完全數與梅仙尼質數

黃文璋

1. 完全數

由自然數 (又稱正整數)、整數、有理數、實數至複數, 數學中所討論的問題往往與數有關。而其中數字的諸多優美及特異的性質, 一直吸引著許多職業及業餘數學家去探討。這探討可歸於數學中的整數論, 或者說數論的問題。數論起源甚早, 與幾何學的發展相當, 但數論的題材似乎是取之不盡的, 影響也較深遠。數論中的優美及豐富的內容, 不知傾倒多少數學家, 許多中學生著迷數學, 也往往是喜歡數論。數學家 Gauss(高斯, 1777-1855, 有史以來三大數學家之一。另兩位爲 Archimedes(阿基米德, 西元前287-212年) 及 Newton(牛頓, 1642-1727)) 曾說“數學是科學的皇后, 而數論是數學的皇后 (Mathematics is the queen of the sciences and the theory of numbers is the queen of mathematics)”。至於 Gauss 則被稱爲數學王子。數論中的有些結果, 後來發現有其實際的用途。如同餘數及質數的分解, 可用在編碼及解碼上。不過大部分的時候, 去探討數論中的問題, 只是數學家純粹覺得有趣, 追求心智上的滿足。本質上十個阿拉伯數字$0, 1, \cdots, 9$所衍生出的問題, 與音樂中七個音階所組合出的各種曲調, 都能帶給人們在不同方面的喜樂。古希臘時代, Pythagoras(畢達哥拉斯, 約西元前580-500年) 門生極多, 稱爲畢氏學派 (the Pythagorean school), 他們研究的範疇主要爲幾何、算術、天文及音樂, 而這些研究均以數字爲其基礎。古希臘的大哲學家 Aristotle(亞里斯多德, 西元前384-322年) 曾說“Pythagoras 認爲宇宙是由音階和數相輔相成”。

愛看武俠小說的人, 對金庸在其武俠小說中, 將數字運用的極爲熟練應留下深刻印象。例如, 在射雕英雄傳 (金庸 (1984)) 第二十九回“黑沼隱女”中, 隱居中的瑛姑何以排除孤寂? 乃是在解各種數學問題, 如求55,225的平方根, 求34,012,224的立方根, 求3×3的魔方陣之解等。

英國大數學家 Hardy (1887-1947), 曾藉下述故事 (見 Hill(1987/88)), 來說明印度的傳奇數學家 Ramanujan (1887-1920, 其部分事蹟可見曹亮吉 (1984) 不

按牌理出牌一文), 能以各種難以想像的方式來記住各個數字。當 Ramanujan 因病在 Putney 休養時, 在西元1919年1月, 有一次 Hardy 乘坐計程車去看他, 車牌號碼爲 1729。Hardy覺得這是一個沒什麼特性的數字。Ramanujan 馬上說“恰恰相反, 這是一個很有趣的數字, 它是能以兩種不同的方式, 表示成二整數的立方和的最小正數”。讀者能試將此兩種表示法寫出嗎?Hardy 接著又問 Ramanujan 是否知道四次方和的對應解? Ramanujan想了一下回答說“我給不出答案, 但此最小正整數若存在一定是很大的”。日後 Hardy 在傳述此故事時, 指出瑞士數學家 Euler(歐拉, 1707-1783) 曾給出此數爲$158^4+59^4=134^4+133^4$。此數當然是很大的, 所以不能怪 Ramanujan 一時想不出。Hardy 的長期合作者, 也是英國大數家 Littlewood (1885-1977) 曾說過“每一正整數皆爲 Ramanujan 的密友”。

古希臘時, 有些數字令人覺得具有特別的象徵及神秘的意義。例如, 畢氏學派在一些數字中, 看到一完美的性質: 這些數等於小於它的所有因數 (即眞因數) 之和。他們稱這種數爲完全數 (perfect number, 事實上稱呼完美數也許較恰當, 不過約定俗成, 我們仍採用完全數)。6是第一個完全數6=1+2+3。6也確實與宗教裡的一些完美性相關連。在西方聖經裡記載, 上帝在六天內創造了世界, 因此古代人認爲6是一個很完美的數字。中國人說六六大順, 顯然對6也有偏好。28是第二個完全數, 28=1+2+4+7+14。婦女擔負著傳宗接代的神聖使命, 月經爲其間的樞紐, 而月經之每周期約28天, 這是巧合或有意的?

Euclid(歐幾里得, 約在西元前375-330年) 寫過原本 (Elements), 也被稱爲幾何原本, 後來成爲中學幾何學的基礎 (九章出版社有出譯本)。在原本的第九卷, 亦爲討論算術的第三卷也是最後一卷, 此卷除包含質數有無限多個的證明, 其最後一命題 (命題36), 即爲完全數的討論。古希臘哲學家 Plato(柏拉圖, 約西元前428-347年) 在其所著共和國 (Republic) 一書中, 也提到完全數。

古希臘時代只知道四個完全數, 在原本第九卷的最後一句話寫著“6, 28, 496, 8, 128 等皆是完全數”。Euclid發現 (只有希臘神才知道他怎麼發現的), 這四個完全數皆可表示爲$2^{n-1}(2^n-1)$的型式, n分別爲$2, 3, 5, 7$:

$$n=2,\ 2^1(2^2-1)=2\cdot 3=6,$$
$$n=3,\ 2^2(2^3-1)=4\cdot 7=28,$$
$$n=5,\ 2^4(2^5-1)=16\cdot 31=496,$$
$$n=7,\ 2^6(2^7-1)=64\cdot 127=8,128。$$

Euclid也看出當$n=2,3,5,7$時, 2^n-1皆爲質數 (一大於1之整數, 若除了1與本身外無其他因數, 便稱爲質數 (prime number 或 prime) 否則稱 爲合成數 (composite number))。這項觀察使他在原本裡, 證明了下述定理。

定理 1: 若2^n-1爲一質數, 則$2^{n-1}\cdot(2^n-1)$爲一完全數。

證明: 設$p=2^n-1$ 爲一質數, 則$2^{n-1}(2^n-1)=2^{n-1}p$ 之因數有$1,2,2^2,\cdots,2^{n-1}$,

$p, 2p, 2^2p, \cdots, 2^{n-1}p$。因此$2^{n-1}(2^n-1)$ 之所有眞因數之和爲

$$\begin{aligned} &1 +2+2^2+\cdots+2^{n-1}+p+2p \\ &\quad +2^2p+\cdots+2^{n-2}p \\ &=2^n-1+p(2^{n-1}-1) \\ &=p+p(2^{n-1}-1)=2^{n-1}p \\ &=2^{n-1}(2^n-1)。\end{aligned}$$

證畢。

我們又有下述定理。

定理2: 對每一正整數n, 若2^n-1爲一質數, 則n爲質數。

證明: 設n不爲質數, 令$n=pq, p>1, q>1$。則

$$\begin{aligned} 2^n-1&=(2^q)^p-1 \\ &=(2^q-1)((2^q)^{p-1}+(2^q)^{p-2} \\ &\quad +\cdots+2^q+1) \\ &=A\cdot B。\end{aligned}$$

因 $p>1$ 且 $q>1$, 故 A, B 皆大於1, 因此 2^n-1 不爲質數, 與假設不合。故得證 n 爲質數。

由上定理立即可看出爲何首四個完全數對應的$n=2,3,5,7$皆爲質數。試看 $n=4$, 則$2^{4-1}(2^4-1)=120$。而120的眞因數和爲$1+2+3+4+5+6+8+10+12+15+20+30+40+60=216\neq 120$, 故120不爲一完全數。

首四個完全數分別爲一位數、二位數、三位數及四位數。讀者是否猜測第五個完全數爲五位數? 結果是不對的。又定理2之逆不眞, 因第五個質數爲11, 但在西元1536年 Regius 證明$2^{11}-1$ =2,047= $23\cdot 89$並不爲質數。事實上$2^{10}(2^{11}-1)$ =2,096,128的確不是一個完全數。但定理1並未指出當2^n-1不爲質數時, $2^{n-1}(2^n-1)$是否爲一完全數, 此問題我們稍後再回答。古希臘人亦看出, 首四個完全數, 其個位數爲6, 8交替 (約在西元前一世紀, Nicomachus 在其著作中雖也只列出首四個完全數, 但他指出偶完全數的個位數不是6就是8。且當個位數爲6時, 十位數必爲奇數, 當個位數爲8時, 十位數必爲2)。後來證實第五個完全數的個位數的確是6, 不過第六個完全數的字尾仍爲6, 這便打破了6, 8交替的型式。不過已知的完全數, 其個位數皆爲6或8。

定理1給出了找偶完全數的充分條件, 但是否尚有其他偶完全數呢?Euclid 之後約兩千年, Euler在一篇他去世後才發表的論文中, 給出了下述找偶完全數的必要條件, 至此偶完全數的型式便完全決定了。

定理3: 偶完全數必呈$2^{n-1}(2^n-1)$的型式, 其中n爲一正整數, 且2^n-1爲一質數。

證明: 設A爲一偶完全數, 則A可表示爲$A=2^{n-1}p$, 其中$n\geq 2$爲一整數, p爲一奇數。則A的所有因數和爲 (證明留在習題)

$$\begin{aligned} 2s(A)&=(2^{n-1}\text{的所有因數和}) \\ &\quad\cdot(p\text{的所有因數和}) \\ &=(2^n-1)(s(p)+p), \qquad (1)\end{aligned}$$

其中 $s(A)$ 及 $s(p)$ 分別表 A 及 p 之所有眞因數之和。因 A 爲一完全數, 故 $s(A)=A$,

即

$$(2^n-1)(s(p)+p)=2A=2^np。$$

由此即得

$$p=(2^n-1)s(p)。\qquad (2)$$

由上式知 $s(p)$ 爲一 p 的因數 (以 $s(p)|p$ 表之)。又 $2^n-1>1$, 故 $s(p)$ 爲一 p 的眞因數。但 $s(p)$ 爲 p 之所有眞因數之和, 由此便得 $s(p)=1$。而 $s(p)=1$ 又導出 p 爲一質數。故由 (2) 知, $p=2^n-1$ 爲一質數。證畢。

第五個完全數, 是在西元1461年左右, 於一份前人留下的文稿中發現的, 其位數達到八位, 即33,550,336。第六個質數爲13, 由定理3知, 欲檢驗$2^{12}(2^{13}-1)=33{,}550{,}336$是否爲一完全數, 只須檢驗$2^{13}-1=8{,}191$是否爲一質數。在初等數論中, 有下二關於質數的檢驗定理。

定理4: 每一大於1之整數必有一質因數。

定理5: 若整數A爲一合成數, 則A必有小於或等於 $\sqrt{A}$ 之質因數。

但即使有上二定理, 在那計算不發達的時代, 檢驗質數仍是一件艱辛的工作。由於$\sqrt{8{,}191}=90.5\cdots$, 必須驗證24個小於91的質數是否能除盡8,191。早期數學家可能沒有去嘗試。在西元1588年, 針對13的下兩個質數17及19, 義大利數學家Cataldi(1548-1626)證明$2^{17}-1=131{,}071$及$2^{19}-1=524{,}287$ 皆爲質數。因$724<\sqrt{2^{19}-1}<725$, 欲檢驗$2^{19}-1$爲一質數, 他先建立一小於725之質數表。然後證明其中總共的128個質數皆無法除盡$2^{19}-1$。這是一不小的工程。他也因此得到第六個完全數$2^{16}(2^{17}-1)=8{,}589{,}869{,}056$, 及第七個$2^{18}(2^{19}-1)=137{,}438{,}691{,}328$。他亦宣稱當$n=23,29,31$及37(19的下四個質數)時, 2^n-1皆爲質數。在西元1640年, 法國大數學家 Fermat(費馬, 1601-1655, 他是一位職業律師, 但在現代數論中, 扮演著極重要的角色) 證明$n=23$及37時, 2^n-1皆非質數。Euler 在西元1738年證明 Cataldi 對$n=29$亦犯了錯。不過後來在西元1772年 (一說1750年),Euler 證明$2^{31}-1$確爲質數, 因而得到第八個完全數。距上一個完全數之發現已近兩百年。

有了定理3, 決定偶完全數, 本來成爲了決定2^n-1是否爲質數的問題。但由於計算工作愈來愈大, 即使願做如 Cataldi 的苦工, 也不可行了。除非有更好的檢驗質數的方法, 否則雖知道該如何去找完全數, 但卻不易產生新的完全數。十七世紀法國數學家 Descartes(笛卡兒, 1596-1650) 曾預言: 能找出的完全數是不會太多的, 好比要在人類中找到完人 (perfect man), 亦非易事。

2. 梅仙尼質數

在 Cataldi 之後, 下一階段尋找完全數工作的重心, 便轉移到法國。找偶完全數與檢驗2^n-1是否爲一質數, 是等價的。

型如 2^n-1 的質數 (n 當然須爲一質數), 最早以 Descartes 的好朋友, 法國神

父 Mersenne(梅仙尼, 1588-1647) 最有興趣, 故後來對一質數p, 便稱$M_p = 2^p - 1$爲一梅仙尼數 (Mersenne number), 且當M_p爲質數時, 稱此爲一梅仙尼質數 (Mersenne prime)。

Mersenne經常與那時的法國著名的數學家通信, 討論的問題包含完全數及型如 M_p 的質數。但爲何這種質數以他的名字命名, 則不是很清楚。因他並未得到任何顯著的結果, 而只做了一個有名的斷言。不過那時的數學家倒是常受到 Mersenne 的鼓舞, 而去研究他所提出的問題。

Mersenne在西元1644年說: 若p爲一不超過257的質數, 則當p =2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257時, $2^p - 1$爲質數, 否則爲合成數。

對$p \leq 257$ 之梅仙尼數M_p,Mersenne 已去掉許多不爲質數的M_p, 如M_{23}, M_{29}等。但他仍犯了一些錯: 多列了兩個, 即$p = 67, 257$, 少列了3個, 即$p = 61, 89, 107$。此因如前所述, 當p大時, 欲檢驗M_p是否爲質數, 便很困難。所以 Mersenne 留給後世此一以他名字命名的他在質數方面唯一的斷言也是錯的。正確地說, 在2到257間共有12個梅仙尼質數, 其對應的p 值爲

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127。$$

這就是人們只用紙筆所得的全部十二個梅仙尼質數。雖然Mersenne 在其宣稱中犯了錯, 但在沒有電子計算機的幫助下, 而當p大時, M_p又是極巨大, 能有此成果, 已是很驚人的成績了 (換一個觀點來看, 在2到257間共有55個質數, 若對每一個其間的質數p, 皆問M_p是否爲質數, Mersenne說對了50個)。一直要到西元1947年, 對$p \leq 257$時, M_p爲質數的名單才完全確定。

雖對首四個質數$p = 2, 3, 5, 7$, M_p皆爲質數, 但由在257之前共有55個質數, 卻只產生12個梅仙尼質數, 你大約可以猜出許多梅仙尼數並非質數。事實上底下我們會看到梅仙尼質數之稀少, 遠超出我們的想像, 且當p愈大,M_p愈不易爲質數。

由定理5知, 欲檢驗A是否爲一質數, 只要用不超過$\sqrt{A}$的質數去除A 即可。但即使如此, 當p很大時, 便需要做許多次除法, 並不易檢驗出M_p是否爲一質數。於是又有下述定理。

定理6: 設p爲一質數, 則M_p的質因數必爲$ap + 1$的型式, 其中a爲一正整數。

證明: 設$M_p = 2^p - 1$有一質因數$\ell = ap+b$, 其中$1 \leq b \leq p-1$, a爲一正整數。在此由 Fermat 小定理 (Fermat's Little Theorem, 即對任一質數q及正整數m, $q|(m^q - m)$) 知, $p \nmid (2^p - 1)$,故$b \neq 0$。因$\ell|(2^p - 1)$, 故

$$\begin{aligned} 2^{\ell-1} - 2^{b-1} &= 2^{ap+b-1} - 2^{b-1} \\ &= 2^{b-1}((2^p)^a - 1) \qquad (3) \end{aligned}$$

爲ℓ之整數倍。因$\ell \neq 2$, Fermat 小定理又導出$\ell|(2^{\ell-1} - 1)$ 。故由 (3) 式得$\ell|(2^{b-1} - 1)$。

現設$b > 1$。因p爲質數, 且$p > b > b - 1 > 0$, 故p與$b - 1$互質。故存在二正整數α, β,使得

$$\alpha p = \beta(b - 1) + 1 \text{ 或 } \alpha(b - 1) = \beta p + 1。$$

當$\alpha p=\beta(b-1)+1$時, 因$2^{b-1}-1$爲ℓ之倍數, 且

$$2^{\alpha p}=2^{\beta(b-1)+1}=((2^{b-1}-1)+1)^{\beta}\cdot 2,$$

故$2^{\alpha p}$除以ℓ餘2。但由$2^{\alpha p}=((2^{p}-1)+1)^{\alpha}$又得$2^{\alpha p}$除以$\ell$餘1。同理當$\alpha(b-1)=\beta p+1$亦導至矛盾。故得$b=1$。本定理證畢。

有了定理 6, 檢驗M_p是否爲質數的工作當然減輕不少。尤有進者, Fermat在西元1640年時向 Mersenne 提出法 (一): 當$p>2$時, M_p的質因數必爲$2kp+1$ 的型式 (Euler 在西元1747年利用二項式定理證明此結果)。例如, 當$p=11$時, $2kp+1=22k+1, k=1$可得質數23, 且$23|M_{11}=23\cdot 89$, 又 $89=22{\cdot}4+1$ 亦爲一質數; 當 $p=23$ 時,$2kp+1=46k+1, k=1$ 得質數47, 且 $47|M_{23}$; 當 $p=29$ 時,$2kp+1=58k+1, k=1,4$皆使此數爲質數, 但$59\nmid M_{29}$, 而 $233|M_{29}=536,870,911$ 。所以只需做一次除法, 即檢驗出 M_{23} 爲一合成數; 只需做兩次除法即檢驗 M_{29} 爲一合成數。同理, 對$p=37,41,43,47,53,59$, 甚至對一些很大的質數p, 如p =16,035,002,279(對此$p, q=2p+1$爲質數, 且$q|M_p$), 皆可利用此法檢驗出M_p爲合成數。

若 Cataldi 知道法 (一), 則只需檢驗 6 個小於 725, 且爲$38k+1$型式的質數 (即$191,229,419,457,571$及647), 是否能除盡M_{19}即可, 工作量顯然大幅度地減輕。不過對於M_{31}, 就要將157個$62k+1$型的質數去除M_{31}。因此 Euler 又提出下述法 (二): M_p的質因數可寫成$8n+1$或$8n-1$的型式。例如,

$$M_{11}=23\cdot 89=(8\cdot 3-1)(8\cdot 11+1)。$$

結合法(一) 及法(二) 將使 M_p 所可能具有的質因數又減少很多。例如, 對 M_{19} 現只需檢驗 $191,457$ 及647等三數, 能否除盡 M_{19} 。而 M_{31} 的質因數必爲 $248k+1$ 或 $248k+63$ 的型式, 可使檢驗 M_{31} 的除法減少至84次。Euler也因此於西元1772年證明 M_{31} $=2,147,483,647$ 爲 M_{19} 的下一個梅仙尼質數。雖距 M_{19} 的發現已隔了近二百年, 但若無前述這些好方法, 顯然要隔得更久。早期尋找梅仙尼質數的工作, 至此告一段落。

附帶一提, 那時的數學家持續地在研究判斷一梅仙尼數是否爲質數的方法。Euler尙有下述檢定法, 我們稱之爲法 (三): 若$p=4m+3, m\geq 1$, 爲一質數, 且$q=2p+1$ 亦爲一質數, 則 $q|M_p$, 因此 M_p 爲一合成數。諸如 p =11,23,83,131,179,191,239, 251等, 皆爲這類質數。再度地, 亦有一些很大的這類質數, 如 $p=$ 16,035,002,279 及 16,188,302,111 (對此二 p, M_p 的位數約有 $5\cdot 10^9$位)。

西元1876年, 法國數學家 Lucas(1842 -1891) 發現一個可很快地測出一梅仙尼數是否爲質數的方法。利用該法他發現 M_{67} 不爲質數 (不過他無法給出其因數), 且M_{127} 爲質數。M_{127} 位居最大質數的時期長達近四分之三世紀。至於 M_{61}, 則是在西元1883年由 Pervushin 證明爲質數。M_{89} 及 M_{107} 則分別在西元1911年及1913年, 由 Powers 及 Fauquembergue 證明爲質數。

Lucas證明當 p 爲型如 $8k-1$ 的質數時, 則 $p|M_{(p-1)/2}$。這結果可用來檢驗出許多 M_p 爲合成數。例如, $47|M_{23}$, $167|M_{83}$, $263|M_{131}$, $359|M_{179}$, $383|M_{191}$, $479|M_{239}$。雖然有這些方法來減少檢驗時的負擔, 但對 p 很大時, 檢驗的工作並非易事。如雖知 $M_{101}=2^{101}-1$ 的質因數爲 $202k+1$ 型式, 但 M_{101} 的質因數並不易找出 (顯然k很大)。西元1930年, Lehmer改良 Lucas 的方法, 提出了底下定理7所謂 Lucas-Lehmer 質數測試法, 並於西元1932年證明 M_{257} 爲質數 (梅仙尼質數名單的最後一個錯誤)。不利用 Lucas-Lehmer 法, 後來那些梅仙尼質數是無法發現的。

定理7: 令$u_1=4$, 且對$n\geq 1$, 令$u_{n+1}=u_n^2-2$。則對每一大於2之質數p, M_p爲質數的充要條件爲$M_p|u_{p-1}$。

定理7之證明可參考 Bruce(1993)。在定理7中數列 u_n 之前四項爲 4, 14, 194, 37,634, 增加快速, 檢驗似乎也不易。不過由定理7不難導出 $M_p|u_{p-1}$ 之充要條件爲 $r_{p-1}=0$, 其中 $r_1=4$, 而對 $n\geq 1$, 令 r_{n+1} 爲 r_n^2-2 除以 M_p 之餘數。顯見每一 $r_n\leq M_p-1$。所以我們把一成長很快的數列, 降成每一項皆不超過M_p的數列, 對計算上方便許多。例如, 若$p=5, M_5=31$, 則$r_1=4$,$r_2=14$,$r_3=8$,$r_4=0$, 故M_5爲一質數。又M_{101}有31位, 而因$r_{100}\neq 0$, 故得M_{101}爲一合成數。諸位是否留意到自定理6以來, 我們數次提到餘數? 事實上同餘 (即只考慮餘數) 爲數論中一重要的概念, 不過在此我們不擬討論。

有人進一步猜測, 若M_n爲一質數, 則 M_{M_n} 也是一質數 (眞是一群狂熱的數學家)。對首四個梅仙尼質數$(3,7,31,127)$,此猜測是對的, 但對第五個梅仙尼質數, 即$M_{13}=8,191$, 西元1953年, Wheeler 證出 $M_{M_{13}}=2^{8,191}-1$ 有2,466位) 爲一合成數, 所以此猜測是錯的。此事之驗證 (仍藉助 Lucas-Lehmer 法), 花了那時計算機一百小時之久 (但並未找出其因數)。後來又發現$M_{M_{17}}$ 爲合成數, 且有質因數1,768$(2^{17}-1)+1$, 而$M_{M_{19}}$亦爲合成數, 並有質因數$120(2^{19}-1)+1$。除此之外, 尙有一些其他的猜測, 我們就此打住。

西元1952年, 美國的 Robinson 以 SWAC 計算機 (這是人類首度以計算機來尋找梅仙尼質數), 找出第十三至第十七等五個梅仙尼質數:M_{521}, M_{607}, $M_{1,279}$, $M_{2,203}$, $M_{2,281}$。西元1957年 Riesel 利用瑞典計算機 BESK 花了五個半小時找出第十八個梅仙尼質數$M_{3,217}$。西元1961年, 美國數學家 Hurwitz 利用 IBM7090計算機找出 $M_{4,253}$ 及 $M_{4,423}$ 兩個。接著在西元1963年, 美國伊利諾大學 (University of Illinois) 的教授 Gillies 找出下三個$M_{9,689}$, $M_{9,941}$ 及 $M_{11,213}$。其中$M_{11,213}$共有3,376位。伊利諾大學對此發現很高興, 就在該校加蓋郵資戳記的機器上加進“$2^{11213}-1$ IS PRIME”一句。於是這句話就出現在該校寄出的每一封郵件上。

第二十四個梅仙尼質數$M_{19,937}$, 是由紐約的 Tuckerman 於西元1971年找到的。七年後, 西元1978年10月, 兩位美國加州十八歲的高中學生 Nickel 及 Noll 合找到第二十五個梅仙尼質數$M_{21,701}$。他們利用當地大學的計算機, 以 Lucas-Lehmer 法 (雖他們並不太了解其中所包含的數學), 花了450個小時找到的。當時美國所有的大新聞通訊社都報導此消息, 連 CBS 著名的主播 Cronkite 也在晚間新聞中報導。西元1979年2月, Noll單獨找到下一個$M_{23,209}$。同年4月加州的 Slowinski 設計了一計算機程式, 在 Nelson 協助下, 找到第二十七個梅仙尼質數$M_{44,497}$, 有13,395位。Slowinski雖在該年2月23日找到第26個梅仙尼質數, 不過後來他才知道 Noll 早他兩周已得到此結果。第二十八個梅仙尼質數$M_{86,243}$亦爲 Slowinski 於西元1983年所發現。他在 Cray 研究實驗室, 利用 CRAY-I 超級電腦, 單是檢驗此數確爲一質數就花了1小時3分鐘又22秒。不過提出此數之前的計算工作 (譬如對從44,497之後的質數p, 皆要檢驗M_p是否爲質數), 便花了數個月。下一個發現的梅仙尼質數, 其p值爲132,049, 這仍是 Slowinski 於西元1984年, 在 Cray 電腦上, 花了一周後得到的。再下一個梅仙尼質數, 則是西元1985年9月依然是由 Slowinski 以 Cray 電腦發現的, 爲$M_{216,091}$, 其位數達到65,050位。

有趣的是, 有幾年的時光, 上段中最後二質數, 分別被視爲第二十九個及第三十個梅仙尼質數。直到西元1988年1月29日, Colquitt 與 Welsh 在 Houston Area Research Center 發現第二十九個梅仙尼質數, 其p值爲110,503, 他們所用的機器爲 NEC SX*2超級電腦。他們並證實$M_{132,049}$確爲第三十個梅仙尼質數。但在p介於139,268與216,090間是否有梅仙尼質數M_p則未知。又他們也確定在p介於216,092與349,914間, 無任何梅仙尼質數M_p。

附帶一提, 在一封寫給 Ribenboim (Ribenboim(1996) 的作者) 的信中, Slowinski 還明確地指出 $M_{132,049}$ 已被他們證實爲第二十九個梅仙尼質數。

在西元1992年四月號的 The American Mathematical Monthly, 登了一則短聞, 標題爲“The Latest Mersenne Prime”。永不停止的 Slowinski 與 Gage 宣佈他們找到了最新的梅仙尼質數, 此第32個已知的梅仙尼質數爲$2^{756,839}-1$, 有227,832位。Slowinski與 Gage 用他們自己寫的程式, 在位於英國 Didcot 的 Harwell 實驗室的 CRAY-2計算機上, 證明此數爲一質數。

Slowinski 與 Gage 仍利用 Lucas-Lehmer 法來檢驗質數。經由一些巧妙的方法, 要求一數之很大的次方是可能的。但對一位數超過二十萬位的數, 即使只是求其平方也很不容易。Slowinski和 Gage 利用他們實驗室的同事 Kuba 所發展出來的快速的 Fourier 轉換 (fast Fourier transform) 的演算法 (algorithm)。但第一次檢驗$M_{756,839}$爲質數, 仍花了許多小時的計算機時間。後來在一台有16個處理器 (processors) 的計算機上再度檢驗時, 只需20分鐘。

在$M_{216,092}$與$M_{756,839}$之間是否有其他梅仙尼質數? 沒有人能肯定 (不過檢視梅仙尼質數出現的頻率, 我們猜測極可能是有的)。在 Harwell 實驗室的計算機, 只檢驗了85個質數, 便得到此新的質數。這位尋找梅仙尼質數的老手 Slowinski 說"我們碰到了難以置信的好運"。

尋找梅仙尼質數的工作是否會停止呢? 沒有, 一直持續地進行。

在 Cray 公司工作的 Slowinski(他在 Wisconsin 州的 Chippewa Falls 廠) 說服許多世界各地的 Cray 計算機的使用者, 利用他們計算機的多餘時間 (spare time) 來協助尋找梅仙尼質數。雖 Slowinski 承認他們的尋找並不是很有系統, 但他們仍在西元1994年1月找到下一個梅仙尼質數, 其p值爲 859,433。此質數位數有 258,716 位。接著在西元 1996 年 9 月 3 日, Slowinski 與 Gage(他在位於 Minnesota 州 Eagan 城的 Cray 公司總部工作) 利用 CRAY T94系統, 發現了目前所知最大的梅仙尼質數

$$2^{1,257,787}-1$$

其位數達到378,632位。事實上在幾個月前他們便發現了這個數, 不過如同以往, 在公佈之前, 他們請各地的研究人員協助檢驗是否正確無誤。

雖然梅仙尼質數的找尋有如大海撈針 (needle-in-a-haystack), 但由於有好的程式及極快速的計算機, 提高了找到的機會。目前最大的八個梅仙尼質數就有七個是在 Cray 研究實驗室發現的。每當他們找出一個新質數, 就會令世界各地的其他找尋者唉嘆不已。

介於最大及第二大的梅仙尼質數間的範圍, 大部分仍未被檢驗過, 在可預見的將來也不會去檢驗。依目前計算機的速度, 去檢驗爲數衆多的介於最大的幾個梅仙尼質數之間的梅仙尼數, 所需耗費的時間是難以想像的。Cray 公司一直鼓勵大家加入尋找的行列。不過$p \le 365,000$之M_p皆已檢驗過, 且大部分的$p \le 472,000$ 之M_p 也檢驗過。

欲知最新的梅仙尼質數的資料可透過網路查詢, 網址爲

http://www.utm.edu/research/primes/mersenne.shtml 。

3. 討論

曾有人問英國登山專家 George Leigh Mallory 爲什麼要去攀登聖母峰 (Mount Everest), 他答"因爲它就在那兒 (Because it's there)"。

西元1811年, 英國的 Peter Barlow, 針對 Euler 在西元1772年所發現的M_{31} (這是那時所知的最大的梅仙尼質數, 下一個要到西元1876年才出現), 曾說"此爲目前所知之最大的完全數, 今後很可能不會發現更大的了。此因這種尋找只是好奇心的驅使, 在沒有用途之情況下, 是沒有人有興趣去找下一個的"。

我們知道此預言當然是錯的, 因自那時起, 又出現了二十六個完全數。先不要管繼續找更大的完全數有什麼用, 對科學家而言, 這種嘗試就如同去攀登一座一座的高峰, 或田徑選手追 求更快的速度及更遠的投擲, 以及

其他的許多只是好奇而沒什麼用的工作。在十九世紀時, 人們自然預想不到現代計算機的威力, 就如我們無法預測五十年後會有什麼樣的機器一樣。

有幾個問題至今仍未解決, 我們只列舉兩個如下。

1. 有沒有奇完全數? 到目前爲止沒有人找到一奇完全數, 也沒有人證明奇完全數不存在。僅有的成果都只是說明在某個範圍內沒有奇完全數。例如, 若有奇完全數存在的話, 則其值必大於10^{200}, 且必須滿足一些條件: 若n爲一奇完全數, 則$n = q^{4\alpha+1}N^2$, 其中α爲一非負整數, q爲一型如$4m + 1$的質數, N爲一奇數且q不能除盡N。又n至少有8個相異質因數, 至少有29個質因數, 其最大者超過300,000, 第二大的必超過1,000。另外, 若一奇完全數不爲3的倍數, 則它必至少有11個相異的質因數。若一奇完全數除以12, 必餘1, 除以36, 必餘9。一個奇完全要滿足的條件越多, 它似乎就越不容易存在。

你會不會覺得相當有趣? 一方面我們可以完全決定偶完全數, 且判斷法看似很簡單, 只需檢驗$2^p - 1$是否爲一質數, 其中p爲一質數。但這檢驗卻是一極艱鉅的工作。另一方面我們無法回答是否有奇完全數, 雖然我們知道奇完全數若存在, 便得要滿足一大堆的條件。

2. 是否有無限多個完全數? 我們也可問類似的問題: 是否有無限多個偶完全數? 此答案很可能爲肯定的。

有人認爲上述二未解決的問題在數學上並不是很重要。探討此二問題的過程中, 也不像對 Fermat 最後定理 (Fermat's Last Theorm, Fermat 宣稱當$n \geq 3$爲一整數, $x^n + y^n = z^n$ 無非零整數解) 的研究, 能引出數學上不少重要的結果。因此就數學本身而言, 此二問題的解決與否並不重要。

近年來, 由於在密碼學 (cryptography) 及計算機系統的安全性, 用到很多數論中的結果, 特別是質數的性質, 所以很多大的電信公司, 如 IBM 及 Bell Telephone Company投入許多經費於質數的研究。而質數尋找的過程便已產生許多效益。

例如, Slowinski 與 Gage 所發展出來的找質數的程式, 便被 Cray 公司採用來檢驗超級電腦的品質保證 (quality assurance, 曾有一度此工作是藉求圓周率π來完成)。此程式中一主要的部分是將一數反覆地平方, 因此繼續下去, 便是在執行將很大的數自乘。這種工作就彷如對計算機做折磨的檢定: 從處理器的邏輯, 至主機的記憶, 編譯器, 操作系統, 及多元工作系統追蹤資料之能力的一很好的檢定。

Slowinski說 CRAY T94系統, 花了6個小時在一個中央處理器上檢定這最新發現的質數, 而若一機器能完成此艱鉅的工作, 我們便相信它能完成任何工作了。

Slowinski又說改進找尋質數程式的技術, 也可用來強化現實世界中, 諸如天氣預測, 汽車的安全設計, 及石油的找尋所需的程式。在研究質數找尋的程式中, 他們學到如何加速某些數學運算的新技術。這些操作, 往往是那些最需耗費大量計算的軟體程式中的主要部分。

梅仙尼質數的找尋可說已成為計算機品質的水準基標 (benchmark)。 Cray公司在一新的機器出廠前, 都會先在該機器上做梅仙尼質數的檢驗。Cray公司的發言人說"Slowinski 與 Gage 找得很有樂趣 (a lot of fun), 但他們的確對公司幫助很大"。不錯, 尋找巨大的質數對科學家而言, 主要的動機是好奇心, 但此找尋的過程卻產生了很多實際的用途。

在西元 1992 之前, 曾有一陣子世上所知之最大質數並非梅仙尼質數, 而是 John Brown 及其在美國加州 Amdahl Corporation 的工作夥伴合找出來的

$$391{,}581 \cdot 2^{216{,}193} - 1。$$

不過通常一個梅仙尼質數的誕生, 往往也是已知最大質數的一個里程碑。對數學家而言, 自Euclid 時代起, 便知質數有無限多個。但質數在自然數中的分佈情況, 本身便是一極有趣的問題。無人可回答下一個質數在何處。對比較小的數, 例如, 在 20 之前有 8 個質數:$2, 3, 5, 7, 11, 13, 17, 19$ 但在較大的數裡, 質數的出現, 便沒那麼頻繁了。但卻又無規律, 可以有任意大的間隔 (見習題), 也可很接近。例如, 在質數 370,261 之後, 接著 111 個合成數。另一方面, 存在很多孿生質數 (twin primes), 在 1,000,000 之前便有超過 8,000 對。在此所謂孿生質數表兩個相差為 2 之質數, 如 3, 5, 及 5, 7 皆是。Parady et al.(1990) 給出三個很大的孿生質數:

$$663,777 \cdot 2^{7,650} \pm 1,\ 571,305 \cdot 2^{7,701} \pm 1,$$
$$1,706,595 \cdot 2^{11,235} \pm 1,$$

可見即使在很大的數中, 仍可有二最接近的質數。事實上, 數學家猜測整數中存在無限多對孿生質數, 但此為一極難且尚未解決的問題。

對這些題材有興趣的讀者可參考 Scourfield(1979/80),Stewart(1987/88) 及 Piper (1988/89) 等文, 及 Ribenboim (1996) 一書, 有一些相關的材料可供進一步參考。在此必須一提, 在數學上 (當然指也藉助計算機), 檢驗一數是否為質數, 比將一數分解容易多了。換句話說即使我們檢驗出一數不為質數, 但若要將其寫成質因數的連乘積, 就困難很多。直到西元 1988 年左右, 最好的方法也只保證 80 位以內的數能分解。此並不表示更大的數便不可能分解, 只是需要更多的好運氣。分解因數牽涉到很多困難, 不只是與其位數多少有關。這也是為什麼在前面我們提到過 Lucas 雖在西元 1876 年檢驗出M_{67}非質數, 但卻沒給出其因數。一直到西元 1903 年, 在美國數學學會的一會議中, 一美國哥倫比亞大學 (Columbia University) 的教授 Cole 震驚了數學界, 在一篇"有關大數字的因數分解法"之報告, 他走上講台, 一聲不響地在黑板上寫下

$$2^{67}-1=193{,}707{,}721 \cdot 761{,}838{,}257{,}287\ 。$$

寫完後他又一言不發地回到座位, 聽眾給他如雷的掌聲, 沒有人問他問題。事後 Cole 說他花了三年的星期日才完成此分解工作。今天, 利用計算機, 我們當然可做得比 Cole 還

好。例如,

$$\begin{aligned}2^{257}-1 = {}&535{,}006{,}138{,}814{,}359\\ &\cdot 1{,}155{,}685{,}395{,}246{,}619,\\ &\quad 182,673,003\\ &\cdot 374{,}550{,}598{,}501{,}810{,}936,\\ &\quad 581,776,630,096,313,\\ &\quad 181,393,\end{aligned}$$

見 Riesel (1985)。這個令人看了眼花的分解, 是由 Penk 及 Baillie 在1979所分解成功的。目前最大的完全被分解的梅仙尼合成數為

$$M_{3{,}359} = 6{,}719 \cdot P1{,}008,$$

其中 $P1{,}008$ 表一有 1,008 位之質數 (見 Ribenboim(1996), p.67)。此數不但只有二質因數, 且其中 $6,719 = 2{\cdot}3{,}359{+}1$ 是$M_{3,359}$所可能有的質因數中之最小者。至西元1992年2月, 最小的尚未被分解出來的梅仙尼數為M_{467}。由於一般而言，若一數為幾個很大的質數的乘積, 其分解極困難, 此性質可應用在密碼學上。此方面的討論我們留在"同餘及質數在密碼學上的應用"一文再談。

註: Frank Nelson Cole 曾長期任美國數學學會的秘書 (1896-1920), 並當過美國數學學會的刊物 Bulletin 之主編長達21年。經由他自己及美國數學學會會員的捐款設立了 Frank Nelson Cole Prize in Algebra 及 Frank Nelson Cole Prize in Number Theory, 西元1928年首次頒獎, 每五年一次, 為代數及數論方面的大獎。

4. 尾聲

結束本文之前, 我們再給一些有趣的性質。

首先, 所謂三角數 (triangular number) 即為自1開始連續整數之和 (這是為何命名為三角數的原因)。而每一偶完全數皆為三角數 (性質 (i))。如

$$\begin{aligned}6 &= 1+2+3,\\ 28 &= 1+2+3+4+5+6+7,\\ 496 &= 1+2+3+4+5+6+7\\ &\quad +8+\cdots+31。\end{aligned}$$

證明就留給各位自己去完成。尚有一些其他的性質, 其證明皆留在習題。設 $A = 2^{p-1}\cdot(2^p-1)$ 為一偶完全數, 則

(ii) $A > 6$時, A為自1起若干個連續奇數的立方和。如 $28 = 1^3+3^3$, $496 = 1^3+3^3+5^3+7^3$, $8{,}128 = 1^3+3^3+\cdots+15^3$, 其中連續奇數的個數 (如28有2個, 496有4個) 為$2^{(p-1)/2}$。

(iii) $A = 2^{p-1}+2^p+\cdots+2^{2p-2}$。如 $6 = 2^1+2^2, 28 = 2^2+2^3+2^4$, $496 = 2^4+2^5+2^6+2^7+2^8$。

(iv) A之所有因數 (含本身) 之倒數和為2。如

$$A=6,\ \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=2,$$
$$A=28,$$
$$\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{7}+\frac{1}{14}+\frac{1}{28}=2。$$

其次, 那些巨大的完全數, 究竟有多大你能想像嗎? 以第三十四個為例, 其位數超過七十五萬位, 若將此數以 A4紙來書寫, 1公分約可寫5個數字, 就算一頁可寫四千位, 需

要188頁 A4紙。此數字總長約1,500公尺。再以另一種方式來看。六個十元銅板其厚度約一公分。若有人要你在一象棋盤 (共64個空格) 第一個空格放一個10元, 第二個空格放2^1個10元, 第二個空格放2^2個10元, 餘類推。總共有幾個銅板? 不難算出有$2^{64}-1$個。將這些銅板疊起來, 你猜有多高? 100公尺?100,000公尺? 答案是超過30兆公里。此距離又是多少呢? 太陽距地球約有$1.496\cdot 10^8$ 公里, 所以約爲太陽與地球間距的20萬倍。至於將$2^{1,257,786}(2^{1,257,787}-1)$個十元銅板疊起有多高? 就更不用去想像了。

你對這些質數有何看法呢? 念質數之悠悠, 獨愴然而涕下, 或余學完全數, 想見其奧妙? 是心嚮往之, 亦或避之惟恐不及?

求一數之因數, 其用途是很容易理解的 (你能列出一些嗎?)。但一數之所有眞因數的和, 代表的意義就不是很淸楚了。至於重視眞因數的和等於該數, 你可以說其實毫無道理。但古希臘人由此引進完全數, 後來轉化爲梅仙尼質數的尋找; 由做苦工似的硬算, 進而發展出一些較有效的方法, 再來是藉助計算機, 最後回饋到計算機品質的檢驗。不但將一看似毫無道理的偏愛, 變成許多人的嗜好, 且居然與現代科技相輔相成。而歷經兩千多年, 卻又只產生區區34個, 完全數在自然數中密度這麼地低, 古希臘人的珍惜, 想來眞是有道理。

Plato說“數是事物之永恆連續的保證 (Number is the bond of the eternal continuous of things)”。數字的優美或有趣的性質俯拾即是。順手拈來, 我們介紹親和數 (amicable number)。Pythagoras 說“朋友是你靈魂的倩影, 要像220與284一樣親密”。這是什麼意思呢? 原來 Pythagoras 發現, 在自然數220與284間有一很特殊的關係。

220的眞因數爲1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, 其和爲284。而284之眞因數爲1, 2, 4, 71, 142,其和爲220。二數之眞因數和恰等於對方 (完全數是眞因數和等於自己), 此二數眞是親密無比。具有這種性質的二數便稱爲一對親和數。220與284是人類所知的第一對親和數, 也是最小的一對。當然, 你一定很納悶, 怎麼連這種性質都留意到? 古希臘人可說玩弄數字於股掌。

親和數在古代也被賦予神秘的色彩, 人們有時將一對親和數分別寫在兩個護身符上, 而佩帶這種護身符的兩個朋友, 被認爲因此能友誼長存。

經過漫長的一段時間, 第二對親和數17,296和18,416是 Fermat 在西元1636年發現的。兩年後 Descartes 也發現了一對, 即9,363,584和9,437,056。十八世紀中葉, Euler 有系統地研究親和數, 在西元1750年發表了64對親和數 (但其中兩對後來發現是錯的), 其中包括2,626和2,924及5,020和5,564等。不過令人感到意外的是, 西元1867年, 一位十六歲的義大利中學生 Paganini 發現1,184和1,210也是一對親和數。這一對在自然數中第二小的親和數, 竟然不在 Euler 的名單中。

不少數學家試圖找出能表示出所有親和數的公式 (彷如能表示出所有偶完全數的公式)。下述公式只能找到某些親和數。西元九

世紀, 阿拉伯數學家提出: 設$n \geq 2$為一整數。令

$$A = 3 \cdot 2^n - 1, B = 3 \cdot 2^{n-1} - 1,$$
$$C = 9 \cdot 2^{2n-1} - 1。$$

若A, B, C均為質數, 則$2^n AB$和$2^n C$為一對親和數。舉例來看。取$n = 2$, 則

$$A = 3 \cdot 4 - 1 = 11, B = 3 \cdot 2 - 1 = 5,$$
$$C = 9 \cdot 8 - 1 = 71$$

皆為質數, 故$2^2 \cdot 11 \cdot 5 = 220$和$2^2 \cdot 71 = 284$為一對親和數。另外, 取$n = 7$, 可找到另一對親和數, 但直至$n \leq 200$ 再也不能找到其他對了。

還有一些其他公式我們便不提了。西元1923年 Madachy 與 Lee 發表1,095對親和數, 同年荷蘭的 Riele 給出一對有152位的親和數。親和數顯然較完全數多許多。當然也有一些未解決的問題, 如 (你可能也猜得到) 是否存在無限多對親和數? 現已找出的每一對親和數, 皆同為偶數或同為奇數, 但是否有一奇一偶的親和數? 不讓你頭痛了, 我們就此打住。

數學家對數字的愛好, 是否令你嘆為觀止呢? 介紹最後一題材給你。所謂階乘數 (factorion) 為一數等於其各位數字之階乘和。例如, 因

$$145 = 1! + 4! + 5!\ ,$$

故 145 為一階乘數。此處“!”為階乘 (factorial) 記號, 即

$$n! = n(n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1, n \geq 1,$$

但將0!定義為1。尚有兩個很小的階乘數, 即

$$1 = 1!,\ 2 = 2!。$$

目前所知之最大的階乘數為

$$40{,}585 = 4! + 0! + 5! + 8! + 5!,$$

為 Dougherty 在西元1964年利用計算機找出來的。這四個也就是現今所知的四個階乘數。你是否眼睛一亮, 聯想到古希臘時代只知四個完全數, 而躍躍一試?

我們不得不澆你一盆冷水, 這就是僅有的四個階乘數, 證明眞的不難, 就留給你自己完成好了。若實在做不出, 請參考 Pickover (1995/96)。看來要成名並不容易。

5. 附錄: 已知之三十四個完全數表

由定理1知, 對一質數p, 若$M_p = 2^p - 1$為一梅仙尼質數, 則$2^{p-1} M_p$ 為一完全數。前面我們依序提到已知的三十四個梅仙尼質數, 因此已知的三十四個完全數也就確定了。為了讀者方便, 我們仍列出此三十四個完全數, 其中年代皆為西元。

序數	完全數	位數	發現年代	發現者
1	$2^1(2^2-1)$	1	不詳	不詳
2	$2^2(2^3-1)$	2	不詳	不詳
3	$2^4(2^5-1)$	3	不詳	不詳
4	$2^6(2^7-1)$	4	不詳	不詳
5	$2^{12}(2^{13}-1)$	8	1461	不詳
6	$2^{16}(2^{17}-1)$	10	1588	Cataldi
7	$2^{18}(2^{19}-1)$	12	1588	Cataldi
8	$2^{30}(2^{31}-1)$	19	1772	Euler
9	$2^{60}(2^{61}-1)$	37	1883	Pervushin
10	$2^{88}(2^{89}-1)$	54	1911	Powers
11	$2^{106}(2^{107}-1)$	65	1913	Fauquembergue
12	$2^{126}(2^{127}-1)$	77	1876	Lucas
13	$2^{520}(2^{521}-1)$	314	1952	Robinson
14	$2^{606}(2^{607}-1)$	366	1952	Robinson
15	$2^{1,278}(2^{1,279}-1)$	770	1952	Robinson
16	$2^{2,202}(2^{2,203}-1)$	1,327	1952	Robinson
17	$2^{2,280}(2^{2,281}-1)$	1,373	1952	Robinson
18	$2^{3,216}(2^{3,217}-1)$	1,937	1957	Riesel
19	$2^{4,252}(2^{4,253}-1)$	2,561	1961	Hurwitz
20	$2^{4,422}(2^{4,423}-1)$	2,663	1961	Hurwitz
21	$2^{9,688}(2^{9,689}-1)$	5,834	1963	Gillies
22	$2^{9,940}(2^{9,941}-1)$	5,985	1963	Gillies
23	$2^{11,212}(2^{11,213}-1)$	6,751	1963	Gillies
24	$2^{19,936}(2^{19,937}-1)$	12,003	1971	Tuckerman
25	$2^{21,700}(2^{21,701}-1)$	13,066	1978	Noll and Nickel
26	$2^{23,208}(2^{23,209}-1)$	13,973	1979	Noll
27	$2^{44,496}(2^{44,497}-1)$	26,790	1979	Nelson and Slowinski
28	$2^{86,242}(2^{86,243}-1)$	51,924	1982	Slowinski
29	$2^{110,502}(2^{110,503}-1)$	60,530	1988	Colquitt and Welsh
30	$2^{132,048}(2^{132,049}-1)$	79,502	1983	Slowinski
31	$2^{216,090}(2^{216,091}-1)$	130,100	1985	Slowinski
?	$2^{756,838}(2^{756,839}-1)$	455,663	1992	Slowinski and Gage
?	$2^{859,432}(2^{859,433}-1)$	517,430	1994	Slowinski and Gage
?	$2^{1,257,786}(2^{1,257,787}-1)$	757,263	1996	Slowinski and Gage

習題:

1. 試將1,729之兩種立方和的表示法寫出。
2. 試找出可以兩種方式表示成二正整數平方和之最小整數, 並試給一找出可以兩種方式表示成二整數平方和之整數的方法。註: 這種整數必非質數 (見林聰源譯(1976)p.38)。
3. 試證定理5。
4. 試證偶完全數的個位數字必爲6或8。
5. 試證 (1) 式成立。
6. 試證 (2) 式成立。
7. 試證質數有無限多個。
8. 試證M_{23}及M_{29}皆爲合成數。
9. 試證 M_{31} 的質因數必爲 $248k+1$ 或 $248k+63$ 的型式。
10. 試證任二梅仙尼數皆無公因數。
11. 設一梅仙尼質數之位數有13,395位。求其p值。
12. 試證偶完全數的性質 (i) 至 (iv)。
13. 令 $s(n)$ 表正整數 n 之所有眞因數的和, 若 $s(n)<n$, 則 n 稱爲一虧數 (deficient); 若 $s(n)>n$, 則 n 稱爲一盈數 (abundant)。完全數恰爲介於虧數與盈數間。試證 (i) 若p爲一質數, 則對每一正整數 α, p^α 爲一虧數;(ii) 首6個盈數爲 $12,18,20,24,30,36$, 而1至39間除了此6個數及二 完全數 $6,28$ 外, 皆爲虧數;(iii) 第一個奇的盈數爲945。
14. 設k爲一正整數, 令$A=(k+1)!$。試證$2|(A+2),3|(A+3),\cdots,(k+1)|(A+k+1)$, 即有連續$k$個整數皆非質數。本例顯示二相鄰質數之間隔可任意遠。
15. 試證17,296與18,416爲一對親和數。
16. 試證僅有四個階乘數。

誌謝:

本文之完成得到同事官大智、李良修、羅春光及羅夢娜等四位教授協助提供資料, 王秀英小姐及蔡菁秤小姐也幫了不少忙, 非常感謝他們。

後記:

本文完成後, 又發現一新資料。目前所知最大的梅仙尼質數爲

$$2^{1,398,269}-1,$$

其位數達到$420,921$ 位, 對應的完全數則有$841,842$。西元1996年初, Woltman 發起了一共同尋找梅仙尼質數的組織 (The Great Internet Mersenne Prime Search, 簡稱 GIMPS), 提供可在個人電腦上使用的找巨大質數的軟體給同好。Armengaud 便是這數百位搜尋者之一, 西元1996年11月13日, 他找到上述第三十五個目前已知的梅仙尼質數。而 Slowinshi 已證實此數確爲一質數。

參考資料

1. 林聰源譯 (1976)。整數論的問題。楓城出版社, 新竹。
2. 金庸 (1984)。射雕英雄傳。遠景出版社, 台北。
3. 曹亮吉 (1984)。談數學。科學月刊社, 台北。
4. 藍紀正、朱恩寬譯 (1992)。歐幾里得幾何原本。九章出版社, 台北。

5. Bruce, J. W. (1993). A really trivial proof of the Lucas-Lehmer test. The American Mathematical Monthly 100, 370-371.
6. Hill,R. (1987/88). Ramanujan-his life and work. Mathematical Spectrum 20, 1-8.
7. Parady, D. K., Smith, J. F. and Zarantonello, S. E. (1990). Largest known twin primes. Mathematics of Computation 55, 381-382.
8. Pickover, C. (1995/96). The loneliness of the fractorions. Mathematical Spectrum 28, 64-65.
9. Piper, F. (1988/89). Cryptographic uses of large numbers. Mathematical Spectrum 21, 1-7.
10. Ribenboim, P. (1996). The New Book of Prime Number Records. Springer-Verlag, New York.
11. Riesel, H. (1985). Prime Numbers and Computer Methods for Factorization. Birkhäuser, Boston.
12. Scourfield, E. J. (1979/80). Perfect numbers and Mersenne primes. Mathematical Spectrum 12, 84-92.
13. Stewart, I. (1987/88). Factorizing large numbers. Mathematical Spectrum 20, 74-77.

—本文作者任教於國立中山大學應用數學系—