數論上的一些未解問題

（徵答對象：職業年齡不拘）

李恭晴

這些問題取自師大數學系李恭晴教授所著整數論的「附錄」中，用來給讀者增廣見聞。

——編者識

數論的發展已有幾千年的歷史，在這幾千年中，數學家曾經解出很多數學上的艱難問題，尤其最近兩三百年來，在數學上更有驚人的進展；然而，面對著數論上的一些「簡單」的問題時，數學家們卻一籌莫展，百思無解，令人有江郎才盡之感。在這裏我們將列出幾個較有名的數論上未解的問題，以供大家參考。

甲、質數分佈問題

我們知道在任意一個區間裏，可能有很多質數，也可能沒有，貝淵德（Bertrand）於一八四五年猜測，在 n 與 $2n$ 之間必有一質數 p 存在，這個猜測已經被蘇俄數學家契必雪夫（Tchebycheff）證明是正確的，一九三七年英格姆（Ingham）更進一步證明出有一常數 k 存在，使得當 $x \geq 1$ 時，在 x 與 $x+kx^{5/8}$ 之間必有一質數，**目前的問題是**：對於所有的 $x \geq 1$，能否找出一更小的區間，使得在此區間中，恒有一質數存在；例如對於每一自然數 n，是否恒有一質數介於 n^2 與 $(n+1)^2$ 之間？

乙、形如 n^2+1 之質數的個數

我們都知道，質數有無限多個，這些質數除了 2 之外，都是奇數，換句話說，它們都是在算術數列 $1,3,5,7,\cdots\cdots,2n+1,\cdots$ 中。至於在一般的無窮算術數列中，是否也有無限多個質數呢？狄利齊累（Dirichlet）曾肯定的答覆這個問題，他證明在每一個無窮算術數列中，只要首項與公差互質，就一定包含有無限多個質數，也就是說，若 a 與 d 互質，則具有 $a+nd$ 之形式的質數有無限多個，例如個位數字爲 1, 3, 7, 9 之質數各有無限多個，因爲它們分別具有 $1+10n$, $3+10n$, $7+10n$, $9+10n$ 之形式。根據狄利齊累所證明的，我們就知道它們中各有無限多個質數，且其個數數「幾乎」一樣多，**現在我們所不知道的是**：形如 n^2+1 或 $2n^2+1$ 之質數，是否也有無限多個？

丙、形如 n^2-n+p 之質數

我們很容易算出，當 $0\leq n\leq 16$ 時 n^2-n+17 一定是質數，同樣地，當 $0\leq n\leq 40$ 時 n^2-n+41 也都是質數，柏格爾更證明出，當 $0\leq n\leq 11000$ 時 $n^2-n+72491$ 恒爲質數；**那麼：是不是**對於每一自然數 N，都可以找到一個質數 p，使得當 $0\leq n\leq N$ 時，n^2-n+p 恒爲質數；如果能找得到，則 p 與 N 之大小關係如何？這也是一個有趣的問題。

丁、p_n-p_{n-1} 之分佈

我們知道，兩個連續質數之差，可能等於 2，也可能無限的大（見該書第 27 頁），換句話說，若以 p_n 表示第 n 個質數（依大小順序），則 p_n-p_{n-1} 是一個很不規則的數，遠超過我們的想像。比較規則點的一個數是

$$\max(p_2-p_1, p_3-p_2, \cdots\cdots, p_n-p_{n-1})$$

這個數如何隨 n 之增大而變動，也是一個值得探討的問題。

戊、費馬數

費馬（Fermat）猜測，所有形如 $2^{2^n}+1$ 之數，都是質數，我們很容易驗證當

$$n=0\text{時，}2^{2^n}+1=3$$
$$n=1\text{時，}2^{2^n}+1=5$$
$$n=2\text{時，}2^{2^n}+1=17$$
$$n=3\text{時，}2^{2^n}+1=257$$
$$n=4\text{時，}2^{2^n}+1=65537$$

都時質數，而相信費馬之猜測爲正確；然而，歐義拉（Euler）在一七三二年卻驗證出

$$2^{2^5}+1=4294967297=641\cdot 6700417$$

爲一合（成）數，推翻了費馬的猜測。事實上，除列上列五個費馬數是質數外，**到現在爲止，還沒有人能找出**其他任何一個費馬數是質數，也沒有人能證明其他的費馬數都不是質數。

雖然我們對於費馬質數所知有限，但我們可以輕易的證明任意兩個費馬數必互質，進而證明質數有無限多個。令 $F(n)=2^{2^n}+1$，並設 $m=n+k$，$k\geq 1$，則

$$F(m)-2=F(n+k)-2=2^{2^{n+k}}+1-2=(2^{2^n})^{2^k}-1$$

爲 $2^{2^n}+1$ 之倍數。

即

$$F(n)\,|\,F(m)-2$$

但因 $F(m)-2$ 與 $F(m)$ 爲連續的二奇數，故互質；所以知 $F(n)$ 與 $F(m)$ 互質。即任意兩個費馬數必互質。

由於費馬數有無限多個，且兩兩互質，可見必有無限多個質數，此爲歐幾里德定理之另一證明。

費馬數與正多邊形作圖問題有密切的關係，所謂正多邊形作圖問題是只利用圓規與直尺，是否可能作一正多邊的問題，這個問題又可能化簡爲正奇數邊形之作圖問題，高斯在十九歲時發現正奇數邊形可作圖的充要條件是其邊數爲一費馬質數或是數個費馬質數之乘積（同一質數在乘積中只能出現一次）因此，正七邊形、正九邊形、正十一邊形及正十三邊形等都不能作圖，而正三

邊形、正五邊形、正十七邊形、正二百五十七邊形及正十五邊形、正五十一邊形等都可利用圓規與直尺作出來，由於這個發現，才使得高斯下定決心做一個數學家，使得十九世紀的數學大放異彩，在他去世之後，哥廷根曾塑鑄了一尊銅像來紀念他，銅像的臺基是設計成正十七邊形的形狀，這實在是再恰當也沒有了。

己、費馬最後問題

費馬生前，喜歡在他看過的書上作批註，當他去逝之後，人們從他遺留下來的一本狄番圖(Diophantus)著的書中，找到如下的眉批:

「我有辦法證明當 $n\geq 3$ 時，$x^n+y^n=z^n$ 無正整數解，可惜證明太長，這裏寫不下。」

這就是有名的費馬最後問題。費馬是否能完整的證明這個問題，頗值懷疑，自從費馬以來，有很多數學家致力於這個問題的研究，德國皇家科學院也曾提供 100000 馬克獎勵最先證明出這個結果的人，可是**至今仍然沒有人能够證明它**，目前最好的結果是已經有人證明出

當 $3\leq n\leq 25000$ 時，$x^n+y^n=z^n$ 無正整數解，

至於當 $n>25000$ 時就無人知道了。

費馬最後問題也可改寫成:

當 $n\geq 3$ 時，$\frac{1}{x^n}+\frac{1}{y^n}=\frac{1}{z^n}$ 無正整數解。

因爲，若 $x^n+y^n=z^n$ 有正整數解 a,b,c，即 $a^n+b^n=c^n$，則

$$\frac{1}{(bc)^n}+\frac{1}{(ca)^n}=\frac{1}{(ab)^n}$$

故 bc,ca,ab 爲 $\frac{1}{x^n}+\frac{1}{y^n}=\frac{1}{z^n}$ 之一組正整數解。反之，若 a,b,c 爲 $\frac{1}{x^n}+\frac{1}{y^n}=\frac{1}{z^n}$ 之一組正整數解，則由 $\frac{1}{a^n}+\frac{1}{b^n}=\frac{1}{c^n}$

可得 $$(bc)^n+(ca)^n=(ab)^n$$

故 bc,ca,ab 爲 $x^n+y^n=z^n$ 之一組解。

我們注意到，在費馬最後問題中 $n\geq 3$，因爲

若 $n=1$，則 $x^n+y^n=z^n$ 顯然有無限多組解。

若 $n=2$，則可證明所有具有 $(u^2-v^2)r, 2uvr, (u^2+v^2)r$ 之正整數都是 $x^2+y^2=z^2$ 之解；反之，$x^2+y^2=z^2$ 之解，必爲上列形式之正整數。這種正整數組我們特別稱之爲畢氏三數組。根據畢氏定理，以畢氏三數組爲邊構成的三角形必爲直角三角形。

庚、梅仙涅質數

具有 2^p-1 之形式的質數，稱爲梅仙涅質數，例如

當 $p=2$ 時	$2^p-1=3$	爲質數
當 $p=3$ 時	$2^p-1=7$	〃
當 $p=5$ 時	$2^p-1=31$	〃
當 $p=7$ 時	$2^p-1=127$	〃
當 $p=11$ 時	$2^p-1=2047=23\times 89$	爲一合數
⋮	⋮	

一般而言，2^p-1 並不一定是質數，不過我們可以證明:

「若 a^n-1 爲質數，$n\geq 2$，$a>1$，則 $a=2$ 且 n 爲一質數。」

證明 因爲 $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots\cdots+1)$，而 $a^{n-1}+a^{n-2}+\cdots+1$ 顯然大於 1，故 $a-1=1$，即得 $a=2$，否則 a^n-1 即爲合數。

假設 n 不是質數，則可設 $n=rs$，其中 $1<r$，$s<n$

則 $2^n-1=2^{rs}-1=(2^r)^s-1=(2^r-1)(2^{r(s-1)}+2^{r(s-2)}+\cdots+2^r+1)$

等式右邊之每一因數都大於 1，故得 2^n-1 爲一合數，此與假設矛盾，故知 n 爲質數。

法國數學家梅仙涅 (Mersenne, 1588-1648) 在一六四四年列舉出對應於從 2 到 257 之質數 p 的梅仙涅質數 $M_p=2^p-1$，在他的表上共列了十七個，後來人們雖然發現其中有五個錯誤 (分別對應於 $p=61, 67, 89, 107$ 和 257)，但在當時，這已經是一個很了不起的成就。實際上，對應於 2 到 257 之質數的梅仙涅質數只有 12 個，它們是 $M_2=3$，$M_3=7$，$M_5=31$，$M_7=127$，$M_{13}=8191$，$M_{17}=131071$，$M_{19}=524287$，$M_{31}=2147483647$，M_{61}，M_{89}，M_{107}，M_{127}，這些數越來越大，計算也越來越困難，M_{31} 是歐義拉在一七五〇年算出的，在一百年後的一八七六年法國數學家魯卡斯 (Lucas) 又算至 M_{127}，這個數高達 39 位數字，已經是人類用紙筆所能算出的最大者，其後累瑪 (Lehmer) 和羅賓遜 (Robinson) 應用電子計算機在一九五二年又找出 5 個梅仙涅質數，它們是 M_{521}，M_{607}，M_{1279}，M_{2203}，M_{2281}，最近又找到了數個，最大的一個是 M_{19937} 居然高達 6002 位數字之多。是不是能再找到一個更大的的梅仙涅質數? 是不是有無限多個梅仙涅質數? **沒有人知道。**

辛、完全數

所謂完全數就是一個自然數，它的所有(正)因數之和爲其本身之兩倍；即滿足 $\Sigma_{d|n}\, d=2n$ 之自然數 n．例如 6 之因數的和爲 $1+2+3+6=12$，28之因數的和爲 $1+2+4+7+14+28=56$，所以 6 和 28 都是完全數，其他已知的完全數還有 496, 8128, 130816, 2096128, 33550336 等，我們注意到這些數都是偶數，對於偶完全數，我們知道得比較多，下面是偶完全數的特性:

「若 2^n-1 爲一質數，則 $a=2^{n-1}(2^n-1)$ 爲一完全數，且每一偶完全數都具有此形式.」

證明 若 2^n-1 爲質數，則由 $(2^{n-1}, 2^n-1)=1$ 可得

$$\sum_{d|a} d=\sum_{t|2^n-1} t\cdot\sum_{k|2^{n-1}} k=(1+2^n-1)(1+2+\cdots+2^{n-1})=2^n\cdot(2^n-1)=2a$$

故 a 爲一完全數。

反之，若 a 爲一偶完全數，則 a 可分解成 $a=2^{n-1}\cdot g$，$n>1$，g 爲正奇數

且 $2^n\cdot g=\sum_{d|a} d=\sum_{t|2^n-1} t\cdot\sum_{k|g} k=(1+2+\cdots+2^{n-1})\cdot\sum_{k|g} k=(2^n-1)\cdot\sum_{k|g} k$

故

$$\sum_{k|g} k=\frac{2^n g}{2^n-1}=g+\frac{g}{2^n-1}$$

因爲 $g/(2^n-1)=(\Sigma_{k|g}\, k)-g$ 爲一整數，故爲 g 之一眞因數 (不等於 g 本身之因數)

換句話說，$\Sigma_{k|g}\ k$ 等於 g 再加 g 之一眞因素，由 $\Sigma_{k|g}\ k$ 之定義知此眞因數必爲 1，且 g 爲質數。卽 $g=2^n-1$ 爲質數，而 $a=2^{n-1}(2^n-1)$。

由上列討論可知，若 2^n-1 爲一梅仙涅質數時，$a=2^{n-1}(2^n-1)$ 卽爲偶完全數，且偶完全數都具有這個性質，由於我們不知道是否有無限多個梅仙涅質數，所以也就不知道有沒有無限多個偶完全數；至於有沒有無限多個奇完全數呢？我不知道。數學家到現在甚至還找不到一個奇完全數，更不用說無限多個了，目前所知道的是：如果有奇完全數存在，則最少是一個 36 位數。由此可知，卽使有奇完全數存在，光是要把它找出來也比挖一顆鑽石還難。

如果 a 是一個完全數，則 $2a=\sum_{d|a} d=\sum_{d|a}\frac{a}{d}=a\sum_{d|a}\frac{1}{d}$

故得 $$\sum_{d|a}\frac{1}{d}=2 \quad 或 \quad \sum_{\substack{d|a\\ d\neq 1}}\frac{1}{d}=1$$

例如 $\sum_{\substack{d|6\\ d\neq 1}} d^{-1}=\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=1$，$\sum_{\substack{d|28\\ d\neq 1}} d^{-1}=\frac{1}{2}+\frac{1}{4}+\frac{1}{7}+\frac{1}{14}+\frac{1}{28}=1$

其中的分母，有些是偶數，有些是奇數，不過，如果 a 爲奇完全數則如此所得的分母，一定全都是奇數，因此

「奇完全數是否存在？」

這個問題就可化爲

「是否存在兩個以上的相異（正）奇數 $n_1,n_2,\cdots,n_r$ 使得

$$\frac{1}{n_1}+\frac{1}{n_2}+\cdots+\frac{1}{n_r}=1 \quad ?」$$

後一問題似乎較易解決，但如何解呢？

類似於完全數，我們可以考慮下一問題：

「是否存在有無限多個正數 $a>1$，使得 $\Pi_{d|a}\ d=a^2$ ？」

這個問題不像完全數那麼困擾我們，

因爲由 $\Pi_{d|a}\ d=\Pi_{d|a}\ (a/d)=(\Pi_{d|a}\ a)/(\Pi_{d|a}\ d)$ 可得

$$\Pi_{d|a}\ a=(\Pi_{d|a}\ d)^2=a^4$$

可以知 a 恰有四個因數。

卽 $a=p^3$ 或 $a=p_1p_2$，其中 p,p_1,p_2 爲質數，$p_1\neq p_2$。

壬、孿生質數

相差爲 2 之兩個質數稱爲孿生質數，例如 3,5；5,7；11,13；17,19；…,29,31；… 等都是，目前所知道的最大孿生質數是 1000000009649，1000000009651。一般猜測，孿生質數有無限多個，可是到現在仍無法證明。

克羅涅卡（Kronecker）更這一步猜測，任一偶數都可寫成兩個正質數之差，且其寫法有無限多種，如果他的猜測正確，則孿生質數就確實有無限多個。

一九二一年布倫（Brun）曾利用篩法（sienl method），證明小於 x 之孿生質數的個數，$T(x)\leq 100x/(10gx)^2$，現在仍有很多數學家試圖造出各種不同的數學篩子，以探討 $T(x)$ 之下界，他們猜測可能存在兩個正的常數 c_1，c_2 使得 $c_1x/(10gx)^2\leq T(x)\leq c_2x/(10gx)^2$，甚至於可

能找到一個常數 c，使得 $T(x)\sim cx/(10gx)^2$，果眞如此，則此問題卽可大白矣。

癸、哥德巴赫問題

這個問題是哥德巴赫(Goldbach，1690-1764)在一七四二年給歐義拉的一封信上所提出的。他觀察很多偶數，發現每一個都可分解成兩個質數之和（在當時，1被認爲是質數），他問歐義拉：「是否所有的偶數，確實都可分解成兩個質數之和？」這個問題歐義拉始終沒有回答他，其後雖然有很多著名的數學家對此問題感到興趣，可是到現在仍然沒有人能證明出這個問題爲眞，也沒有人能夠找出一個不能分解成兩個質數之和的偶數。

哥德巴赫問題，用現在的說法（1不是質數），就是:

「所有≥ 6之偶數皆可分解成兩個奇質數之和。」

一旦這個猜測被證明成立，則

「任何≥ 9之奇數n必可分解成三個奇質數之和。」

因爲 $n-3\geq 6$，且爲偶數，故 $n-3=p_1+p_2$，卽 $n=3+p_1+p_2$，其中 p_1,p_2 爲奇質數。

數學家雖然還不能證明哥德巴赫的問題，但是目前有很多研究，已經使此問題顯露端倪:

(1) 在一九三一年蘇俄數學家希尼曼（Schnirelmann，1905-1938）證明出所有的正數均可分解爲不多於 300000 個質數之和，這個成就與哥德巴赫原先的問題似乎有天壤之別，但是它已邁出了解哥德巴赫問題的第一步，也指示我們一個研究的方向。

(2) 在一九三七年，蘇俄數學家維諾格拉夫（Vinogradoff，1891- ）成功的證明出所有足夠大的奇數，都可分解成三個奇質數之和，也就是說：存在一常數 N，使得奇數 $n\geq N$ 時，n 可分解成三個奇質數之和，如果我們能夠驗算出所有小於 N 之奇數也能分解成三個奇質數之和，則哥德巴赫問題中之奇數部份卽可解決，可惜維諾格拉多夫所算出的這個數 N 是太大了，卽使我們用電子計算機也無法驗算出所有小於 N 之奇數是否都可分解成三個奇質數之和。目前利用電子計算機只算至 $n\leq 100000$ 之情形。

(3) 布倫利用篩法在一九一九年證明出每一個正偶數n皆可寫成二個正奇數之和: $n=q_1+q_2$，其中 q_1,q_2 最多是9個質數之積，最近又被改進成4個質數之積。

(4) 華羅庚曾證明「幾乎」所有的偶數都可分解成兩個奇質數之和，「幾乎」的意思是：不能分解成兩個奇質數之和的偶數的個數與能分解的偶數之個數的比非常小，但是並不排除:

「有無限多個偶數不能分解成兩個奇質數之和」

的可能性。

(5) 匈牙利數學家雷尼（Renyi）證明出每一個大於2的偶數，都可分解成一個質數與一個合數之和，且合數的質數不超過某一定值。