費馬小定理

許介彥

私立大葉大學 電機工程學系

壹、前言

我們在小時候都背過九九乘法表；以下是一個「六六乘法表」:

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	8	10	12
3	3	6	9	12	15	18
4	4	8	12	16	20	24
5	5	10	15	20	25	30
6	6	12	18	24	30	36

上表中的每個乘積除以 7 的餘數分別是：

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

上表具有一個有趣的性質：它的每一列（及每一行）都是 1, 2, 3, 4, 5, 6 這六數的一個排列;同一列中沒有任何兩數相同。

這個性質其實並不普遍；對任意一個大於 1 的正整數 n，如果我們先畫出一個 $(n-1)\times(n-1)$ 乘法表，然後將表中的每個數以該數除以 n 的餘數取代，所得的表的每一列未必都會是 1, 2, 3,..., $n-1$ 等數的一個排列，例如當 $n=6$ 時就不滿足上述性質：

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

如果您再多畫幾個表，多嘗試幾個不同的 n 值，您將發現滿足上述性質的 n 由小而大依序爲 $2,3,5,7,11,13,\ldots$；n 爲質數「似乎」是滿足上述性質的充要條件。

當 n 不是質數時我們不難理解上述性質爲什麼一定不滿足，因爲如果 $n=ab$ 且 a 與 b 皆大於 1，那麼表中第 a 列的第 b 個數將是 ab 除以 n 的餘數，也就是 0，而 0 並非 1, 2, 3,..., $n-1$ 等數之一。

下面我們說明當 n 爲質數時上述性質一定能滿足，即當 n 爲質數時，對任意一個小於 n 的正整數 a，表中第 a 列的 $a, 2a, 3a, \ldots, (n-1)a$ 等 $n-1$ 個數除以 n 的餘數一定會是 1, 2, 3,..., $n-1$ 等數的一個排列，也就是說，這些餘數一定全都不爲 0，而且其中不會有任何兩個餘數相等。

首先，由於 n 是質數，任意兩個小於 n 的正整數（一定都與 n 互質）的乘積不

可能是 n 的倍數，因此第 a 列的所有 $n-1$ 個餘數的確全都不會是 0。

接著我們利用歸謬證法來說明第 a 列的 $n-1$ 個餘數皆相異。假設有某兩個餘數相等：

$$sa \equiv ta \pmod{n}$$

其中 $1 \le s < t \le n-1$，經過移項可得

$$(t-s)a \equiv 0 \pmod{n}$$

即 $t-s$ 與 a 的乘積是 n 的倍數，但這顯然不可能，因爲 $t-s$ 和 a 都小於 n，都與 n 互質。

事實上，仿照上面的論述，您不難自行證明：對任意整數 n（$n>1$）及整數 a，只要 a 與 n 互質，$a, 2a, 3a, \ldots, (n-1)a$ 等數一定會與 $1, 2, 3, \ldots, n-1$ 等數對模 n 而言同餘（不考慮順序的話）。

貳、費馬小定理

當 p 是質數時，對任意與 p 互質的整數 a，由上面的討論我們知道 $a, 2a, 3a, \ldots, (p-1)a$ 等數一定會與 $1, 2, 3, \ldots, p-1$ 等數對模 p 而言同餘，因此 $a, 2a, 3a, \ldots, (p-1)a$ 等數的乘積一定會與 $1, 2, 3, \ldots, p-1$ 等數的乘積對模 p 同餘：

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

即

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

由於 $(p-1)!$ 與 p 互質，我們可將上式左右兩邊的 $(p-1)!$ 消去而得

$$a^{p-1} \equiv 1 \pmod{p}.$$

這是數學上有名的「費馬小定理」（Fermat's little theorem），因法國數學家 Pierre de Fermat（1601–1665）而得名。如果我們將上式的左右兩邊同時乘以 a 又可得

$$a^p \equiv a \pmod{p}.$$

這是費馬小定理的另一個常見的形式。請注意後面這個形式的費馬小定理對任意整數 a 皆成立（即使 a 是 p 的倍數仍成立）。

參、另一個證明

以下是費馬小定理的另一種證明方式。首先，我們用數學歸納法證明：當 p 爲質數時，對任意非負整數 a，a^p 與 a 對模 p 而言同餘。

當 $a=0$ 及 $a=1$ 時顯然成立，因爲 $0^p \equiv 0$ 且 $1^p \equiv 1$。假設當 a 爲某正整數時 a^p 與 a 對模 p 同餘，我們考慮 $(a+1)^p$ 是否與 $a+1$ 同餘。由二項式定理可知

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a^1 + 1$$

上式等號右邊除了頭尾兩項之外的每一項都是 p 的倍數（見參考資料[3]），因此對模 p 而言，

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

又由於我們假設 $a^p \equiv a$，所以由上式可得

$$(a+1)^p \equiv a+1 \pmod{p}$$

因此 $(a+1)^p$ 果然與 $a+1$ 同餘。數學歸納法的證明於焉完成。

我們接著考慮 a 爲負整數的情形。如果 p 等於 2，那麼 $a^p - a = a^2 - a = a(a-1)$ 顯然是 2 的倍數（因爲 a 與 $a-1$ 兩數中必有一數爲偶數），因此 a^2 與 a 對模 2 一定同餘。如果 p 不是 2，那麼 p 一定是奇數，

因此

$$a^p - a = -[(-a)^p - (-a)]$$

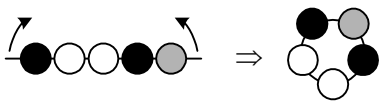
而我們已知 $(-a)^p - (-a)$ 是 p 的倍數（因爲 $(-a)$ 爲正整數），所以此時的 $a^p - a$ 也是 p 的倍數。綜合以上情形可知對任意質數 p 及任意整數 a， a^p 與 a 對模 p 而言一定同餘。

肆、有幾條項鍊？

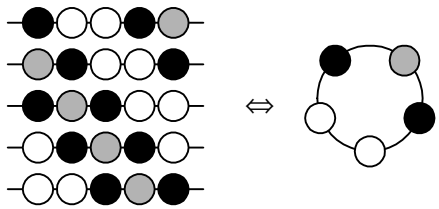
以下我們換個角度，從排列組合的觀點來說明費馬小定理爲什麼成立。假設我們有 a 種不同顏色的珠子，每種珠子各有無窮多顆；請考慮以下問題：從這些珠子中挑出顏色不全相同的 p 顆珠子來串成項鍊，總共可作出多少種不同的項鍊？我們假設這裡的 a 是正整數，p 是質數，而如果某串項鍊可經由另一串項鍊旋轉而得，我們將這兩串項鍊視爲同一種項鍊。

如果我們先只考慮將任意 p 顆珠子串成如下圖的一長條「珠串」，那麼作法顯然有 a^p 種，因爲每顆珠子的顏色都有 a 種選擇（下圖的 p 爲 5）：

每條珠串若依下面的方式將頭尾相接即對應到一條項鍊：



上述 a^p 條珠串中，整條鍊子的珠子全部同色的有 a 條，因此顏色不全相同的有 $a^p - a$ 條；但是這個數目還不是我們想要的答案，因爲我們要的是顏色不全相同的項鍊而非珠串，而 $a^p - a$ 條珠串中有許多珠串其實對應到相同的項鍊，例如下面五條珠串就都對應到同一條項鍊：



我們尚待解決的問題是：一條項鍊有可能在 $a^p - a$ 中被重覆算了幾次？以下我們將說明：每條項鍊都被算了不多不少正好 p 次，也就是如果我們將一條項鍊在不同的位置剪斷，所得的 p 條珠串必定全都不同。

採歸謬證法；假設某條項鍊可在某兩個不同的位置剪斷而得到兩條相同的珠串；如果這兩個剪斷的位置以反時鐘方向來看是隔著 d（ $d < p$ ）顆珠子，那麼將這條項鍊往反時鐘方向旋轉 d 個位置後所得的項鍊將會與原來的項鍊「重合」——每個位置的珠子的顏色都與旋轉之前相同。請留意由於 $d = 1$ 將意味著項鍊上所有的珠子同色，因此 d 的值一定大於 1。

既然這條項鍊旋轉 d 個位置後所得的項鍊與原來的項鍊重合，再旋轉 d 個位置後所得的項鍊還是會與原來的項鍊重合，依此類推，旋轉 $d, 2d, 3d, 4d, \ldots$ 個位置後所得的項鍊都將與原來的項鍊重合；如果

$$p = qd + r, \quad 0 < r < d$$

（因爲 p 爲質數所以 $r \neq 0$），那麼旋轉 qd 個位置後所得的項鍊一定與原來的項鍊重合；又由於旋轉 p 個位置後所得的項鍊也一定會與原來的項鍊重合（每顆珠子都繞

了一整圈），因此我們推知其實只須旋轉 $p-qd=r$ 個位置（$r<d$）就能讓所得的項鍊與原來的項鍊重合。依此類推，我們由 r 又一定能找到一個更小的正整數 r_1（$0<r_1<r$）使得旋轉 r_1 個位置後所得的項鍊與原來的項鍊重合，由 r_1 我們又一定能找到一個更小的 r_2，由 r_2 我們又一定能找到一個更小的 r_3……；由於介於 0 與 d 之間的整數個數有限，我們不可能可以無窮盡地找下去（無窮遞降），可見一開始的假設是錯的，因此對任意一條珠子顏色不全相同的項鍊，如果我們在不同的位置將項鍊剪斷，所得的珠串一定不同。

既然每條項鍊在 a^p-a 中都被算了正好 p 次，我們所求的項鍊個數因此就等於 $(a^p-a)/p$；此數既然是項鍊的「個數」當然一定是一個整數，因此 a^p-a 必定是 p 的倍數，也就是說，a^p 與 a 對模 p 而言一定同餘，這就說明了費馬小定理在 a 爲正整數時的情形。

伍、幾個應用

下面是費馬小定理的三個簡單的應用。

例題一：

求出 25^{8000} 除以 7 的餘數是多少。

由於 25 和 7 互質，由費馬小定理可知對模 7 而言，$25^6\equiv 1$，所以

$$25^{8000}\equiv 25^{6\times 1333+2}\equiv (25^6)^{1333}\cdot 25^2$$
$$\equiv 25^2\equiv 4^2\equiv 2$$

因此所求爲 2。

例題二：

假設 p 爲任意一個大於 5 的質數。試證：p 必可整除 $n_p=111\ldots1$（假設這是十進制中由 $p-1$ 個 1 構成的數）。

由於 p 和 10 互質而且 $9n_p=10^{p-1}-1$，由費馬小定理可知對模 p 而言，$10^{p-1}\equiv 1$，因此 p 一定能整除 $9n_p$。又由於 p 和 9 互質，因此 p 一定能整除 n_p。

例題三：

假設 $p=3k+2$ 是一個質數。試證：如果 p 可整除 a^2+ab+b^2（a 和 b 都是整數），那麼 a 和 b 必定都是 p 的倍數。

由於 p 可整除 a^2+ab+b^2，p 必定也能整除 $(a-b)(a^2+ab+b^2)=a^3-b^3$，因此

$$a^3\equiv b^3 \pmod{p}$$

左右兩邊同時取 k 次方，得

$$a^{3k}\equiv b^{3k} \pmod{p} \qquad (1)$$

假設 p 不能整除 a，那麼 p 必定也不能整除 b；由費馬小定理可知對模 p 而言，

$$a^{p-1}\equiv b^{p-1}\equiv 1$$

將 $p=3k+2$ 代入上式得

$$a^{3k+1}\equiv b^{3k+1} \qquad (2)$$

綜合(1)式與(2)式可知 $a\equiv b \pmod{p}$，因此 $a^2+ab+b^2\equiv a^2+a^2+a^2\equiv 3a^2$；既然 $3a^2$ 是 p 的倍數且 3 和 p 互質，可知 a 一定是 p 的倍數，這與我們假設的 p 不能整除 a 矛盾；因此 a 和 b 必定都是 p 的倍數。

陸、形如 4k+1 的質數個數

在本刊第 254 期「數不盡的質數」一文中，筆者曾經介紹如何證明形如 $3k+2$ 的質數與形如 $4k+3$ 的質數都各有無窮多個。以下我們證

明形如$4k+1$的質數也有無窮多個。

假設 n 是任意一個大於 1 的正整數；$n!$顯然爲偶數，因此 $(n!)^2+1$爲奇數，而 $(n!)^2+1$的每個質因數都可表爲 $4k-1$或 $4k+1$的形式。

假設 $p=4k-1$是 $(n!)^2+1$的一個質因數（可知 p 和 $n!$互質），由於

$$(n!)^2 \equiv -1 \pmod{p}$$

將左右兩邊同時取 $(p-1)/2$次方，得

$$(n!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}$$

由於 $(p-1)/2=2k-1$爲奇數，因此

$$(n!)^{p-1} \equiv -1 \pmod{p}$$

但這與費馬小定理牴觸，因爲根據費馬小定理，由於 p 和 $n!$互質，$(n!)^{p-1}$必定會和 1 對模 p 同餘。

由此我們推知 $(n!)^2+1$不可能有形如 $4k-1$的質因數，也就是 $(n!)^2+1$只有形如 $4k+1$的質因數。又由於 $(n!)^2+1$的每個質因數顯然都大於 n，因此我們證明了：不管 n 是多少，一定有比 n 大而且形如 $4k+1$的質數存在，這就說明了等差數列 $1,5,9,13,\ldots$中包含著無窮多個質數。

柒、費馬小定理的逆命題

當 p 爲質數，由費馬小定理我們知道 2^p-2必定是 p 的倍數（即前面的討論中當 $a=2$的情形）；反過來說成不成立呢？也就是說，如果有某個正整數 n 可以整除 2^n-2，我們能不能斷定 n 一定是質數呢？如果可以的話，這將是個不錯的判別任意整數 n 是否爲質數的方法；歷史上確實曾經有一段時期數學家們猜測這個方法是可行的，不過法國數學家 Pierre Sarrus 於西元 1819 年指出 $n=341$是一個反例；341 是 11 與 13 的乘積，因此不是質數，但是由

$$\begin{aligned} 2^{341}-2 &= 2[(2^{10})^{34}-1^{34}] = 2[(2^{10}-1)(\cdots)] \\ &= 2(1023)(\cdots) = 2(3)(341)(\cdots) \end{aligned}$$

可知 341 能整除 $2^{341}-2$。

對任意正整數 a，如果有某個大於 1 的正整數 n 本身不是質數卻能整除 a^n-a，我們稱 n 對底數 a 而言是一個「僞質數」（英文常稱作 a-pseudoprime）。因此對底數 2 而言，341 是一個僞質數（即 341 是一個 2-pseudoprime）。

幾個衍生出來的問題是：341 是唯一的 2-pseudoprime 嗎？除了奇數的僞質數外，是否還存在著「偶僞質數」？對任意正整數 a，a-pseudoprime 的個數是有限或是無限？

對底數 2 而言，如果 n 是一個奇僞質數，我們不難證明 2^n-1將是另一個更大的奇僞質數（見練習題 4）；既然我們已知奇僞質數 341 的存在，對底數 2 來說奇僞質數的個數因此是無窮的。尋找偶僞質數（對底數 2 而言）的工作比尋找奇僞質數要困難許多，其中最小的數直到西元 1950 年才由美國數學家 D. H. Lehmer 找到，其值爲 $161038=2\times73\times1103$。由於

$$2^{161038}-2=2(2^{161037}-1)$$

要說明 161038 可以整除 $2^{161038}-2$，我們只需說明 73 與 1103（此兩數皆爲質數）都能整除 $2^{161037}-1$即可。由於 161037 可經質

因數分解爲 $3^2\times29\times617$，因此

$$2^{161037}-1 = (2^9)^{29\times617}-1^{29\times617} = (2^9-1)(\cdots)$$
$$= (511)(\cdots) = 7(73)(\cdots)$$

可知 73 能整除 $2^{161037}-1$。又由於

$$2^{161037}-1 = (2^{29})^{9\times617}-1^{9\times617} = (2^{29}-1)(\cdots)$$
$$= (1103)(486737)(\cdots)$$

因此 1103 的確也能整除 $2^{161037}-1$。數學家 N. G. W. H. Beeger 於 1951 年證明了對底數 2 而言，偶僞質數的個數也是無窮的。

數學上還能證明：對任意正整數 a，以 a 爲底數的僞質數的個數都是無窮的。

捌、絕對的偽質數

2-pseudoprime 的個數是無窮的，3-pseudoprime 的個數也是無窮的；是否存在整數 n 使得 n 既是 2-pseudoprime 又是 3-pseudoprime 呢？答案是肯定的；令人訝異的是，我們甚至還能找到合數 n 使得不管 a 是多少，n 都能整除 a^n-a，也就是說，存在合數 n 使得 $2^n-2,\ 3^n-3, 4^n-4,\ldots$ 全都是 n 的倍數。這樣的 n 不僅存在而且還有不只一個，其中最小的是 $561=3\times11\times17$。由於

$$a^{561}-a = a(a^{560}-1) = a[(a^{10})^{56}-1^{56}]$$
$$= a[(a^{10}-1)(\cdots)] = (a^{11}-a)(\cdots)$$

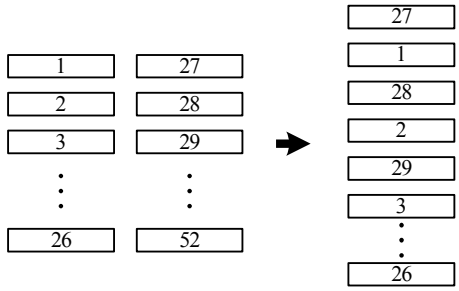
而由費馬小定理可知 $a^{11}-a$ 必定是 11 的倍數，因此 $a^{561}-a$ 也必定是 11 的倍數。經由類似的方法可推知 $a^{561}-a$ 也必定是 3 的倍數和 17 的倍數，因此不論 a 是多少，$a^{561}-a$ 必定是 561 的倍數。

如果不論 a 是多少，合數 n 都能整除 a^n-a（即 n 都是 a-pseudoprime），數學上稱 n 爲一個「絕對僞質數」（absolute pseudoprime），亦稱作 Carmichael number，因美國數學家 R. D. Carmichael 而得名；他在西元 1909 年首先注意到有這種數的存在，最小的十個依序爲 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341。Carmichael number 的總數到底是有限或是無限的問題曾經困擾了數學家許多年，直到 1994 年才被證明出來其個數是無窮的。

Carmichael numbers 在數線上的分布比質數稀疏許多，例如在所有小於一百萬的正整數中，總共有 78498 個質數，總共有 245 個 2-pseudoprime，但是總共只有 43 個 Carmichael number。

玖、需要洗幾次牌？

考慮以下動作：將一副撲克牌（52 張）由中間分成各含 26 張牌的兩小疊，然後洗牌使得這兩疊牌一張一張交錯，重新組合成 52 張牌。下圖顯示了洗牌前後位置的變化：



我們稱上述動作爲洗牌一次。請問：經過洗牌幾次後可使得每張牌都回到它最原始的位置？

由上圖洗牌前後的位置變化，我們看到原來在位置編號 $1,2,3,\ldots,26$ 的牌經過一次洗牌後將被放到編號 $2,4,6,\ldots,52$ 的位置，而原來編號 $27,28,29,\ldots,52$ 的牌則被放到了編號 1, 3, 5,…, 51 的位置，因此如果某張牌原來的位置爲 x，經過一次洗牌後的位置爲 y，那麼 y 與 x 的關係爲 $y \equiv 2x \pmod{53}$；因此這張牌經過 n 次洗牌後的位置必定與 $2^n x$ 對模 53 同餘，而我們的目標是希望能找到某個 n 使得對所有 $1 \le x \le 52$，

$$2^n x \equiv x \pmod{53}.$$

既然 x 與 53 互質（因爲 53 爲質數），我們可將上式左右兩邊的 x 約掉而得

$$2^n \equiv 1 \pmod{53}$$

由費馬小定理我們知道 $n = 52$ 一定滿足上式；事實上，52 是滿足上式最小的 n（我們在此不予證明）。因此經過 52 次洗牌後所有的牌必定都回到了原始的位置。

一般而言，如果一副牌有 m 張（m 爲偶數），而正整數 n 滿足

$$2^n \equiv 1 \pmod{m+1}$$

那麼經過上述方式洗牌 n 次後所有的牌必定都回到了原始的位置。

舉例來說，如果 $m = 62$，那麼我們只需洗牌 6 次即可，因爲 $2^6 \equiv 1 \pmod{63}$。

拾、質數的判定

費馬小定理的逆命題（converse）雖然不成立，不過僞質數與 Carmichael numbers 的數量在所有正整數中畢竟只占少數，因此如果 n 不是質數，對我們任意選擇的一個整數 a，a^{n-1} 與 1 對模 n 同餘的機率並不高。

我們在小學都學過如何判斷一個正整數 n 是否爲質數，只要測試介於 1 與 n 之間的整數是否有 n 的因數即可（事實上只須測試 $\lfloor \sqrt{n} \rfloor$ 個數即足夠）；但是當 n 很大時（例如當 n 是 200 位數），要判斷 n 是否爲質數的工作將變得相當困難。我們這裡所謂的「難」當然不是說完全沒有方法解決，而是很難在短時間內解決；然而質數的判定卻是某些領域裡常需面臨的問題，例如密碼學裡就有許多演算法在應用上需要由電腦隨機產生很大的質數，因此實際應用上很需要有較快的方法來判斷一個大整數是否爲質數。

當我們要判斷 n 是否爲質數，如果我們選擇幾個不同的 a 值（例如 $a = 2,3,5,7$），分別計算 a^{n-1} 除以 n 的餘數，結果發現所有的餘數都是 1，那麼 n 爲質數的機率其實相當高，而如果有任何一個餘數不是 1 我們立即可確定 n 不是質數。這個方式雖然不能保證通過測試的 n 一定是質數，但是在大部分情形下卻可以有效地將合數剔除，可以在判斷質數的過程中提供初步而快速的篩選，因此爲許多實際程式所採用。

拾壹、結語

費馬小定理最早出現於西元 1640 年 Fermat 寫給友人的一封信上，他在信中聲稱他知道如何證明這個定理，只是因爲信紙的空間太小了以至未能寫下其證明（這

是他出了名的「習慣」)。正式發表的證明要等到大約 100 年後才由數學家 Euler 於 1736 年提出，Euler 所用的方法是本文介紹的第二種證明方式（即利用二項式定理的方式)；不過由數學家 Leibniz 留下的未發表過的手稿顯示他應該早在 1683 年之前就已經用相同的方法證明出來了。

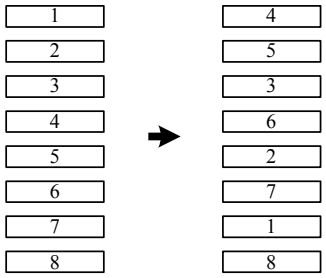
如果某個合數 n 滿足：「對任意整數 a，只要 a 與 n 互質，n 就一定能整除 $a^{n-1}-1$」，那麼 n 其實就是一個 Carmichael number；這是 Carmichael numbers（即絕對僞質數）的另一種常見的定義方式；兩種方式本質上並無不同。

既然有費馬小定理自然有費馬「大」定理（Fermat's great theorem)；費馬大定理也就是一般俗稱的費馬最後定理（Fermat's last theorem)。「小」與「大」只是在名稱上做區隔；就重要性而言，費馬小定理其實並不小，它所表達的關係不僅漂亮，在數學上更有相當廣泛的應用。

拾貳、練習題

以下是幾個與本文相關的問題，提供讀者參考。

1. 試說明當 p 爲質數且不等於 2 時，n^p-n 必定可被 $2p$ 整除。
2. 試證：對任意正整數 a 與 b，等差數列 $a, a+b, a+2b, \ldots$ 中必含有無窮多個合數。
3. 試證：對任意質數 p，2^p-1 的每個質因數都大於 p。
4. 試證：如果 n 對底數 2 而言是奇僞質數，那麼 2^n-1 必定也是一個奇僞質數。
5. 假設我們將手上的一疊撲克牌的最頂端與最底端的兩張牌抽出來放在桌上，再將剩下的牌的最頂端與最底端的兩張牌抽出來疊在桌上的兩張牌上面，並持續上述動作以完成一次洗牌。以 8 張牌爲例，洗牌前後的位置變化如下圖所示：



試證：如果一開始有 2^n 張牌，經過 $n+1$ 次洗牌後必可使得每張牌都回到它原始的位置。

6. 假設 p 爲質數且 a 與 p 互質。試證：如果 d 是滿足 $a^d \equiv 1 \pmod{p}$ 的最小正整數，那麼 d 一定是 $p-1$ 的因數。

參考資料

許介彥 (2002)，數不盡的質數，科學教育月刊，第254期。

許介彥 (2003)，同餘的基本概念，科學教育月刊，第261期。

許介彥 (2004)，巴斯卡三角形的幾個性質，科學教育月刊，第275期。

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford, 1979.