0 & 2 \end{bmatrix}^{a_4}}_{\text{設為} A_{4,5}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

令$P_{2,5}=\begin{bmatrix}0&0&1&0\\1&0&0&0\\0&0&0&1\\0&1&0&0\end{bmatrix}$，則$A_{1,5}=2I$，$A_{2,5}=2I+P_{2,5}$，$A_{3,5}=2I+2{P_{2,5}}^3$，$A_{4,5}=2I+3{P_{2,5}}^2$。

對角化$P_{2,5}=CDC^{-1}$，得$C=\begin{bmatrix}1&1&1&1\\1&-i&-1&i\\1&i&-1&-i\\1&-1&1&-1\end{bmatrix}$，$D=\begin{bmatrix}1&0&0&0\\0&i&0&0\\0&0&-1&0\\0&0&0&-i\end{bmatrix}$，$C^{-1}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\frac{1}{4}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$。

因此$\begin{bmatrix}r_1\\r_2\\r_3\\r_4\end{bmatrix}=(2I)^{a_1}(2I+P_{2,5})^{a_2}(2I+2{P_{2,5}}^3)^{a_3}(2I+3{P_{2,5}}^2)^{a_4}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=C(2I)^{a_1}(2I+D)^{a_2}(2I+2D^3)^{a_3}(2I+3D^2)^{a_4}C^{-1}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$。

乘開後得$\begin{bmatrix}r_1\\r_2\\r_3\\r_4\end{bmatrix}=\frac{2^{a_1}}{4}\begin{bmatrix}3^{a_2}4^{a_3}5^{a_4}+(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}+1^{a_2}0^{a_3}5^{a_4}+(2-i)^{a_2}(2+2i)^{a_3}1^{a_4}\\3^{a_2}4^{a_3}5^{a_4}-i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}-1^{a_2}0^{a_3}5^{a_4}+i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4}\\3^{a_2}4^{a_3}5^{a_4}+i(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}-1^{a_2}0^{a_3}5^{a_4}-i(2-i)^{a_2}(2+2i)^{a_3}1^{a_4}\\3^{a_2}4^{a_3}5^{a_4}-(2+i)^{a_2}(2-2i)^{a_3}1^{a_4}+1^{a_2}0^{a_3}5^{a_4}-(2-i)^{a_2}(2+2i)^{a_3}1^{a_4}\end{bmatrix}$

〔mod7〕分別以$a_1+1$、$a_2+1$、$a_3+1$、$a_4+1$、$a_5+1$、$a_6+1$與餘1,2,3,4,5,6寫出36個遞迴式，可併為6個遞迴矩陣，

就可以將$a_1,a_2,a_3,a_4,a_5,a_6$都遞降為0。

$$\begin{bmatrix}f(a_1,a_2,a_3,a_4,a_5,a_6,1)\\f(a_1,a_2,a_3,a_4,a_5,a_6,2)\\f(a_1,a_2,a_3,a_4,a_5,a_6,3)\\f(a_1,a_2,a_3,a_4,a_5,a_6,4)\\f(a_1,a_2,a_3,a_4,a_5,a_6,5)\\f(a_1,a_2,a_3,a_4,a_5,a_6,6)\end{bmatrix}=\begin{bmatrix}2&0&0&0&0&0\\0&2&0&0&0&0\\0&0&2&0&0&0\\0&0&0&2&0&0\\0&0&0&0&2&0\\0&0&0&0&0&2\end{bmatrix}^{a_1}\begin{bmatrix}2&0&0&1&0&0\\1&2&0&0&0&0\\0&0&2&0&1&0\\0&1&0&2&0&0\\0&0&0&0&2&1\\0&0&1&0&0&2\end{bmatrix}^{a_2}\begin{bmatrix}2&0&0&0&2&0\\0&2&2&0&0&0\\0&0&2&0&0&0\\0&0&0&2&0&2\\0&0&0&0&2&2\\0&2&0&0&0&2\end{bmatrix}^{a_3}\begin{bmatrix}2&2&0&0&0&1\\0&2&0&2&1&0\\0&0&2&1&0&2\\2&0&1&2&0&0\\0&1&2&0&2&0\\1&0&0&0&2&2\end{bmatrix}^{a_4}\begin{bmatrix}2&0&2&0&2&0\\0&2&2&0&0&2\\2&2&2&0&0&0\\0&0&0&2&2&2\\2&0&0&2&2&0\\0&2&0&2&0&2\end{bmatrix}^{a_5}\begin{bmatrix}4&0&0&0&0&3\\0&4&0&0&3&0\\0&0&4&3&0&0\\0&0&3&4&0&0\\0&3&0&0&4&0\\3&0&0&0&0&4\end{bmatrix}^{a_6}\begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix}$$

設為$A_{1,7}$　設為$A_{2,7}$　設為$A_{3,7}$　設為$A_{4,7}$　設為$A_{5,7}$　設為$A_{6,7}$

令$P_{3,7}=\begin{bmatrix}0&0&0&0&1&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&0&0&1&0&0\\0&1&0&0&0&0\end{bmatrix}$，則$A_{1,7}=2I$，$A_{2,7}=2I+{P_{3,7}}^2$，$A_{3,7}=2I+2P_{3,7}$，$A_{4,7}=2I+2{P_{3,7}}^4+{P_{3,7}}^3$，$A_{5,7}=2I+2P_{3,7}+2{P_{3,7}}^5$，$A_{6,7}=4I+3{P_{3,7}}^3$。

對角化$P_{3,7}=CDC^{-1}$，得$C=\begin{bmatrix}1^6&\omega^6&(\omega^2)^6&(\omega^3)^6&(\omega^4)^6&(\omega^5)^6\\1^4&\omega^4&(\omega^2)^4&(\omega^3)^4&(\omega^4)^4&(\omega^5)^4\\1^5&\omega^5&(\omega^2)^5&(\omega^3)^5&(\omega^4)^5&(\omega^5)^5\\1^2&\omega^2&(\omega^2)^2&(\omega^3)^2&(\omega^4)^2&(\omega^5)^2\\1^1&\omega^1&(\omega^2)^1&(\omega^3)^1&(\omega^4)^1&(\omega^5)^1\\1^3&\omega^3&(\omega^2)^3&(\omega^3)^3&(\omega^4)^3&(\omega^5)^3\end{bmatrix}$，$D=\begin{bmatrix}1&0&0&0&0&0\\0&\omega&0&0&0&0\\0&0&\omega^2&0&0&0\\0&0&0&\omega^3&0&0\\0&0&0&0&\omega^4&0\\0&0&0&0&0&\omega^5\end{bmatrix}$，$C^{-1}\begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix}=\frac{1}{6}\begin{bmatrix}1\\1\\1\\1\\1\\1\end{bmatrix}$，$(\omega=e^{\frac{\pi}{3}i})$。

因此$\begin{bmatrix}r_1\\r_2\\r_3\\r_4\\r_5\\r_6\end{bmatrix}=C(2I)^{a_1}(2I+D^2)^{a_2}(2I+2D)^{a_3}(2I+2D^4+D^3)^{a_4}\left(2I+2D+D^5\right)^{a_5}(4I+3D^3)^{a_6}C^{-1}\begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix}$。

乘開後得$\begin{bmatrix}r_1\\r_2\\r_3\\r_4\\r_5\\r_6\end{bmatrix}=\frac{2^{a_1}}{6}\begin{bmatrix}1^6&\omega^6&(\omega^2)^6&(\omega^3)^6&(\omega^4)^6&(\omega^5)^6\\1^4&\omega^4&(\omega^2)^4&(\omega^3)^4&(\omega^4)^4&(\omega^5)^4\\1^5&\omega^5&(\omega^2)^5&(\omega^3)^5&(\omega^4)^5&(\omega^5)^5\\1^2&\omega^2&(\omega^2)^2&(\omega^3)^2&(\omega^4)^2&(\omega^5)^2\\1^1&\omega^1&(\omega^2)^1&(\omega^3)^1&(\omega^4)^1&(\omega^5)^1\\1^3&\omega^3&(\omega^2)^3&(\omega^3)^3&(\omega^4)^3&(\omega^5)^3\end{bmatrix}\begin{bmatrix}3^{a_2}4^{a_3}5^{a_4}6^{a_5}7^{a_6}\\(2+\omega^2)^{a_2}(2+2\omega)^{a_3}(1-2\omega)^{a_4}(2+2\omega-2\omega^2)^{a_5}1^{a_6}\\(2-\omega^2)^{a_2}(2+2\omega^2)^{a_3}(3+2\omega^2)^{a_4}(2-2\omega+2\omega^2)^{a_5}7^{a_6}\\3^{a_2}0^{a_3}3^{a_4}(-2)^{a_5}1^{a_6}\\(2+\omega^2)^{a_2}(2-2\omega)^{a_3}(3-2\omega)^{a_4}(2-2\omega+2\omega^2)^{a_5}7^{a_6}\\(2-\omega)^{a_2}(2-2\omega^2)^{a_3}(1+2\omega^2)^{a_4}(1+2\omega-2\omega^2)^{a_5}1^{a_6}\end{bmatrix}$

〔說明〕1. 定義$0^0=1$。　2. 當$C$的第一列全為1時，$C^{-1}$不須實際計算。

〔mod $p$〕分別以$a_1+1$、$a_2+1$、…、$a_{p-1}+1$與餘$1,2,\cdots,p-1$寫出遞迴式。

$$f(a_1,\cdots,a_k+1,\cdots,a_{p-1},j)=\sum_{l=1}^{p-1}F\left(k,p,\frac{j}{l}\right)\times f(a_1,\cdots,a_k,\cdots,a_{p-1},l)\ ,\ (1\le j,k\le p-1)$$

定義$P_{k,p}$為$(p-1)\times(p-1)$的方陣使得$\left[P_{k,p}\right]_{ij}=\begin{cases}1\text{，若}i\equiv kj\ (\mathrm{mod}\ p)\\0\text{，其他}\end{cases}$，則$P_{k,p}$是「置換矩陣」，且滿足：

(1)若$xy\equiv z(\mathrm{mod}\ p)$，則$P_{x,p}P_{y,p}=P_{z,p}$　(2)若$x^n=y(\mathrm{mod}\ p)$，則${P_{x,p}}^n=P_{y,p}$　(3) ${P_{x,p}}^{\mathrm{T}}={P_{x,p}}^{-1}=P_{x^{-1},p}$

運用$A_{k,p}$寫出遞迴矩陣，並將$a_1,a_2,\cdots,a_{p-1}$都遞降為0。

則$A_{k,p}=\begin{bmatrix}F(k,p,\frac{1}{1})&F(k,p,\frac{1}{2})&\cdots&F(k,p,\frac{1}{p-1})\\F(k,p,\frac{2}{1})&F(k,p,\frac{2}{2})&\cdots&F(k,p,\frac{2}{p-1})\\\cdots&\cdots&\cdots&\cdots\\F(k,p,\frac{p-1}{1})&F(k,p,\frac{p-1}{2})&\cdots&F(k,p,\frac{p-1}{p-1})\end{bmatrix}=\sum_{j=1}^{p-1}F(k,p,j)\,P_{j,p}$，$\begin{bmatrix}r_1\\r_2\\\vdots\\r_{p-1}\end{bmatrix}=\left(A_{1,p}\right)^{a_1}\left(A_{2,p}\right)^{a_2}\cdots\left(A_{p-1,p}\right)^{a_{p-1}}\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}$

〔定義〕若$\alpha$滿足$\{\alpha^1,\alpha^2,\alpha^3,\cdots,\alpha^{p-1}\}=\{1,2,3,\cdots,p-1\}$，則稱$\alpha$為「可用」。

將所有的$P_{j,p}$用$P_{\alpha,p}$的次方表示後，則$A_{k,p}$為$P_{\alpha,p}$的多項式，將$P_{\alpha,p}$對角化並帶入可求得$\begin{bmatrix}r_1\\r_2\\\vdots\\r_{p-1}\end{bmatrix}$。

## 陸、討論 在這一章節，我們將探討研究動機中的數奧問題，並加以推廣。

### 一、研究動機在 $p=3$、5、7的結果

〔mod3〕$r_1-r_2=2^{a_1}>0$

〔mod5〕$(r_1+r_4)-(r_2+r_3)=2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}\geq 0$

〔證明〕矩陣$P_{2,5}$特徵值$(-1)$的特徵向量$x=[1\quad -1\quad -1\quad 1]^{\mathrm{T}}$，將$x^{\mathrm{T}}$乘在每個$A_{i,5}$矩陣前，得到下列4式：

$x^{\mathrm{T}}A_{1,5}=2x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{2,5}=1x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{3,5}=0x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{4,5}=5x^{\mathrm{T}}$

把$x^{\mathrm{T}}$乘在$\begin{bmatrix}r_1\\r_2\\r_3\\r_4\end{bmatrix}=(A_{1,5})^{a_1}(A_{2,5})^{a_2}(A_{3,5})^{a_3}(A_{4,5})^{a_4}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$的前面化簡得證。

〔mod7〕$(r_1+r_2+r_4)-(r_3+r_5+r_6)=2^{a_1}\cdot 3^{a_2}\cdot 0^{a_3}\cdot 3^{a_4}\cdot(-2)^{a_5}\cdot 1^{a_6}$

〔證明〕矩陣$P_{3,7}$特徵值$(-1)$的特徵向量$x=[1\quad 1\quad -1\quad 1\quad -1\quad -1]^{\mathrm{T}}$，將$x^{\mathrm{T}}$乘在每個$A_{i,7}$矩陣前，得到下列6式：

$x^{\mathrm{T}}A_{1,7}=2x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{2,7}=3x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{3,7}=0x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{4,7}=3x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{5,7}=(-2)x^{\mathrm{T}}$，$x^{\mathrm{T}}A_{6,7}=1x^{\mathrm{T}}$

把$x^{\mathrm{T}}$乘在$\begin{bmatrix}r_1\\r_2\\r_3\\r_4\\r_5\\r_6\end{bmatrix}=(A_{1,7})^{a_1}(A_{2,7})^{a_2}(A_{3,7})^{a_3}(A_{4,7})^{a_4}(A_{5,7})^{a_5}(A_{6,7})^{a_6}\begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix}$的前面化簡得證。

### 二、轉置矩陣的特徵向量

〔觀察〕考慮$p=7$，$\alpha=3$，矩陣$P_{3,7}$的特徵值$\omega$的特徵向量為$x=[x_1\quad x_2\quad x_3\quad x_4\quad x_5\quad x_6]^{\mathrm{T}}$。

由$(\omega I-P_{3,7})x=O$可得$x_1=\omega x_3$，$x_2=\omega x_6$，$x_3=\omega x_2$，$x_4=\omega x_5$，$x_5=\omega x_1$，$x_6=\omega x_4$。

所以$x_j=\omega x_{3j}(1\leq j\leq 6)$。令$x_1=1$，則$x_{3j}=\omega^{-j}$。

〔結果〕考慮一般的質數$p$與可用的$\alpha$，矩陣$P_{\alpha,p}$的特徵值$(-1)$的特徵向量為$x=[x_1\quad x_2\quad \cdots\quad x_{p-1}]^{\mathrm{T}}$。

所以$x_j=(-1)x_{\alpha j}(1\leq j\leq p-1)$。令$x_1=1$，則$x_{\alpha^j}=(-1)^j$。

〔定義〕勒讓德符號(Legendre symbol)：$\left(\frac{k}{p}\right)=\pm 1\equiv k^{\frac{p-1}{2}}(\mathrm{mod}\ p)$

〔公式〕矩陣$P_{\alpha,p}$的特徵值$(-1)$的特徵向量$x=\left[\left(\frac{1}{p}\right)\quad\left(\frac{2}{p}\right)\quad\cdots\quad\left(\frac{p-1}{p}\right)\right]^{\mathrm{T}}$。

〔證明〕若$k=\alpha^{2t}(t\in N)$，則$k^{\frac{p-1}{2}}=(\alpha^{2t})^{\frac{p-1}{2}}=(\alpha^t)^{p-1}\equiv 1$(費馬小定理)。

若$k=\alpha^{2t-1}$，則$k^{\frac{p-1}{2}}=(\alpha^{2t-1})^{\frac{p-1}{2}}=(\frac{\alpha^{2t}}{\alpha})^{\frac{p-1}{2}}=\frac{(\alpha^t)^{p-1}}{(\alpha)^{\frac{p-1}{2}}}\equiv\frac{1}{(\alpha)^{\frac{p-1}{2}}}\equiv(-1)$。因此$\left(\frac{\alpha^j}{p}\right)=(-1)^j$。

### 三、研究動機的一般結果

〔公式〕對於所有的正整數$n$，令$r_i$為巴斯卡三角形第$n$列$C_0^n,C_1^n,\cdots,C_n^n$除以$p$餘$i$的個數，則：

$$\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)r_i=\prod_{l=1}^{p-1}\left[\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\mathrm{F}(l,p,j)\right]^{a_l}$$

其中$\mathrm{F}(l,p,j)$為$C_0^l,C_1^l,\cdots,C_l^l$除以$p$餘$j$的個數，$a_l$為$n$化為$p$進位後$l$的個數，$\left(\frac{i}{p}\right)$和$\left(\frac{j}{p}\right)$為勒讓德符號$(1\leq i,j,l\leq p-1)$。

〔推導〕若$j=\alpha^t$，則$x^{\mathrm{T}}P_{j,p}=x^{\mathrm{T}}P_{\alpha^t,p}=\left[P_{\alpha,p}{}^{-t}x\right]^{\mathrm{T}}=[(-1)^{-t}x]^{\mathrm{T}}=\left(\frac{\alpha^t}{p}\right)x^{\mathrm{T}}=\left(\frac{j}{p}\right)x^{\mathrm{T}}$。

將$x^{\mathrm{T}}$乘在$A_{k,p}=\sum_{j=1}^{p-1}F(k,p,j)\,P_{j,p}$前，得$x^{\mathrm{T}}A_{k,p}=\sum_{j=1}^{p-1}F(k,p,j)x^{\mathrm{T}}P_{j,p}=\sum_{j=1}^{p-1}F(k,p,j)\left(\frac{j}{p}\right)x^{\mathrm{T}}$。

把$x^{\mathrm{T}}$乘在$[r_1\quad r_2\quad\cdots\quad r_{p-1}]^T=(A_{1,p})^{a_1}(A_{2,p})^{a_2}\cdots(A_{k,p})^{a_k}\cdots(A_{p-1,p})^{a_{p-1}}[1\quad 0\quad\cdots\quad 0]^{\mathrm{T}}$的前面化簡得證。

### 四、使用公式計算出更多結果

〔mod11〕$(r_1+r_3+r_4+r_5+r_9)-(r_2+r_6+r_7+r_8+r_{10})=2^{a_1}\cdot 1^{a_2}\cdot 4^{a_3}\cdot 3^{a_4}\cdot 2^{a_5}\cdot 3^{a_6}\cdot(-4)^{a_7}\cdot 1^{a_8}\cdot 6^{a_9}\cdot 1^{a_{10}}$

〔mod13〕$(r_1+r_3+r_4+r_9+r_{10}+r_{12})-(r_2+r_5+r_6+r_7+r_8+r_{11})=2^{a_1}\cdot 1^{a_2}\cdot 4^{a_3}\cdot 3^{a_4}\cdot 2^{a_5}\cdot(-3)^{a_6}\cdot 0^{a_7}\cdot(-1)^{a_8}\cdot 6^{a_9}\cdot 1^{a_{10}}\cdot 0^{a_{11}}\cdot 13^{a_{12}}$

〔mod17〕$(r_1+r_2+r_4+r_8+r_9+r_{13}+r_{15}+r_{16})-(r_3+r_5+r_6+r_7+r_{10}+r_{11}+r_{12}+r_{14})$

$=2^{a_1}\cdot 3^{a_2}\cdot 0^{a_3}\cdot 3^{a_4}\cdot(-2)^{a_5}\cdot 1^{a_6}\cdot 4^{a_7}\cdot 1^{a_8}\cdot 6^{a_9}\cdot(-3)^{a_{10}}\cdot(-4)^{a_{11}}\cdot 3^{a_{12}}\cdot 2^{a_{13}}\cdot(-1)^{a_{14}}\cdot 0^{a_{15}}\cdot 17^{a_{16}}$

〔mod19〕$(r_1+r_4+r_5+r_6+r_7+r_9+r_{11}+r_{16}+r_{17})-(r_2+r_3+r_8+r_{10}+r_{12}+r_{13}+r_{14}+r_{15}+r_{18})$

$=2^{a_1}\cdot 1^{a_2}\cdot 0^{a_3}\cdot 5^{a_4}\cdot 2^{a_5}\cdot 3^{a_6}\cdot 4^{a_7}\cdot(-1)^{a_8}\cdot 2^{a_9}\cdot 7^{a_{10}}\cdot 8^{a_{11}}\cdot 3^{a_{12}}\cdot(-2)^{a_{13}}\cdot(-3)^{a_{14}}\cdot(-4)^{a_{15}}\cdot 9^{a_{16}}\cdot 6^{a_{17}}\cdot 1^{a_{18}}$

## 柒、結論

利用遞迴式及矩陣給出$r_j$的公式，利用特徵向量給出$r_1,r_2,\cdots,r_{p-1}$的關係式。

## 捌、參考資料


一、數學奧林匹亞大集新編；黃宣國著，中國科學技術大學出版社。

二、Linear Algebra with Applications; W.Keith Nicholson 著,黃孟糠 編譯，東華書局。