35 質數問題

在 1 節中，我們對“質數有無窮多個”給了許多種不同的證明方法。事實上，除了 2 是偶質數之外，剩下的質數都是奇質數。因為奇數可以分為被 4 除之，餘數為 1 與 3 兩類，所以在兩類中，是否都有無窮多個質數是這裡要探討的重點。我們將質數依被 4 除之，所得的餘數做分類如下：

$$\text{質數}\begin{cases} 2, \\ \text{奇質數}\begin{cases} 3,7,11,\cdots & (\text{被 4 除之，餘數為} 3), \\ 5,13,17,\cdots & (\text{被 4 除之，餘數為} 1). \end{cases} \end{cases}$$

事實上，任一公差與首項互質的算術數列（等差數列）均包含有無窮多個質數。這是十九世紀很有名的狄利克雷定理。由於狄利克雷定理的證明很難，在此我們僅討論一些特殊的算術數列而已（如被 4 除之，餘數為 1 或 3，被 6 除之，餘數為 5 等算術數列）。底下是整數論常用有關因數，倍數的一個引理：設 d 為正整數，a,b 為整數且 $d \mid a, d \mid b$ 則

$$d \mid am+bn,$$

其中 m,n 為整數。

定理 35.1 證明：被 4 除之，餘數為 3 的質數有無窮多個。

【証明】假設被 4 除之，餘數為 3 的質數僅有有限個且恰為

$$p_1=3, p_2=7, p_3,\cdots, p_n$$

等 n 個質數。現在考慮正整數

$$N=4p_1p_2\cdots p_n-1.$$

因為 $N>1$ 且 $N\equiv 3 \pmod 4$，所以 N 可以寫成若干個奇質數的乘積且其中至少有一個被 4 除之，餘數為 3；即有一個質數 p_m $(1\le m\le n)$ 使得

$$p_m \mid N=4p_1p_2\cdots p_n-1, p_m \mid p_m \Rightarrow p_m \mid -1.$$

此與 $p_m > 1$ 矛盾。

定理 35.2　證明：被 4 除之，餘數為 1 的質數有無窮多個。

【証明】假設被 4 除之，餘數為 1 的質數僅有有限個且為

$$p_1 = 5, p_2 = 13, p_3, \cdots, p_n$$

n 個。現在考慮正整數

$$N = (2p_1p_2\cdots p_n)^2 + 1.$$

若 p 是 N 的一個質因數，則由

$$\begin{aligned} p \mid N &\Rightarrow (2p_1p_2\cdots p_n)^2 \equiv -1 \pmod p \\ &\Rightarrow (2p_1p_2\cdots p_n)^4 \equiv 1 \pmod p. \end{aligned}$$

因為 4 是滿足上式最小的正整數，由費馬小定理知道：

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

因此 $p = p_m (1 \le m \le n)$。由 $p_m \mid N$ 及 $p_m \mid p_m$ 得到 $p_m \mid 1$ ，矛盾。故被 4 除之，餘數為 1 的質數有無窮多個。

習題 35.1　證明：被 6 除之，餘數為 5 的質數有無窮多個。

習題 35.2　證明：被 8 除之，餘數為 1 的質數有無窮多個。

習題 35.3　設 n 為給定的正整數。證明：被 2^n 除之，餘數為 1 的質數有無窮多個。[18]

[18] 如果你已經會證明了，請仔細想想你的證明是否有瑕疵。

習題 35.4　是否存在整數 n 使得 $n^4 - 20n^2 + 4$ 為質數。

習題 35.5　設 n 為整數。若

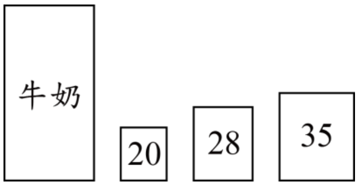
$$\left|n^3-6n^2+2n-12\right|$$

是一個質數或是兩個質數（可以相同）相乘的正整數，則 n 的值為何？[19]

[19] 試著因數分解此多項式並證明此多項式必為 3 的倍數。

動手玩數學

某人有一大桶的牛奶，但卻僅有 20 公升、28 公升及 35 公升的量杯各一個。請問應如何操作才能量得一公升的牛奶。



挑戰題

試證明

(1) 設 p 為奇質數且 x, y 為互質的整數。若 $p \mid x^2+y^2$ ，則證明

$$p \equiv 1 \pmod 4.$$

(2) 證明：被 8 除之，餘數為 5 的質數有無窮多個。[20]

[20] 令 $N=(5\cdot 13\cdot 29\cdots p_n)^2+2^2, N\equiv 5 \pmod 8$。證明：若質數 p 整除 N ，則 $p\equiv 1 \pmod 4$。

狄利克雷定理

如果a與b是互質的正整數，我們用符號$\pi(n;a,b)$表示不大於n且被a除之，餘數為b的質數個數。狄利克雷定理是說

$$\lim_{n\to\infty}\frac{\pi(n;a,b)}{\frac{n}{\left(\phi(a)\cdot\ln n\right)}}=1.$$

也就是說，當n很大時，不大於n且被a除之，餘數為b的質數個數大約為

$$\frac{n}{\phi(a)\cdot\ln n},$$

這裡的$\phi(a)$是指尤拉ϕ函數。