

# 中華民國第42屆中小學科學展覽會

::: 作品說明書 :::

## 高中-數學科

科 別：數 學 科

組 別：高 中 組

作品名稱：洗牌的數學

關 鍵 詞：向下洗牌、性質(F)

編 號：040406

---

**學校名稱：**

國立板橋高級中學

**作者姓名：**

姜兆徽、吳承峰、林郁翔、廖奕璋

**指導老師：**

蔡志強、楊朗生



# 洗牌的數學

## 壹、摘要

本文主要是將生活中玩撲克牌時分兩堆的洗牌程序，抽象化為將  $n$  張牌等份為  $m$  堆，探討至少需要幾次「向下洗牌」才能回覆到原來次序。在處理過程中，我們先利用電腦以歸納原則觀察後，發現與整數系中的餘數有密切的關係。於是利用整數系中最基本的性質：長除法原理及多項式的因式分解著手。當我們從  $n$  的標準分解式作分類討論時，發現以 2 為質因數的  $n$  的相關問題，如當  $n=2^2p$  時( $p$  為質數)，則將牌等分成堆數不同，要回覆到原來次序的「向下洗牌」，所需的最少次數就會不一樣。而當  $n=2^3p$  時，所需的最少次數則又似會都一樣。就我們目前所學，尚無能力解決這類問題。故僅考慮牌數  $n=a^b$  及  $n=a^b+1$ ( $a, b$  為正整數)兩種情形。為方便計，我們也利用模的符號及一些簡單性質。

## 貳、研究動機

### (一).問題介紹

玩撲克牌時總要洗牌，洗牌方式之一是將牌等分成兩堆，然後將兩堆牌「交叉放置」，也就是將牌等分成 A、B 兩堆後，先從 A 堆中取出最上面的一張(稱之為  $a_1$ )，再從 B 堆中取出最上面的一張(稱之為  $b_1$ )放在  $a_1$  後面，接下來從 A 堆剩下的牌中取出最上面的一張(稱之為  $a_2$ )放在  $b_1$  後面，又從 B 堆剩下的牌中取出最上面的一張(稱之為  $b_2$ )放在  $a_2$  後面，依此程序繼續下去。由於我們洗牌過程是從上面開始依序往下取，因此我們將此洗牌程序稱為一次「向下洗牌」，底下是兩個例子。

[例一]將編號為 1、2、3、4 的 4 張牌，分成  $\{1,2\}$ ， $\{3,4\}$  兩堆，則

|   | 洗牌前 | 洗牌後 |
|---|-----|-----|
| A | 1   | 1   |
|   | 2   | 3   |
| B | 3   | 2   |
|   | 4   | 4   |

[例二]將編號為 1、2、3、4、5、6 的 6 張牌，分成  $\{1,2,3\}$ ， $\{4,5,6\}$  兩堆，則

|   | 洗牌前 | 洗牌後 |
|---|-----|-----|
| A | 1   | 1   |
|   | 2   | 4   |
|   | 3   | 2   |
| B | 4   | 5   |
|   | 5   | 3   |
|   | 6   | 6   |

我們發現一個有趣的現象是：若重複上面的洗牌程序，只要經過有限次「向下洗牌」後，就會回覆到原來次序。比如：當牌數為 4 張時，如下圖所示，只需 2 次「向下洗牌」就可回覆到原來的次序。

|   | 洗牌前 | 第一次洗牌後 | 第二次洗牌後 |
|---|-----|--------|--------|
| A | 1   | 1      | 1      |
|   | 2   | 3      | 2      |
| B | 3   | 2      | 3      |
|   | 4   | 4      | 4      |

又如：當牌數為 6 張時，如下圖所示，只需 4 次「向下洗牌」就可回復到原來的次序。

|   | 洗牌前 | 第一次洗牌後 | 第二次洗牌後 | 第三次洗牌後 | 第四次洗牌後 |
|---|-----|--------|--------|--------|--------|
| A | 1   | 1      | 1      | 1      | 1      |
|   | 2   | 4      | 5      | 3      | 2      |
|   | 3   | 2      | 4      | 5      | 3      |
| B | 4   | 5      | 3      | 2      | 4      |
|   | 5   | 3      | 2      | 4      | 5      |
|   | 6   | 6      | 6      | 6      | 6      |

P.Glaister 於文獻[1]中提到不一定要將牌只等分為兩堆，比如：當牌數為 6 張時，也可將牌等分為 A、B、C 三堆，每堆各 2 張。令人訝異的是仍只要經過有限次(實際上是 4 次)「向下洗牌」之後，就可以回復到原來的次序，如下圖所示。

|   | 洗牌前 | 第一次洗牌後 | 第二次洗牌後 | 第三次洗牌後 | 第四次洗牌後 |
|---|-----|--------|--------|--------|--------|
| A | 1   | 1      | 1      | 1      | 1      |
|   | 2   | 3      | 5      | 4      | 2      |
| B | 3   | 5      | 4      | 2      | 3      |
|   | 4   | 2      | 3      | 5      | 4      |
| C | 5   | 4      | 2      | 3      | 5      |
|   | 6   | 6      | 6      | 6      | 6      |

如此一來，就引發一個問題：當將牌等分成不一樣堆數時，要回復到原來的次序的「向下洗牌」，所需的最少次數可能會不一樣。比如：當牌數為 12 張時，就有如下表的現象。

| 堆數 | 每堆的牌數 | 「向下洗牌」的最少次數 |
|----|-------|-------------|
| 2  | 6     | 10          |
| 3  | 4     | 5           |
| 4  | 3     | 5           |
| 6  | 2     | 10          |

然而當牌數為 24 張時，無論等分成幾堆(不能 24 堆)，要回復到原來的次序的「向下洗牌」的最少次數都是 11 次。由此我們想到一個問題：當牌數滿足什麼性質時？無論我們將其等分成幾堆(不能每堆 1 張)，則要回復到原來的次序的「向下洗牌」的最少次數會都一樣。

## (二).與教材相關性

我們只要把問題抽象化，就會發現在高一上有關整數系的性質中，除法原理的餘數問題。與上述問題有密切的關係。比如：將 12 張牌，等分成六堆，每堆 2 張，要回復到原來的次序的「向下洗牌」的最少次數為 10 次。其實就是對所有正整數  $t$ ，以  $11$ (即  $12-1$ )除  $6^t$ ，所得餘數為 1 時， $t$  的最小值為 10。而等分成四堆，每堆 3 張，要回復到原來的次序的「向下洗牌」的最少次數為 5 次。其實就是對所有正整數  $t$ ，以  $11$  除  $4^t$ ，所得餘數為 1 時， $t$  的最小值為 5。然而當牌數為 24 張時，無論等分成幾堆(當然不能 24 堆)，要回復到原來的次序的「向下洗牌」的最少次數都是 11 次，其實就是對所有正整數  $t$  且  $d|24$ ，以  $23$ (即  $24-1$ )除  $d^t$ ，所得餘數為 1 時， $t$  的最小值均為 11。

### (三).文獻探討

首先，先定義一些符號。

$n$ ：表示一堆牌的總數。

$m$ ：表示將牌數為  $n$  張的牌分為相等的  $m$  堆(其中  $n > m > 1$ )。

$f(m, n)$ ：表示將  $n$  張牌分為相等的  $m$  堆(其中  $n > m > 1$ )後「向下洗牌」，要回復到原來的次序所需的「向下洗牌」最少次數。

在本文中， $n$ 、 $m$ 、 $f(m, n)$ ，這三個符號均表示上述定義。

P.Glaister 教授於文獻[1]中探討了  $n$ 、 $m$  與  $f(m, n)$  的一些簡單性質，並推導了刻劃  $f(m, n)$  的方程式的定理。

**[定理](P.Glaister)**

(1).若將  $n$  張牌等分為  $m$  堆(其中  $n > m > 1$ )「向下洗牌」，則要回復到原來的次序所需的「向下洗牌」最少次數  $f(m, n)$  是滿足下列同餘方程式的最小正整數  $k$

$$m^k \equiv 1 \pmod{n-1} \quad (*)$$

(2).若  $n$  張牌可以等分為  $m_1$  堆及  $m_2$  堆(其中  $n > m_1 > m_2 > 1$  且  $n = m_1 m_2$ )，

則  $f(m_1, n) = f(m_2, n)$

但  $f(m, n)$  的存在性，P.Glaister 並未說明，底下引理就是要證明它。

**[引理一]**

若將  $n$  張牌等分為  $m$  堆(其中  $n > m > 1$ )「向下洗牌」，則要回復到原來的次序所需的「向下洗牌」最少次數  $f(m, n)$  是存在的。

**[證明]：**

因為  $m|n$ ，令  $n = mt$ ，由  $mt - (n-1) = 1$  得  $(m, n-1) = 1$ ，則無窮數列  $m^1, m^2, m^3, \dots$ ，中的每一項，於模  $n-1$  中均不同餘於 0。由鴿籠原理知：存在正整數  $r > s$ ，使得  $m^r \equiv m^s \pmod{n-1}$ 。

因  $(m, n-1) = 1$ ，故  $m^{r-s} \equiv 1 \pmod{n-1}$ 。因為  $r-s$  滿足同餘方程式(\*)，因此，可以找到最小正整數  $k$  滿足同餘方程式(\*)，於是得證  $f(m, n)$  的存在性。

**[引理二]**

當將  $n$  張牌等分為  $m$  堆時(其中  $n > m > 1$ )，任何回復到原來的次序的「向下洗牌」次數都必定是「向下洗牌」的最少次數  $f(m, n)$  的倍數。

以數學語言寫出就是：設  $n > m > 1$  為整數， $m|n$ ， $f$  是大於 1 且滿足  $m^f \equiv 1 \pmod{n-1}$  的最小正整數。若正整數  $d$  滿足  $m^d \equiv 1 \pmod{n-1}$ ，則有  $f|d$ 。

**[證明]**

由[引理一]得知  $f(m, n)$  是存在的。另一方面洗牌的程序固定，因此當將  $n$  張牌等分為  $m$  堆時(其中  $n > m > 1$ )，任何回復到原來的次序的「向下洗牌」次數都必定是  $f(m, n)$  的倍數。

**[註解一]**其實[引理二]只是下列著名的數論定理的特例，但[引理二]的證明我們是用洗牌遊戲中的實際意義，非如一般數論書中的證明。

**[定理](證明見[2])**

設  $a, s$  為正整數， $s > 1$ ， $f$  是大於 1 且滿足  $a^f \equiv 1 \pmod{s}$  的最小正整數  $t$ 。若正整數  $d$  滿足  $a^d \equiv 1 \pmod{s}$ ，則有  $f|d$ 。

## 參、研究目的

### [性質(F)的定義]

將  $n$  張牌等分為  $m$  堆(其中  $n > m > 1$ )，若對於所有  $m$ (顯然  $m|n$ )，「向下洗牌」的最少次數  $f(m,n)$  都是定值，則稱  $n$  滿足性質(F)。

本文所要探討的問題就是：滿足性質(F)的  $n$ ，要具備什麼條件？

## 肆、研究設備及器材

筆，紙以及電腦。

## 伍、研究過程

$n$  的標準分解式很複雜，就我們目前所學，尚無能力對一般牌數  $n$  作完整討論。因此在本文中僅考慮牌數  $n=a^b$  及  $n=a^b+1$  兩種情形。考慮牌數  $n=a^b$  情形的原因是因為任意正整數均可寫成某些質數幕次的乘積，而顯然  $n=a^b$  是最簡單的情形；而考慮  $n=a^b+1$  情形的理由是我們的問題的本質是同餘方程式(參考刻畫方程式(\*))，因此為了數學處理的方便，我們也考慮牌數  $n=a^b+1$  的情形。

首先考慮牌數  $n=a^b(b>1)$  的情形。

### (一)、 $[n=a^b(b>1)]$

首先我們先考慮  $a$  為質數的情形，也就是  $n=p^b(p$  是質數)的情形，並注意到此時  $n$  的真因數只有  $p^r(1<r<b)$  的形式。

- (1).當  $b=2$  時，符合問題的  $n$  的分解式只有  $n=p \times p$ ，因此  $n$  只能等分成  $p$  堆，於是  $n$  顯然滿足所求。
- (2).當  $b=3$  時，符合問題的  $n$  的分解式只有  $n=p \times p^2 = p^2 \times p$ ，由 P.Glaister 教授的定理知， $n$  滿足性質(F)。(即無論我們將  $n=p^3$  的牌等分成  $p$  堆或  $p^2$  堆，要回復到原來的次序的「向下洗牌」的最少次數會都一樣)

因此在下面的定理中，我們只考慮  $b \geq 4$  的情形。

### [定理一]

- (1).若  $p, b$  為質數，則  $n=p^b$  滿足性質(F)且  $f(p^r, p^b)=b(1 \leq r < b)$ 。(即無論我們將牌等分成幾堆，要回復到原來的次序的「向下洗牌」的最少次數都是  $b$  次。
- (2).若  $b$  不為質數，則  $n$  不滿足性質(F)。(即若  $b$  不為質數，可將牌分成兩種不同的堆數，而回復到原來的次序的「向下洗牌」的最少次數不同)。

用數學語言寫出來就是：

存在  $1 < m_1 < m_2 < p^b$  且  $m_i | p^b (i=1,2)$ ，使得  $f(m_1, p^b) \neq f(m_2, p^b)$ 。

[證明]：

首先，我們證明不論  $p, b$  是否為質數， $f(p, n)$  均等於  $b(n=p^b)$ 。

由整數  $p^1, p^2, p^3, \dots, p^{b-1}$  均小於  $p^b-1$ ，可推得整數  $p^1, p^2, p^3, \dots, p^{b-1}$  對於模  $n-1$  均不同餘於 1。再由  $p^b \equiv 1 \pmod{n-1}$  可推得滿足  $p^k \equiv 1 \pmod{n-1}$  的最小正整數  $k$  是  $b$ ，於是  $f(p, p^b)=b$ 。

(1).若  $b$  為質數，則對所有  $1 < r < b$ ， $(p^r)^b \equiv (p^b)^r \equiv 1 \pmod{p^b-1}$

由[引理二]可知  $f(p^r, p^b) | b$ 。

再由  $b$  為質數，可推得對所有  $1 \leq r < b$ ，均有  $f(p^r, p^b) = b$

因此  $n = p^b$  滿足性質(F)。

(2).若  $b$  不為質數，則存在兩整數  $r, s > 1$  使得  $b = rs$ 。

則由  $(p^r)^s \equiv p^b \equiv 1 \pmod{p^b-1}$  以及[引理二]可知  $f(p^r, p^b) \leq s < b$

於是  $f(p^r, p^b) \neq b = f(p, p^b)$ 。因此  $n = p^b$  不滿足性質(F)。

### [推論一]

當  $a, b$  均不為質數時，則  $n = a^b$  不滿足性質(F)。(即若  $a, b$  均不為質數，可將牌分成兩種不同的堆數，則回復到原來的次序的「向下洗牌」的最少次數不同)。用數學語言寫出來就是：存在  $1 < m_1 < m_2 < a^b$  且  $m_i | a^b$  ( $i=1,2$ )，使得  $f(m_1, a^b) \neq f(m_2, a^b)$ 。

[證明]：由  $f(a, n) = b$ ，並利用與[定理一]第二部分完全一樣的證法。

接下來，我們考慮牌數  $n = a^b + 1$  的情形。

## (二)、 $[n = a^b + 1]$

這一小節，我們的目的是要討論牌數  $n = a^b + 1$  的情形。考慮這種情形的主要理由是為了便於處理刻畫方程式(\*)，然而即便是如此，這個問題仍是很難處理。因此我們換一個角度思考這個問題。若牌數  $n = a + 1$  與牌數  $n = a^b + 1$  均可以等分成  $q$  堆，從直觀上來看，將牌數  $n = a^b + 1$  的牌等分成  $q$  堆並作向下洗牌，則要回復到原來的次序的「向下洗牌」的最少次數  $f(q, a^b + 1)$  應該會隨著  $b$  的增加而增加，事實上，底下的[引理四]證明了  $f(q, a^b + 1)$  與  $f(q, a + 1)$  之間有著倍數關係(更進一步，如果  $a$  為質數，則底下的[定理三]計算出  $f(q, a^b + 1)$  與  $f(q, a + 1)$  的關係式)。由這項觀察，我們於[定理二]證明了牌數  $n = a^{kq^t} + 1$  的牌(其中  $k$  為奇數， $t$  為充分大的整數)不滿足性質(F)。也就是說：對任意足夠大的正整數  $t$  及正奇數  $k$ ，牌數  $n = a^{kq^t} + 1$  的牌可分成兩種不同的堆數，分別做向下洗牌，則回復到原來的次序的「向下洗牌」的最少次數不同。

### [引理三]

設  $a$  為正整數， $q$  為  $a + 1$  之真奇因數，則對任意非負整數  $t$ ，

$a^{q^t} \equiv -1 \pmod{q^{t+1}}$ ，特別地，對任意非負整數  $t$ ， $a^{q^t} + 1$  含有  $q^{t+1}$  的因數。

[註解二]這個引理主要是說明：當牌數  $n = a + 1$  的牌可等分成  $q$  堆時( $q$  為奇數)，則對任意非

負整數  $t$ ，牌數  $n = a^{q^t} + 1$  的牌可等分成  $q^{t+1}$  堆。

[證明]：利用數學歸納法

當  $t=0$  時，結論顯然為真。

假設當  $t=i$  時，結論是對的，即設  $a^{q^i}+1$  含有  $q^{i+1}$  的因數。

當  $t=i+1$  時，令  $x=a^{q^i}$ ，得  $a^{q^{i+1}}+1=x^q+1=(x+1)(x^{q-1}-x^{q-2}+\cdots-x+1)$

由歸納假設知  $a^{q^i}+1$  有  $q^{i+1}$  的因數。

因此  $q^{i+1} \mid (x+1)$ ，即得  $x \equiv -1 \pmod{q}$

再由  $q$  為奇數可得  $x^{q-1}-x^{q-2}+\cdots-x+1 \equiv 1+1+\cdots+1 \equiv q \equiv 0 \pmod{q}$

於是  $q \mid x^{q-1}-x^{q-2}+\cdots-x+1$ ，另一方面，由歸納假設知  $q^{i+1} \mid (x+1)$ ，因此， $q^{i+2} \mid x^q+1$ ，

也就是  $q^{i+2} \mid a^{q^{i+1}}+1$ 。

#### [引理四]

設  $a$  為正整數， $q$  為  $a+1$  之真奇因數，則

- (1). 對於任意的正整數  $b_2 > b_1$ ， $f(q, a^{b_1}+1) \mid f(q, a^{b_2}+1)$ 。(即若牌數  $a^{b_1}+1$ 、 $a^{b_2}+1$  的牌均可等分成  $q$  堆，並分別做向下洗牌，則要回復到原來的次序的「向下洗牌」的最少次數  $f(q, a^{b_1}+1)$ 、 $f(q, a^{b_2}+1)$ ，有  $f(q, a^{b_1}+1) \mid f(q, a^{b_2}+1)$  的關係)。
- (2). 存在大於 1 之正整數  $r \mid a$  以及  $s$ ，使得對任意正整數  $b \geq s$ ，都有  $rf(q, a+1) \mid f(q, a^b+1)$ 。(即存在大於 1 之正整數  $s$  及  $a$  的真因數  $r$ ，使得對任意正整數  $b \geq s$ ，若牌數  $a+1$ 、 $a^b+1$  的牌均可等分成  $q$  堆並分別做向下洗牌，則要回復到原來的次序的「向下洗牌」的最少次數  $f(q, a+1)$ 、 $f(q, a^b+1)$ ，有  $rf(q, a+1) \mid f(q, a^b+1)$  關係)。

[註解三] 當  $b$  為偶數時， $q$  未必是  $a^b+1$  的因數，但由  $(q, a^b) = (q, a) = 1$  及  $f(m, n)$  的刻劃方程(\*) 知，若將刻劃方程(\*) 視作同餘方程式，而不管  $f(q, a^b+1)$  的實際意義，則  $f(q, a^b+1)$  仍有數學意義，只是在洗牌的數學遊戲中，可能沒有實際的意義(因為  $q$  未必是  $a^b+1$  的因數，也就是牌數  $n=a^b+1$  的牌未必能等分成  $q$  堆)。

[證明]：

- (1). 設  $f(q, a^{b_2}+1)=z$ ，則由  $f(q, a^{b_2}+1)$  的定義知  $q^z \equiv 1 \pmod{a^{b_2}}$ ，又因為  $b_2 > b_1$ ，  
因此  $q^z \equiv 1 \pmod{a^{b_1}}$ ，

注意到  $f(q, a^{b_1}+1)$  是滿足此同餘方程式的最小正整數，由[引理二]，可得

$$f(q, a^{b_1}+1) \mid z, \text{ 也就是 } f(q, a^{b_1}+1) \mid f(q, a^{b_2}+1).$$

- (2). 由(1)知  $f(q, a^b+1)$  是  $b$  的遞增函數，由此我們首先證明：必存在最大正整數  $t$ ，使得對任意正整數  $1 \leq b \leq t$ ，有

$$f(q, a^b+1) = f(q, a+1), \text{ 且 } f(q, a^t+1) < f(q, a^{t+1}+1).$$

否則由(1)，對於任意的正整數  $b$ ，都有  $f(q, a^b+1) = f(q, a+1)$ 。

為方便起見，在此引理的證明中，我們均令  $f(q, a+1)=k$ 。

取一個充分大的正整數  $b_1$ ，使得  $a^{b_1} > q^k+1$ 。

則由整數  $q^1, q^2, q^3, \dots, q^k$  均小於  $a^{b_1}-1$ ，可推得整數  $q^1, q^2, q^3, \dots, q^k$  對於模  $a^{b_1}$  均不同餘於 1，  
因此，滿足同餘方程式  $q^y \equiv 1 \pmod{a^{b_1}}$ ，

的最小正整數  $f(q, a^{b_1}+1) > k$ ，此與  $f(q, a^{b_1}+1) = k$  矛盾。由此得證正整數  $t$  的存在性。

接著證明存在大於 1 的整數  $r$ ，使得  $f(q, a^{t+1}+1) = rf(q, a+1)$ 。

事實上根據  $q^{ka}-1=(x-1)(x^{a-1}+x^{a-2}+\cdots+x+1)$  (其中  $x=q^k$ )。

由本引理的第一部份、 $f(q, a^t+1)$  以及  $k$  的定義知： $q^k \equiv 1 \pmod{a^t}$ ，因此  $a^t | (x-1)$

於是  $(x^{a-1}+x^{a-2}+\cdots+x+1) \equiv 1+1+\cdots+1 \equiv a \equiv 0 \pmod{a}$

因此  $a | (x^{a-1}+x^{a-2}+\cdots+x+1)$ ，再由  $a^t | (x-1)$ ，可推得  $x^a \equiv 1 \pmod{a^{t+1}}$ ，

也就是  $q^{ka} \equiv 1 \pmod{a^{t+1}}$ 。

注意到  $f(q, a^{t+1}+1)$  是滿足此同餘方程式的最小正整數，再由[引理二]以及本引理的第一部份可知  $f(q, a^{t+1}+1) | ka$  及  $k | f(q, a^{t+1}+1)$ ，又由  $f(q, a^{t+1}+1) > f(q, a^t+1) = k$ ，因此存在大於 1 的整數  $r | a$ ，使得  $f(q, a^{t+1}+1) = kr$ 。令  $s=t+1$ ，由本引理的第一部份可得(2)的結論。

## [定理二]

對任意正整數  $a$ ，設  $q$  為  $a+1$  之真奇因數，則存在一正整數  $t_0$ ，使得對任意正整數  $t \geq t_0$  及正奇數  $k$ ， $n=a^{kq^t}+1$  不滿足性質(F)。(即存在一正整數  $t_0$ ，使得對任意正整數  $t \geq t_0$  及正奇數  $k$ ，將牌數  $n=a^{kq^t}+1$  的牌分成兩種不同的堆數，分別做向下洗牌，則回復到原來的次序的「向下洗牌」的最少次數不同。)用數學語言寫出來就是：存在  $1 < m_1 < m_2 < n$  且  $m_i | n (i=1,2)$ ，使得  $f(m_1, n) \neq f(m_2, n)$ 。

[證明]：

由[引理三]、[引理四]知，存在一充分大的正整數  $t_0$ ，使得對任意正整數  $t \geq t_0$ ， $a^{q^t}+1$  含有  $q^r$  的因數，且  $f(q, a^{q^t}+1)$  含有  $r$  的因子( $r$  的定義在[引理四]中)。因為  $k$  為正奇數，因此有下列的等式

$$x^k+1=(x+1)(x^{k-1}-x^{k-2}+\cdots-x+1), \text{ 其中 } x=a^{q^t}$$

由  $a^{q^t}+1$  含有  $q^r$  的因數，可知  $a^{kq^t}+1$  含有  $q^r$  的因數。因為  $f(q, a^{q^t}+1)$  含有  $r$  的因子，因此由[引理四]的第一部份知  $f(q, a^{kq^t}+1)$  含有  $r$  的因子。令  $y=f(q, a^{kq^t}+1)/r$ ，則  $y$  為正整數且由  $f(q, a^{kq^t}+1)$  的定義知  $(q^r)^y (\equiv q^{ry}) \equiv 1 \pmod{a^{kq^t}}$ ，

因  $f(q^r, a^{kq^t}+1)$  是滿足此同餘方程式的最小正整數，因此對任意正奇數  $k$ ，由[引理二]知  $f(q^r, a^{kq^t}+1)$  至多為  $y$ ，即  $f(q, a^{kq^t}+1)/r$ ，則  $f(q, a^{kq^t}+1) \neq f(q^r, a^{kq^t}+1)$ ，因此  $a^{kq^t}+1$  不滿足性質(F)。

下一個定理是用來計算：當  $p$  為大於 3 的質數， $q$  為  $p+1$  之真奇因數，且牌數  $n=p^b+1$  及牌數  $n=p+1$  的牌都可分成  $q$  堆時，則存在一正整數  $b_0$ ，使得當  $b \geq b_0$  時，將牌數  $n=p^b+1$  的牌作向下洗牌，則回復到原來的次序所需要的「向下洗牌」的最少次數  $f(q, p^b+1)$  是將牌數  $n=p+1$  的牌作向下洗牌，回復到原來的次序所需要的「向下洗牌」的最少次數  $f(q, p+1)$  的  $p^{b-b_0+1}$  倍；當  $b < b_0$  時，則  $f(q, p^b+1)=f(q, p+1)$ 。

## [定理三]

設  $p$  為大於 3 的質數， $q$  為  $p+1$  之真奇因數，則存在一正整數  $b_0$ ，使得(1).對任意正整數  $b_0 > b \geq 1$ ， $f(q, p^b+1)=f(q, p+1)$ 。

(2).對任意正整數  $b \geq b_0$ ， $f(q, p^b+1)=f(q, p+1) p^{b-b_0+1}$ 。

**[註解四]**當  $b$  為偶數,  $q$  未必是  $p^b+1$  的因數, 但由  $(q, p^b)=(q, p)=1$  及  $f(m, n)$  的刻畫方程(\*)知, 若將刻畫方程(\*)視作同餘方程式而不管  $f(q, p^b+1)$  的實際意義, 則  $f(q, p^b+1)$  仍有數學意義。只是在洗牌的數學遊戲中, 可能無實際意義(因  $q$  未必是  $p^b+1$  的因數)。

**[證明]** :

首先由[引理四]的第一部份可得  $f(q, p^b+1)$  是  $b$  的遞增函數。故一定存在最大正整數  $t$ , 使得對任意正整數  $1 \leq b \leq t$ , 均有

$$f(q, p^b+1)=f(q, p+1), \text{ 且 } f(q, p^t+1)<f(q, p^{t+1}+1)。$$

否則由(1), 對任意正整數  $b$ , 都有  $f(q, p^b+1)=f(q, p+1)$ 。

為方便起見, 在此引理的證明中, 我們均令  $f(q, p+1)=k$ 。取一個充分大的正整數  $b_1$ , 使得  $p^{b_1} > q^k+1$ 。

則由整數  $q^1, q^2, q^3, \dots, q^k$  均小於  $p^{b_1}-1$ , 可推得整數  $q^1, q^2, q^3, \dots, q^k$  對於模  $p^{b_1}$  均不同餘於 1, 因此, 滿足同餘方程式

$$q^x \equiv 1 \pmod{p^{b_1}},$$

的最小正整數  $f(q, p^{b_1}+1) > k$ , 此與  $f(q, p^{b_1}+1)=k$  矛盾, 因此得證正整數  $t$  的存在性。

接著我們用數學歸納法證明: 對任意正整數  $s$ ,  $f(q, p^{t+s}+1)=kp^s$ 。(如此再令  $b_0=t+1$  即可得證本定理)

當  $s=1$  時, 根據  $q^{kp}-1=(x-1)(x^{p-1}+x^{p-2}+\dots+x+1)$  (其中  $x=q^k$ )。

由  $f(q, p^t+1)=k$  的定義知  $p^t|(q^k-1)$ , 因此  $p|(x-1)$

於是  $x^{p-1}+x^{p-2}+\dots+x+1 \equiv 1+1+\dots+1 \equiv p \equiv 0 \pmod{p}$

所以,  $p|(x^{p-1}+x^{p-2}+\dots+x+1)$ , 再由  $p^t|(q^k-1)$ , 可推得

$$q^{kp} \equiv 1 \pmod{p^{t+1}}。$$

注意到  $f(q, p^{t+1}+1)$  是滿足此同餘方程式的最小正整數, 由[引理二]以及[引理四]的第一部份可知  $f(q, p^{t+1}+1)|kp$  及  $k|f(q, p^{t+1}+1)$ , 其中  $k=f(q, p+1)$ 。由  $p$  為質數及  $f(q, p^{t+1}+1) > f(q, p^t+1)=k$ , 因此  $f(q, p^{t+1}+1)=kp$ , 於是當  $s=1$  時, 結論成立。

設  $s=i$  時, 結論成立, 也就是  $f(q, p^{t+i}+1)=kp^i$  成立。

當  $s=i+1$  時, 令  $u=kp^i$ ,  $y=q^u$

根據  $q^{up}-1=(q^u)^p-1=(y-1)(y^{p-1}+y^{p-2}+\dots+y+1)$ 、 $u$  的假設及  $f(q, p^{t+i}+1)$  的定義知  $p^{t+i}|(q^u-1)$ 。

即得  $p|(y-1)$ ,

於是  $y^{p-1}+y^{p-2}+\dots+y+1 \equiv 1+1+\dots+1 \equiv p \equiv 0 \pmod{p}$

所以  $p|(y^{p-1}+y^{p-2}+\dots+y+1)$ , 再由  $p^{t+i}|(q^u-1)$ , 可推得

$$q^{up} \equiv 1 \pmod{p^{t+i+1}}。$$

注意到  $f(q, p^{t+i+1}+1)$  是滿足此同餘方程式的最小正整數, 因此由[引理二]及[引理四]的第一部份可知  $f(q, p^{t+i+1}+1)|up$  及  $u|f(q, p^{t+i+1}+1)$ , 其中  $u=f(q, p^{t+i}+1)$ 。再由  $p$  為質數, 得  $f(q, p^{t+i+1}+1)=u$  或是  $up$ 。

接下來說明  $f(q, p^{t+i+1}+1)$  不可能等於  $u$ 。若  $f(q, p^{t+i+1}+1)=u$ ,

由歸納假設知  $f(q, p^{t+i}+1)=u$ , 因此  $p^{t+i}|q^u-1$ ,  $p^{t+i}$  不整除  $q^{up}-1$  (注意到  $p|u$ ),

但是  $p|q^{up}-1$  (因為  $u/p=kp^{i-1}$  及  $f(q, p+1)=k$ )。

令  $z=q^{u/p}$ ，由  $p|q^{u/p}-1$ ，則存在一正整數  $c$ ，使得  $z=1+cp$ 。

由二項式定理知，對每一個  $p-1 \geq j \geq 1$ ，存在對應整數  $c_j$ ，使得  $z^j=1+j(cp)+c_jp^2$ 。

$$\begin{aligned} \text{因此 } z^{p-1} + z^{p-2} + \dots + z + 1 &= p + [(p-1) + \dots + 1](cp) + (c_{p-1} + c_{p-2} + \dots + c_1)p^2 \\ &= p + [(p-1)/2](cp^2) + (c_{p-1} + c_{p-2} + \dots + c_1)p^2 \\ &= p + Cp^2, \end{aligned}$$

其中  $C=[(p-1)/2]c+(c_{p-1}+c_{p-2}+\dots+c_1)$ 。

因此， $z^{p-1} + z^{p-2} + \dots + z + 1$  至多只能被  $p$  整除

再觀察等式  $q^u-1=(z-1)(z^{p-1}+z^{p-2}+\dots+z+1)=AB$ 。

由  $f(q, p^{t+i}+1)$  的定義知  $A$  至多只能被  $p^{t+i-1}$  整除，而由上面的討論知  $B$  至多只能被  $p$  整除，則  $q^u-1$  至多只能被  $p^{t+i}$  整除，卻不能被  $p^{t+i+1}$  整除，故  $f(q, p^{t+i+1}+1) \neq u$ ，此為矛盾。因此  $f(q, p^{t+i+1}+1)=up=f(q, p+1)p^{i+1}$ 。

## 陸、研究結果

首先我們回想一下  $n$  滿足性質(F)的意思：將  $n$  張牌等分為  $m$  堆(其中  $n>m>1$ )並作向下洗牌，若對於所有  $m$ (顯然  $m|n$ )，「向下洗牌」的最少次數  $f(m, n)$  都是定值，則稱  $n$  滿足性質(F)。

一、因此由[定理一]、[定理二]、[定理三]及[推論一]知。

- (1). 當牌數  $n=p^b$  ( $p, b$  為質數)，則  $n$  滿足性質(F)。而且若將牌等分成  $p^r$  ( $1 \leq r < b$ ) 堆，則將牌回復到原來的次序所需要的「向下洗牌」的最少次數為  $f(p^r, p^b)=b$  次。
- (2). 當牌數  $n=a^b$  ( $a$  未必是質數) 且  $b$  不為質數時，則  $n$  不滿足性質(F)。
- (3). 當牌數  $n=a^{kq^t}+1$  時(其中  $a$  為正整數， $q$  為  $a+1$  之真奇因數， $k$  為正奇數)，則存在

一正整數  $t_0$ ，使得對任意正整數  $t \geq t_0$ ， $a^{kq^t}+1$  不滿足性質(F)。

- (4). 當牌數  $n=p^b+1$  ( $b$  為奇數， $p$  為大於 3 的質數， $q$  為  $p+1$  之真奇因數) 則可等分成  $q$  堆，即  $q|(p^b+1)$ ，並存在正整數  $b_0$ ，使得當  $b \geq b_0$ ，將牌數  $n=p^b+1$  的牌回復到原來的次序所需的「向下洗牌」的最少次數  $f(q, p^b+1)$  是將牌數  $n=p+1$  時，回復到原來的次序所需的「向下洗牌」的最少次數  $f(q, p+1)$  的  $p^{b-b_0+1}$  倍，也就是
 
$$f(q, p^b+1)=f(q, p+1)p^{b-b_0+1}$$
 當  $b < b_0$  時，則  $f(q, p^b+1)=f(q, p+1)$ 。

## 二、有待繼續探討的問題

- (1). 當  $n=2^2p$  時，將牌等分成兩堆時所需的「向下洗牌」的最少次數  $f(2, 2^2p)$  為偶數，而當  $n=2^3p$  時( $p$  為質數)，則將牌等分成兩堆時所需的「向下洗牌」的最少次數  $f(2, 2^3p)$  為奇數。
- (2). 由利用電腦實驗觀察得知[定理三]中的  $b_0$  均等於 2(除了  $p=11$  之外)，也就是當  $p$  為大於 3 且不等於 11 的質數， $q$  為  $p+1$  之真奇因數，則  $f(q, p^b+1)=f(q, p+1)p^{b-1}$ 。

## 柒、參考資料

- [1].P. Glaister, Card Shuffling for Beginners, Mathematical -Spectrum 27 (1994), p5-7.  
[2].潘承洞等著, 初等數論, 凡異出版社 台灣, 1995.  
[3].洪維恩, Mathematica 3.0 版入門指引, 松岡出版社 1997.

## 捌、附錄

(一)、下列是用數學軟體 **Mathematica** 寫的程式, 目的是用來計算最少洗牌次數  $f(m,n)$ , 以及相關問題。

(1).

```
shuffletest[n_]:=Module[{d, s},  
  d=Divisors[n];  
  For[i=1;s=0, i≤Length[d]-2, i=i+1, s=s+(MultiplicativeOrder[d[[i+1]], n-1]-  
    MultiplicativeOrder[d[[2]], n-1]);  
  If[s2==0 && Length[Divisors[n]]>4, {n, MultiplicativeOrder[d[[2]], n-1}}, {}]  
]
```

[說明]shuffletest[n]是測試  $n$  是否滿足性質(F)。若滿足則輸出  $\{n, f(m,n)\}$ , 否則輸出  $\{\}$ 。

(2).

```
shuffle[n_]:=Complement[Table[shuffletest[i], {i, 2, n}], {}]
```

[說明]shuffle[n]是計算正整數 1 到  $n$  中, 有哪些正整數滿足性質(F)。

(3).

```
shufflenum[n_]:=Module[{d},  
  d=Divisors[n];  
  Table[{d[[k]], MultiplicativeOrder[d[[k]], n-1]}, {k, 2, Length[d]-1}  
]
```

[說明]shufflenum[n]是計算將牌數為  $n$ , 分成  $m$  堆時,  $f(m, n)$  的值。

(二)、文獻[1]的原稿如附件。