最大質數的新里程碑

2,3,5,7,11,13,17,19,……凡是僅能被1與自己整除的正整數被稱為質數。判斷一個正整數 n 是否為質數除了使用艾勒托塞尼斯篩法（sieve of Eratosthenes）或稱質數篩（拿比$\sqrt{n}$ 小的質數去除 n），對於某特定形式的質數有著其他的判斷方法。歐幾里得使用反證法證明質數的個數有無窮多個，歐拉則是利用調和級數

$$\prod_{\text{prime } p} \frac{1}{1-1/p} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

給出不同的證明。

凡表示為 2^p-1（記為 M_p）型式的質數被稱為莫森尼質數（Mersenne prime），是以第一個尋找莫森尼質數的法國數學家和修道士莫森尼（Marin Mersenne）命名的。如果 p 不是質數則 M_p 必非質數，但即使 p 是質數也並不能保證 M_p 是質數；例如前四個莫森尼質數為 $M_2=3$，$M_3=7$，$M_5=31$，$M_7=127$ 但 $M_{11}=2047=23\times 89$ 並非質數。莫森尼找到 $p\le 257$ 以內的9個莫森尼質數（扣掉找錯的兩個），後人又找出他遺漏的3個，而更大的就無法依靠人力了。

在莫森尼之後約一百年，歐拉在研究完全數時意外與莫森尼質數扯上了關係；一個等於自己以外的因數和的正整數稱為完全數或完美數（perfect number），例如：$6=1+2+3$，$28=1+2+4+7+14$。歐幾里得與歐拉分別對偶數的完全數的刻畫給出了必要性與充分性的證明：所有偶數的完全數必為型如 $2^{p-1}(2^p-1)$ 且 2^p-1 為質數（因此 p 也是質數）；也就是說，所有偶數的完全數

$$2^{p-1}(2^p-1)=\frac{M_p(M_p+1)}{2}$$

與莫森尼質數 M_p 一樣多。

至於是否存在奇數的完全數，以及與是否有無窮多個莫森尼質數，仍為未解之謎。

一篇在2003年關於發現最大質數 $M_{20996011}$（約六百萬位數）的報導，吸引了住在美國田納西州的51歲聯邦快遞（FedEx）的電子工程師佩斯（Jonathan Pace）的注意，使他踏入了尋找最大質數的旅程。自從加入網際網路莫森尼質數大搜索（Great Internet Mersenne Prime Search, GIMPS），在歷經了14年的努力後，佩斯終於在2017年12月26日找到了它 —— $M_{77232917}$，同時也是第50個莫森尼質數（暫時排名，第47個尚在確認中）；這個新的人類已知最大質數足足有23,249,425（約兩千三百多萬）位數，比前一個最大已知質數 $M_{74207281}$ 多了90,807（約九萬）位數。

佩斯並沒有使用高規格硬體的超級電腦，而是在身兼田納西州的日耳曼敦基督教會的執事，負責電腦設備與網路管理的同時，只是拿教會裡的其中一部桌上電腦，來執行由www.mersenne.org GIMPS網頁所免費下載的搜尋質數軟體。這部電腦跑了六天才確認 $M_{77232917}$ 是質數，再經過四組不同規格與程式的電腦檢驗，於2018年1月3日正式被GIMPS宣告這個結果，距離上一次已經是兩年之前的事了。

找尋莫森尼質數除了使用質數篩，在1772年歐拉利用同餘運算簡化篩選的過程，證明了

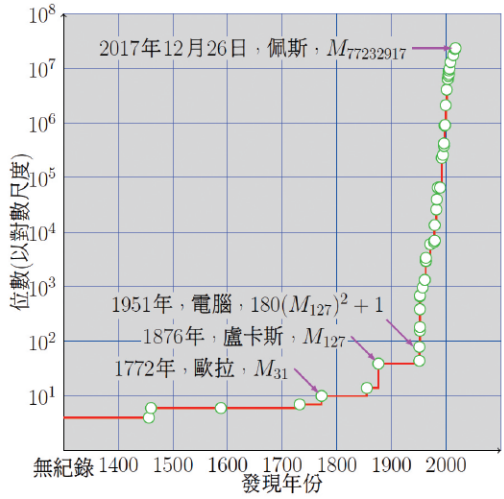
$$M_{31}=2,147,483,647$$

是質數（第8個莫森尼質數）；當時並沒有電子計算機，同時他是個65歲的全盲老人，而這個質數也稱冠了約一個世紀。目前主要是使用盧卡斯/萊默（Lucas-Lehmer）判定法，由盧卡斯（François Édouard Anatole Lucas）於1878年提出後，經萊默（Derrick Henry Lehmer）於1930年改善完成；盧卡斯利用他的方法在1876年找到了 M_{127}（39位數，第12個莫森尼質數），在這之後找到的質數都是透過電子計算機或電腦。其方法為：如欲檢驗

M_p 是否為質數，只要從4開始重複「平方後減2」此程序 $p-2$ 次，再檢驗最後得到的數字是否能被 M_p 整除。例如：$M_5=31$ ， $((4^2-2)^2-2)^2-2=37,634=M_5\times 1,214$ 。在運算中過程中每執行完一次程序後，可以改用除以 M_p 的餘數取代現有的數，這樣就能大幅降低運算的時間。因此，比起盲目地找尋最大的質數，從莫森尼質數中去找機會比較大。這個方法是目前判斷莫森尼質數最有效的方法，也是GIMPS從1996年後不斷找到最大質數（都是莫森尼質數）所用的方法。

既然莫森尼質數 M_p 中的 p 必須也是個質數，因此 $M_{M_p}=2^{2^p-1}-1$ 有機會是質數；這種型式的質數稱為雙重莫森尼質數（double Mersenne prime）。例如：$M_{M_2}=M_3$ ， $M_{M_3}=M_7$ ， $M_{M_5}=M_{31}$ ， $M_{M_7}=M_{127}$ 。目前只找到上述（$p=2,3,5,7$）四個雙重莫森尼質數，同時當 $p=13,17,19,31$ 已知 M_p 是莫森尼質數但 M_{M_p} 不是雙重莫森尼質數，而下一個的 $M_{M_{61}}$ 是不是質數則還在檢驗中。

有著 $2^{2^n}+1$（記為 F_n）型式的數被稱為費馬數（Fermat number）。在1650年費馬發現 $F_0=3$ ， $F_1=5$ ， $F_2=17$ ， $F_3=257$ ， $F_4=65,537$ 這五個費馬數都是質數，而且如果 m 不是 2^n 的型式 2^m+1 就不是質數；因此他猜想所有費馬數都是質數（稱為費馬質數）。但是歐拉在1732年給出 $F_5=4,294,967,297=641\times 6,700,417$ 摧毀了他的夢想，並且之後證明所有的費馬數 F_n 必有一個 $k\times 2^{n+1}+1$ 的質因數（後來盧卡斯改進成 $k\times 2^{n+2}+1$）。因此使用質數篩檢驗費馬數 F_n 是否為質數時，只要找比 $2^{2^n-1}(<\sqrt{F_n})$ 小同時有 $k\times 2^{n+2}+1$ 型式的質數去除；例如：$641=5\times 2^{5+2}+1$ 能整除 F_5。沒想到時至今日，即使目前已知的最大費馬數（於2014年發現）有超過一百萬位數，但還是沒能發現第六個費馬質數。



下一個質數在哪裡？質數定理（prime number theorem）中闡明比 n 小的質數約有 $n/\ln n$ 個，也就是第 n 個質數大約是 $n\ln n$ 這麼大。這個定理是1798年勒讓德提出的，而一封高斯在1849年的信中回憶說到他在15歲時（1792年）就提出質數的密度約為 $1/\ln n$ 的等價猜想，直到1896年由阿達瑪（Jacques Solomon Hadamard）以及瓦里普桑（Charles Jean de la Vallée-Poussin）分別都使用上複分析與黎曼 ζ 函數來證明。

既然已知有無窮多個質數，但為何人們持續地尋找大質數呢？三位美國麻省理工學院的學者李維斯特（Ronald Linn Rivest）、沙米爾（Adi Shamir）、艾得曼（Leonard Max Adleman）在1977年提出一個非對稱的加密演算法，稱為RSA加密法 —— 透過公開的公鑰加密後的密文，持有私鑰的一方可以將其還原；這是目前廣泛應用在網路通訊安全（SSL，TLS）、數位簽章與電子商務認證所使用的方法。加密過程中使用兩個相異的質數的乘積作為金鑰，因此其安全性與將此數因數分解的時間相關；因數分解遠比判斷質數難多了，而且使用的質數越大就越難分解，但是加解密的時間也越長。隨著電腦運算能力與速度的進步，大質數的需求因應而生；自2009年768位元（232位數的金鑰）的RSA加密法被破解後，目前使用的1024位元也逐漸改成2048位元以上；即使用目前世界上最快的超級電腦 —— 中國的神威・太湖之光也難在有生之年解開。（編輯室）

知識的代價

開放近用是解決方案？

想像一下，透過納稅人所贊助的經費，學者將研究的成果寫成一篇文章，投稿到出版商所發行的學術期刊，經過同儕評閱（peer review）接受後，出版商會向學者索取刊登的費用，最後出版刊登手稿在期刊上。文章一旦出版，出版商就擁有它的版權。他們會把它賣給想要閱讀的人，但是學者不會分到任何利潤。假若學者願意向出版商支付更高的印刷費用，就可免費向公眾發布。這是學術界在主流期刊上發表研究成果的選擇。

然而，在上世紀的90年代起，期刊與出版商彼此合併或兼併之後，學術出版業已經成為一項利潤豐厚的業務。呈現寡占狀態的學術出版市場被Elsevier、Springer、Taylor & Francis和Wiley等跨國商業出版商出版發行了佔比超過70%以上不同學科領域的學術研究期刊。這衍生出了文獻過度集中化的現象與不合理的商業模式，使得世界各國的大學與研究機構圖書館漸漸無力負擔出版商以每年約10%提高的訂閱費用。根據美國研究圖書館（Association of Research Libraries）統計，自1986年到2012年間，期刊價格漲幅達456%，約為同期間消費者物價指數（CPI）上漲幅度的四倍，期刊價格高居圖書館開支最高的寶座多年。Elsevier，Springer和Taylor & Francis的利潤率平均在35%左右，高於Facebook（27%）。

在網路時代前，這些大型的出版商在傳播新的科思想和發現上扮演了重要的角色。網路的出現迫使出版商必須重新考慮他們的商業模式，部分原因在於學者可以很容易的跳過眾所周知的中間商，並直接與讀者接觸。但他們仍然是科學出版領域的主要參與者。

近十多年來，許多學者的挫敗感表現在學術出版商正在從他們的勞動和貢獻中獲得豐厚的利潤（就像文章本身一樣，同儕評閱也是免費提供給期刊）。

公共贊助的研究成果應該可供所有人閱讀。過去幾年呼籲改革的聲浪越來越高。主要例子是由劍橋大學1994年菲爾茲獎得主高爾斯（Timothy Gowers）發起的「知識的代價」（The Cost of Knowledge）運動。呼籲學界共同抵制最大的學術期刊出版商Elsevier剝削研究學者與社會的商業模式，以高爾斯的文章為序幕，一場向Elsevier抗議的「學術之春」（Academic Spring）開始在美、加與許多歐盟的國家的學術機構蔓延。本刊的第9期〈學術界揭竿而起——推倒貪婪期刊付費高牆〉一文中曾有相關的報導。

在這波抵制Elsevier的浪潮中，臺灣也沒有缺席。代表215所公、私立大學、科技大學、專科院校及研究機構的臺灣學術電子資訊資源共享聯盟（CONCERT）也在2016年12月7日宣布，暫緩和Elsevier更新合約。Elsevier轉而單獨與大學打交道。但包括中央研究院在內的許多其他研究機構都決定自2017年1月1日起維持抵制活動。

將學術出版讓從期刊訂閱模式推向網路上免費提供內容的開放近用（open-access）模式的努力正逐步升級中。例如，美國的國立衛生研究院（NIH）的公共近用政策就規定「由NIH贊助的所有研究者必須提交已被同儕評閱接受發表文章的一份電子版本到PubMed Central資料庫中並提供出版年份。」（美國與Elsevier的所有醫學相關期刊合約都符合此要求。）歐盟各國也正在分享如何促成與Elsevier談判新合約的策略，這份新合約可能會在付費牆（paywall）外出現更多文章。

經過同儕評閱開放近用的期刊可以更有效的服務科學，也可以在保證研究質量的同時提供給公眾使用。除此之外，政府和大學及研究機構還必須加大力度，以公眾可以理解的方式傳達研究成果。（編輯室）

2018年數學獎

2018年的阿貝爾獎頒給了普林斯頓高等研究院的榮譽教授朗蘭茲（Robert Langlands）。獲獎的原因是「他連結了表現論與數論有遠見的綱領。」朗蘭茲也是1996年的沃爾夫獎以及2007年邵逸夫數學獎得主。

很多數學家因為證明「定理」或「猜想」而成名。但只有朗蘭茲是提出一個「綱領」而不朽。事實上，他的觀點非常激進，他為建立這些數學領域所建議的機制如此豐富，這對於數學家來說是很令人興奮的，因為它將顯然不相關的學科連接在一起，揭示了許多數學背後的更深層次的結構，並提供了解決棘手問題的新方法。它不僅有一個深遠的猜想脈絡，有時還包括定理，它將數論、代數幾何、表現論和數學物理，以意想不到的方式與物理學相聯繫。

朗蘭茲綱領在過去的50年中吸引了數百名世界上最好的數學家投入研究。現代數學中沒有其他綱領具有如此廣泛的影響，產生了如此多的深刻結果，並且有這麼多人在研究它。隨著深度和廣度的增長，因此它常被形容是「數學的大一統理論」。

數學家們證明朗蘭茲綱領中的猜想，被授予菲爾茲獎的，除了1990年在因「在量子群與數論的研究工作」的狄林費德（Vladimir Drinfeld），還有2002年的拉弗格（Laurent Lafforgue）因「在函數體的一般線性群 $\mathbf{GL}_r(r \geq 1)$ 上證明了朗蘭茲對應」以及2010年吳寶珠（Ngô Bảo Châu）證明了「朗蘭茲所提議的的自守形式基本引理」。

2018年數學大獎的沃爾夫獎頒給了兩位同在芝加哥大學的貝林森（Alexander Beilinson）與狄林費德。得獎的理由是「在代數幾何，表現論和數學物理方面有開創性的工作。」貝林森與狄林費德在幾何朗蘭茲綱領的合作，甚至可追溯到1975年，當時他們還是在莫斯科國立大學馬寧（Yuri Manin）的學生時期。

貝林森的傑出成就有：證明了在表現論的發展中扮演了重要角色的卡茲丹/魯茨提格猜想（Kazhdan-Lusztig conjecture）和岩琛猜想（Jantzen conjecture）。提出了在代數幾何領域裡的許多貝林森猜想，它們在幾何與數學物理的連結有很重要的貢獻。

有許多的數學名詞是以狄林費德的研究工作而命名的，例如：狄林費德（Drinfeld module）、狄林費德上半平面（Drinfeld upper half plane）以及狄林費德接合子（Drinfeld associator）等等。曾有人半開玩笑的說：「狄林費德是形容詞，而非人名。」

2016年起迄今十位的「數學新秀獎」得主中有五位都是因為在朗蘭茲綱領的研究有重大突破而獲獎。而且他們全部都尚未滿40歲。今年的9月1日到5日將在巴西的里約熱內盧舉辦國際數學家年會，2018年菲爾茲獎的宣布與頒發將是年會的重頭戲之一。是否有第四位因從事朗蘭茲綱領的研究而被授予菲爾茲獎，值得觀察。

有「亞洲諾貝爾獎」之稱的2018年邵逸夫數學獎是頒給了德州奧斯汀分校的卡法瑞里（Luis Caffarelli）。以「表彰他在偏微分方程上的開創性研究工作。包含了創建了一系列的非線性方程正則性理論，如蒙日/安培方程；以及自由邊界問題，如障礙問題。影響了這整個世代的研究該領域的學者。」

卡法瑞里是世界公認的非線性偏微分方程自由邊界問題的領先專家。在許多長期挑戰數學家們的經典問題的研究方法上，卡法瑞里是先驅者之一。他在納維爾/史托克斯方程的部分正則性問題（千禧年大獎難題之一）有開創性的工作。他也是2012年沃爾夫數學獎的得主。（編輯室）