24 費馬小定理

24.1 費馬小定理

費馬小定理是初等數論上一個基本而且重要的定理。現在敘述而且證明如下：

定理 24.1(費馬小定理) 設 p 是質數，a 是與 p 互質的一個整數則

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

(2) 若 d 是使得 $a^d \equiv 1 \pmod{p}$ 成立的最小正整數，則

$$d \mid (p-1).$$

【証明】

(1) 因為 p 是質數，a 是與 p 互質的整數，所以模 p 之後的同餘數

$$1\cdot a, 2\cdot a, 3\cdot a, \cdots, (p-1)\cdot a \pmod{p}$$

是同餘數

$$1, 2, 3, \cdots, (p-1) \pmod{p}$$

的某種排列。因此我們有

$$\begin{aligned} &(1\cdot a)\cdot(2\cdot a)\cdots((p-1)\cdot a) \equiv 1\cdot 2\cdots(p-1) \pmod{p} \\ &\Rightarrow a^{p-1}\cdot 1\cdot 2\cdots(p-1) \equiv 1\cdot 2\cdots(p-1) \pmod{p} \\ &\Rightarrow (a^{p-1}-1)(1\cdot 2\cdots(p-1)) \equiv 0 \pmod{p}. \end{aligned}$$

因為 p 與 $1\cdot 2\cdots(p-1)$ 互質，所以

$$a^{p-1}-1 \equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

(2) 設 $p-1$ 被 d 除之，所得的商及餘數分別為 q 與 r。可以表為

$$p-1 = dq + r,\ 0 \le r < d.$$

由

$$\begin{cases} a^{p-1} \equiv 1 \pmod{p}, \\ a^{d} \equiv 1 \pmod{p}, \end{cases}$$

得到

$$a^r = a^r \cdot 1^q \equiv a^r \cdot (a^d)^q = a^{dq+r} = a^{p-1} \equiv 1 \pmod{p}.$$

因為 d 是最小的，所以必須有 $r = 0$，即 $d \mid (p-1)$。

（註）費馬小定理的(2)是習題 5.5 的特別情況，你注意到了嗎？

24.2 利用費馬小定理來因數分解大的正整數

費馬小定理的一個很重要的運用是利用它來因數分解很大的正整數。

例題 24.1　因數分解第四個費馬數

$$F_4 = 2^{2^4} + 1 = 65537.$$

【解】設質數 p 整除 F_4。我們有

$$\begin{aligned} p \mid 2^{16} + 1 \quad &\Rightarrow 2^{16} \equiv -1 \pmod{p} \\ &\Rightarrow 2^{32} \equiv 1 \pmod{p}. \end{aligned}$$

利用習題 5.5 的結果，容易推得 32 是滿足上式的最小正整數。由費馬小定理得到

$$32 \mid (p-1) \Rightarrow p \equiv 1 \pmod{32}.$$

令 $p = 32n + 1$ 則

n	1	2	3	4	5	6	7	8
p	33	65	97	129	161	193	225	257

因為 $33, 65, 129, 161, 225$ 不是質數，又 $97, 193$ 不能整除 65537 且

$$\sqrt{65537} < 257,$$

所以 $F_4 = 2^{2^4} + 1 = 65537$ 是一個質數。

例題 24.2　因數分解 $2^{13} - 1 = 8191$。

【解】設質數 p 整除8191。我們有

$$p \mid 2^{13}-1 \Rightarrow 2^{13} \equiv 1 \pmod{p}.$$

利用習題 5.5 的結果，容易推得13是滿足上式的最小正整數。由費馬小定理得到

$$\begin{cases} 13 \mid (p-1) \\ p \equiv 1 \pmod{2} \end{cases} \Rightarrow \begin{cases} p \equiv 1 \pmod{13} \\ p \equiv 1 \pmod{2} \end{cases} \Rightarrow p \equiv 1 \pmod{26}.$$

令 $p = 26n+1$ 則

n	1	2	3
p	27	53	79

因為 27 不是質數，又 53, 79 不能整除 8191 且 $\sqrt{8191} < 92$ ，所以 $2^{13}-1 = 8191$ 是一個質數。

24.3 其它運用

例題 24.3 設 p 為奇質數，a,b 為互質的整數且 $p \mid a^2+b^2$ 。證明

(1) 存在整數 n 使得 $p \mid 1+n^2$ 。

(2) $p \equiv 1 \pmod{4}$ 。

【解】

(1) 因為 a,b 為互質的整數，所以存在整數 x,y 使得 $ax-by=1$ 。利用恆等式

$$(a^2+b^2)(x^2+y^2) = (ax-by)^2 + (ay+bx)^2,$$

我們得到

$$p \mid (x^2+y^2)(a^2+b^2) = 1+n^2, \text{其中 } n = ay+bx.$$

(2) 由 $p \mid 1+n^2$ 得到 $n^2 \equiv -1 \pmod{p}$，推得 $n^4 \equiv 1 \pmod{p}$。利用習題 5.5 的結果，容易推得 4 是滿足此式的最小正整數。根據費馬小定理知道：

$$4 \mid (p-1) \Rightarrow p \equiv 1 \pmod{4}.$$

例題 24.4　設 m,n 為整數。證明

(1) $m^2-n^2,2mn$ 兩數中至少有一個為 3 的倍數。

(2) $m^2-n^2,2mn$ 兩數中至少有一個為 4 的倍數。

(3) $m^2-n^2,2mn,m^2+n^2$ 三數中至少有一個為 5 的倍數。

【解】

(1) 若 m,n 有一為 3 的倍數，則 $3\mid 2mn$，所以可假設 m,n 與 3 互質。根據費馬小定理知道：

$$\begin{aligned} m^2\equiv 1 \pmod 3, n^2\equiv 1 \pmod 3 &\Rightarrow m^2-n^2\equiv 0 \pmod 3 \\ &\Rightarrow 3\mid m^2-n^2. \end{aligned}$$

(2) 若 m,n 有一為 2 的倍數，則 $4\mid 2mn$,所以可假設 m,n 與 2 互質。因此知道：

$$\begin{aligned} m^2\equiv 1 \pmod 4, n^2\equiv 1 \pmod 4 &\Rightarrow m^2-n^2\equiv 0 \pmod 4 \\ &\Rightarrow 4\mid m^2-n^2. \end{aligned}$$

(3) 若 m,n 有一為 5 的倍數，則 $5\mid 2mn$，所以可假設 m,n 與 5 互質。根據費馬小定理知道

$$\begin{aligned} m^4\equiv 1 \pmod 5, n^4\equiv 1 \pmod 5 &\Rightarrow m^4-n^4\equiv 0 \pmod 5 \\ &\Rightarrow 5\mid m^4-n^4 \\ &\Rightarrow 5\mid m^2-n^2 \text{ 或 } 5\mid m^2+n^2. \end{aligned}$$

習題 24.1　因數分解 $2^{11}-1=2047$。

習題 24.2　因數分解 $2^{17}-1=131071$。

習題 24.3　證明 $2^{37}-1=137438953471$ 不是質數。

習題 24.4　是否存在滿足下列條件的正整數 n ：將集合

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

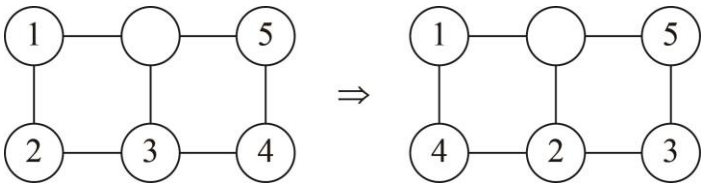
分成兩個不相交的非空子集合且第一個子集合的元素的乘積等於第二個子集合的元素的乘積。

習題 24.5　設 a, b, c 是三個整數，試證明

$$7 \mid abc(a^3 - b^3)(b^3 - c^3)(c^3 - a^3).$$

動手玩數學

將寫有 1,2,3,4,5 的五枚硬幣擺在左圖六格中的五格。規定每次移動僅能將空白格附近的硬幣沿著路徑滑動至空白格的位置。試問：是否可以將左圖經過有限次的滑動之後，變成右圖。



挑戰題

若 a 為整數，且 $x^2 - x + a$ 整除 $x^{13} + x + 90$ ，則求 a 的值。

費馬

費馬是法國數學家，生於 1601 年，死於 1665 年。最有名的“費馬最後猜想”終於在 1994 年被英國數學家威爾斯證明是正確的定理。費馬最後猜想的敘述是這樣的：方程式

$$x^n + y^n = z^n,$$

當$n>2$時沒有正整數解x,y,z。

事實上，費馬僅證明了$n=4$的情形，$n=4$的證明方法是很特殊的，今天我們稱此種方法為費馬無窮遞降法。關於$n=4$的證明，可以看本書的**定理 25.3**。

除了費馬最後猜想之外，費馬小定理，平方和，四個平方和的問題都是費馬在數論上很有名的工作。費馬曾經認為所有的費馬數

$$F_n = 2^{2^n}+1$$

都是質數。事實上這個猜想是錯誤的，例如

$$F_5 = 2^{2^5}+1 = 4294967297 = 641\times 6700417.$$

至於是否有無窮多個費馬數是質數是一個很難，而且至今仍未解的大難題。