孿生質數猜想的一大步

張益唐

Lisa Nugent提供
新罕布夏大學照片服務處

五月數學界最引人議論的大新聞，是華人數學家張益唐證明了弱孿生質數猜想，媒體用斗大的標題寫著「質數不再孤獨了！」

「質數的孤獨」拜義大利暢銷小說之賜，成了目前流行的話語。質數是除了1與本身之外，沒有其他因數的自然數。依照定義，質數不像12有著1、2、3、4、6、12這麼多「朋友」，因此是孤獨的。

但是質數的孤獨有另一層意思。

歐幾里得早在2000多年前就在《原本》中證明質數有無窮多個。這是數學史上的重要定理，不但有數論的意義，它也演示了人類第一次嚴格思考「無窮」，並帶入歸謬法這個與無窮常相左右的重要證明工具。用康托（G. Cantor）的說法，質數甚至和整數一樣多！

不過質數的孤獨，不是多寡、而是密度的問題。如果將質數一路表列下去，質數會愈來愈稀疏。例如在一億之內有5,761,455個質數，密度大約是0.06；一兆之內有37,607,912,018個質數，密度大約只剩0.038。

事實上，如果用 $\pi(n)$ 表示不超過 n 的質數數目，高斯曾經給出下面的猜想：

$$\frac{\pi(n)}{n} \sim \frac{1}{\ln n}$$

意思是說隨著 n 變大，左式除以右式的比值將會趨近於1。例如在一億時，比值大約是1.06，到了一兆，比值大概是1.04。

高斯的猜想透過黎曼引入複變函數的演繹（包括他更宏大的黎曼假說），在1896年由阿達瑪（J. Hadamard）與瓦里普桑（C. Vallée-Poussin）兩人獨立證明，史稱質數定理。由於這個定理太優美，1949年知名數學家艾狄胥（P. Erdös）和塞爾伯格（A. Selberg）又以基本數學加以重證，到了80年代甚至被簡化到兩三頁的證明。

質數定理的顯然推論，是質數之間的平均距離在 n 之內大約是

$$\frac{n}{\pi(n)} \sim \ln n$$

例如一億之內質數的平均距離大約是17.4，一兆之內質數的平均距離大約是26.6。這似乎正是質數孤獨的「鐵證」。

不過再仔細觀察質數表，很容易發現質數的出現並不均勻，好比質數經常成對出現，例如2和3、29和31、431和433等。打個比方，如果將質數想成天上相對距離愈來愈遠的星星，孿生質數就好像雙星一樣。但因爲質數定理，這種現象是不是終究會消失呢？

數學家對質數奇特的叢聚現象充滿信心。1849年數學家波里納克（A. Polignac）提出一項猜測：對任何自然數 k，距離 $2k$ 的質數對會出現無窮次。至於對孿生質數的特別關心，則可能出自英國天文數學家葛萊許（J. Glaisher）1878年的文章，他曾是知名哲學家維根斯坦的導師。

在張益唐之前，關於這個猜想的最好結果是三位數學家的研究，他們證明如果任意選擇一個很小的因子，你總是可以找到兩個質數，讓它們的距離落在這個因子與平均距離的乘積之內。不過任意小的因子並不表示他們證明了孿生質數猜想，這是因爲平均距離會隨著 n 愈來愈大的緣故。

2005年出現的這個結果，引起張益唐的興趣，在苦思多年之後，終於在去年夏天找到解謎的關鍵，證明了比較弱的孿生質數猜想：有無窮多質數對，其距離小於70,000,000。2和70,000,000相比似乎差距很大，但是數學家看重的是如何從無限跨到有限的新方法。確立了固定距離的存在，就足以證明有無窮多質數不孤獨，這是數論研究的一大步。

張益唐深知這個結果的重要性，將論文投交知名的數學期刊 *Annals of Mathematics*，並在很短的時間內通過審查。5月13日他在哈佛大學做首次公開演講，獲得在座數學家的掌聲與賀喜，並開始獲得媒體的注意。

不過媒體對這段故事之所以驚豔，並不只是因爲質

數不再孤獨，而是張益唐的傳奇際遇。

張益唐今年大約58歲，目前的職銜是新罕布夏大學數學統計系的講師。除了2001年在 *Duke Journal* 發表過一篇文章，他幾乎可說是名不見經傳。新罕布夏大學也非美國的名校，系上最知名的老師應該是剛過世的阿培爾（K. Appel），他曾和哈肯（W. Haken）合證四色定理。

由於文革的普遍影響，張益唐23歲才進北大唸書，碩士班的導師是潘成彪，是班上頭角崢嶸的學生。1985年赴美在普渡大學讀博士班，論文指導老師是來自臺灣的莫宗堅。但張益唐撰寫論文的過程並不順遂，七年後才通過口試。

1991年畢業之後，他一直無法找到學術工作，據說曾經當過多年會計、餐館外送。最後在1999年，才由他北大的學弟、任教於新罕布夏大學的葛力明，在美國南方一家Subway潛艇堡店將他「救」了回來，擔任系上助教，並在2005年升任講師。

這段懷才不遇的罕見際遇，結合長年懸宕的知名數學難題，讓中西媒體爲之瘋狂。許多人剛開始把他當作素人數學家，懷疑他證明的正確性，逼得他只好提出通過期刊審查的信件來證明。但看過他證明的數學家，都確認他的文章寫得清晰明白、無懈可擊。

他普渡時期的臺灣同學說，張益唐爲人沉靜害羞。即使在這段失意的歲月，仍然潛心於數學。尤其是新罕布夏大學的學生對他的教學讚譽有加（在華人數學家算是少見），更讓人體認到他落落大方的學術個性。張益唐告訴訪問他的美國記者，自己對至今黯淡的學術生涯並無怨懟，名利如浮雲，他的心很平和，只想繼續安靜研究。

個人的修養可以坦然面對失落的黃金二十年，但這段故事仍然讓人心生感慨與警惕。在張益唐證明了質數並不孤獨之後，我們祝福他在數學上也不再孤獨。

編輯室

新一，這次要破解的是ABC之謎

孤獨數學家又一則

這裡的ABC之謎不是神探白羅手上的謀殺案，新一也不姓工藤，他叫望月新一，是京都大學數理解析研究所（RIMS）的教授。2012年8月，他在自己的網頁放了四篇論文，聲稱證明了ABC猜想。

ABC猜想是數論的知名猜想，可以導出費馬最後定理、摩岱爾猜想（Mordell conjecture）及許多數論猜想。懷爾斯(A. Wiles)十年磨一劍證明費馬最後定理的故事膾炙人口。法亭斯（G. Faltings）則因證明摩岱爾猜想獲得1986年費爾茲獎。由此可知ABC猜想的重要性與困難程度。

不過這個事件成爲去年最知名的數學新聞還別有原因。原來望月的論文不止局外人摸不著邊際，甚至連當行的專家也讀不懂。堪稱爲「望月流」的數學世界，籠罩抽象的文字障，是他多年苦心孤詣的擘築，被戲稱爲「來自未來的數學」。

不過望月的背景絕不容人忽視他的證明。他16歲進入普林斯頓大學，23歲拿到數學博士。弦論大師韋頓（E. Witten）曾指導他的大學論文，法亭斯更是他博士論文的指導教授。仔細瀏覽望月的網頁，看得出他是行事正常的數學家，甚至清楚記錄自己寫作的心路歷程，這四篇他費時十年構思完成的偉文，其中種種轉折，都可以從網路上讀到。

相對於隱然成風的「孤獨數學家」現象，望月提供另一種模式，肇因於他學術天地與數學社群的鴻溝。一般認定邏輯正確即爲眞，但是如果由於語言的障礙，缺乏數學同儕的審核，這些論文還是「正確」的嗎？我們如何面對無法審查的正確證明呢？

望月在網頁放了有心解釋論文結構的「小論文」，至少他有自信看待自己的結果，數學界也不乏有興趣理解這個證明的人。也許雙方終究有辦法跨出這個難局。

編輯室

「安全性證明」不保證安全

密碼學不僅應用於軍事，在現今網路環境已經深入日常生活。每天打開電腦或智慧型手機，瀏覽器自動以公鑰（public-key）密碼系統驗證網站。若需登入帳戶、進行轉帳或購物，則通訊與儲存設備再以對稱式加密、數位簽章、雜湊函數等各式密碼演算法與協定來保障資訊安全。

密碼學牽涉電機、資訊、數學三大領域。以晶片等硬體實作演算法，需電機背景；寫程式實現密碼的則需資訊人才。推導演算法的複雜度，亦屬資訊領域的計算理論。除了破解或分析密碼演算法，需機率統計及較深的抽象代數外，全世界廣泛使用的密碼系統，大量使用了下述代數工具。

先進加密標準（AES）是對稱式，將位元組視爲有限體 GF(2^8) 的元素，加解密均操作加法、乘法、與乘法反元素。美國國家安全局規定AES必須搭配迦羅瓦計數模式，運算 GF(2^{128}) 加法與乘法，保護政府敏感文件的完整與可鑑別。

RSA公鑰應用初等數論，安全性基於因數分解的計算困難度；橢圓曲線密碼（ECC）安全性基於橢圓曲線群上離散對數問題的困難度。近年美國國家安全局與北約組織逐漸淘汰RSA，分別以建構於384與256位元質數體 p 上的ECC，對政府極機密和機密文件的傳遞，進行密鑰協議與數位簽章。

橢圓曲線的研究超過150年，內涵豐富；柯博立茨（N. Koblitz）引入橢圓曲線，對現代密碼學有直接貢獻。柯博立茨出身數學，所受訓練與資訊或電機學者不同，一起投入密碼學研究，難免於論證嚴謹度或思考模式產生分歧，因而出現柯博立茨在 *Notices* 撰文批評部分理論密碼學研究，被指名道姓者紛紛反擊的衝突。

2007年9月柯博立茨文章前段，敘述密碼學自1970年代快速進展以來，數學的有趣應用及諸多良性互動。例如爲了隨機生成安全的橢圓曲線（群階最好是夠大的質數），必須研發快速計算群階的演算法。最初有修夫（R. Schoof）使用特定多項式的算則，新方法則利用模形式與 p 進（p-adic）技術（臺灣也有數學系學生寫程式實作並移交政府運用）。接著柯博立茨話鋒一轉，開始批評令人不滿的現狀，尤其是研究安全性證明（proof of security）的新興子領域「可證明安全性（provable security）」。

提出新密碼演算法或協定，若能證明「破解它」和「解決一項公認的計算難題」難度等價，是最理想的。例如已嚴格證明「破解拉賓（Rabin）公鑰密碼系統等價於因數分解」，因此學界對拉賓公鑰的信任甚於RSA。但欲證明這種等價關係通常極困難，導致安全性證明最常見論述是「若Y是計算難題，則系統可抵擋X類型攻擊」；論證工具來自計算複雜度理論的歸約（reduction）概念，以及數學模型的建立與演繹。

顯然，此類論述無法充分保障安全性，因爲

+ 新出現的Y不見得眞的是計算難題，或許認眞研究後就被解決了。
+ 雖然X類型攻擊無效，但另一攻擊可能奏效。

柯博立茨認爲這些論文，「定理」和「證明」的寫法太氾濫，容易誤導非專業人士產生不切實際的過度信任。至今有一些宣稱具備安全性證明的系統已經被攻破，讓不少學者也感到不安。*Notices* 2010年又刊登一篇柯博立茨的文章，指出基於不穩固假設所推導的安全性證明，將使得若干著名密碼協定暴露於風險中。

圖靈獎是資訊科學界的最高榮譽，2012年頒給密卡力（S. Micali）和郭德瓦瑟（S. Goldwasser），表彰兩位麻省理工學院教授在「可證明安全性」的先驅研究。在「安全性證明不能保證安全」的亂象消失前，是否適合如此頒發大獎？密碼學界部分學者對2012圖靈獎頗不以爲然。

無論如何，在這個子領域發展成熟前，許多專家的看法傾向「雖然不能因爲它有『安全性證明』就信任其安全性，但有證明總比沒有好。」

編輯室

2013年阿貝爾獎與沃爾夫獎

兼談數學界的諾貝爾獎

一般人知道的數學諾貝爾獎是國際數學聯盟頒發的費爾茲獎，這是數學家的桂冠。但是費爾茲獎和諾貝爾獎有根本的不同。

諾貝爾獎接近終生成就獎，但費爾茲獎只獎勵年齡不超過40歲的年輕數學家，這激勵了許多年輕人的鬥志，從得獎史也可以見到許多年輕的見證者。但這個條件也造成誤導，以爲數學家年齡一過四十就江郎才盡，和實情相去甚遠。

其次是獎金。費爾茲獎的獎金是15,000美金，諾貝爾獎依最近的行情則是得獎者合得約1,200,000美金。雖然「富貴非所求」是好事，不過這也加強費爾茲獎是年輕人獎的印象，不足以彰顯得獎人成就之偉大。還有一個差別是頒發的時間，費爾茲獎配合國際數學家大會四年一頒，而諾貝爾獎則是年年頒獎，大大增加了該獎的媒體能見度。

因此有很長的時間，足以媲美諾貝爾獎的數學獎，除了費爾茲獎之外，一般認爲就是由沃爾夫基金會頒發的沃爾夫獎。沃爾夫獎沒有年齡限制，涵蓋了農業、化學、數學、醫學、物理、藝術六大領域，的確有第二諾貝爾獎的架勢，也是數學界受人矚目的大獎。

不過沃爾夫獎號稱每年頒發，但卻常有變動（進入21世紀，就有兩次兩年合頒，三次從缺），獎金100,000美金，遠高於費爾茲獎，但是仍遠低於諾貝爾獎。再加上物理、化學不但有沃爾夫獎，還有諾貝爾獎，感覺上數學比別人矮了個頭。這些都讓人期待眞正的數學諾貝爾獎。

有趣的是早在19世紀末，挪威數學家李（S. Lie）就曾經因爲諾貝爾獎獨缺數學，倡議設立阿貝爾獎，一方面慶祝挪威數學家阿貝爾（N. Abel）1902年的百年誕辰，並可做爲數學的諾貝爾獎。可惜這項計畫雖然獲得挪威王室的支持，卻在1899年李過世後胎死腹中。

結果在千禧年與阿貝爾兩百年誕辰的雙喜時刻，2001年挪威政府重提此議，決定設立數學家專屬的阿貝爾獎。阿貝爾獎的格局和諾貝爾獎相當，目標放在獎勵長年與跨領域的研究者，每年一頒，獎金高達1,000,000美金。2003年第一屆得獎者是塞爾（J.-P. Serre），他將在七月來臺參加世界華人數學家大會。

今年的阿貝爾獎和沃爾夫獎都已經宣布。阿貝爾獎2013年的得主是普林斯頓高等研究院的比利時數學家德利涅（P. Deligne）。而沃爾夫獎的共同得主是美國數學家耶魯大學的莫司特（G. Mostow）與麻省理工學院的亞丁（M. Artin）。

德利涅是代數幾何大師格羅騰迪克（A. Grothendieck）的傑出弟子，也是新代數幾何的宗師。他完成格羅騰迪克未竟之志，完整證明了跨越幾何和數論的威伊猜想（Weil conjecture）中最深刻的部分，他因此獲得1978年費爾茲獎，並成爲法國高等科學研究院（IHÉS）最年輕的終身成員。之後他仍然持續研究代數幾何、數論、表現論等深刻議題。

莫司特最知名的貢獻是他的剛性定理（rigidity theorem），證明了維度大於2的閉雙曲流形，其幾何性質由其基本群所決定，建立了拓樸與幾何的深刻關係。他的「無窮遠作用」觀點，影響了許多數學領域的發展包括微分幾何、低維拓樸與克萊恩群、幾何群論。另外他曾經與德利涅合作研究低維複雙曲空間的非算術格理論。

亞丁和德利涅一樣，都是格羅騰迪克學派的大將，新代數幾何的大師。他和格羅騰迪克共同發展的平展上同調理論（étale cohomology）是代數幾何的基本工具。另外他發展了代數空間、代數堆（algebraic stack）與變形理論，成爲探討代數幾何模空間與相交理論的根本概念，其中包括他知名的「逼近定理」與「存在性定理」。

關於亞丁、德利涅、格羅騰迪克的故事可以參看本期86頁〈宛如來自空無的召喚〉。

編輯室

數不再孤獨，而是張益唐的傳奇際遇。

張益唐今年大約58歲，目前的職銜是新罕布夏大學數學統計系的講師。除了2001年在 *Duke Journal* 發表過一篇文章，他幾乎可說是名不見經傳。新罕布夏大學也非美國的名校，系上最知名的老師應該是剛過世的阿培爾（K. Appel），他曾和哈肯（W. Haken）合證四色定理。

由於文革的普遍影響，張益唐23歲才進北大唸書，碩士班的導師是潘成彪，是班上頭角崢嶸的學生。1985年赴美在普渡大學讀博士班，論文指導老師是來自臺灣的莫宗堅。但張益唐撰寫論文的過程並不順遂，七年後才通過口試。

1991年畢業之後，他一直無法找到學術工作，據說曾經當過多年會計、餐館外送。最後在1999年，才由他北大的學弟、任教於新罕布夏大學的葛力明，在美國南方一家Subway潛艇堡店將他「救」了回來，擔任系上助教，並在2005年升任講師。

這段懷才不遇的罕見際遇，結合長年懸宕的知名數學難題，讓中西媒體爲之瘋狂。許多人剛開始把他當作素人數學家，懷疑他證明的正確性，逼得他只好提出通過期刊審查的信件來證明。但看過他證明的數學家，都確認他的文章寫得清晰明白、無懈可擊。

他普渡時期的臺灣同學說，張益唐爲人沉靜害羞。即使在這段失意的歲月，仍然潛心於數學。尤其是新罕布夏大學的學生對他的教學讚譽有加（在華人數學家算是少見），更讓人體認到他落落大方的學術個性。張益唐告訴訪問他的美國記者，自己對至今黯淡的學術生涯並無怨懟，名利如浮雲，他的心很平和，只想繼續安靜研究。

個人的修養可以坦然面對失落的黃金二十年，但這段故事仍然讓人心生感慨與警惕。在張益唐證明了質數並不孤獨之後，我們祝福他在數學上也不再孤獨。

編輯室

新一，這次要破解的是ABC之謎

孤獨數學家又一則

這裡的ABC之謎不是神探白羅手上的謀殺案，新一也不姓工藤，他叫望月新一，是京都大學數理解析研究所（RIMS）的教授。2012年8月，他在自己的網頁放了四篇論文，聲稱證明了ABC猜想。

ABC猜想是數論的知名猜想，可以導出費馬最後定理、摩岱爾猜想（Mordell conjecture）及許多數論猜想。懷爾斯(A. Wiles)十年磨一劍證明費馬最後定理的故事膾炙人口。法亭斯（G. Faltings）則因證明摩岱爾猜想獲得1986年費爾茲獎。由此可知ABC猜想的重要性與困難程度。

不過這個事件成爲去年最知名的數學新聞還別有原因。原來望月的論文不止局外人摸不著邊際，甚至連當行的專家也讀不懂。堪稱爲「望月流」的數學世界，籠罩抽象的文字障，是他多年苦心孤詣的擘築，被戲稱爲「來自未來的數學」。

不過望月的背景絕不容人忽視他的證明。他16歲進入普林斯頓大學，23歲拿到數學博士。弦論大師韋頓（E. Witten）曾指導他的大學論文，法亭斯更是他博士論文的指導教授。仔細瀏覽望月的網頁，看得出他是行事正常的數學家，甚至清楚記錄自己寫作的心路歷程，這四篇他費時十年構思完成的偉文，其中種種轉折，都可以從網路上讀到。

相對於隱然成風的「孤獨數學家」現象，望月提供另一種模式，肇因於他學術天地與數學社群的鴻溝。一般認定邏輯正確即爲眞，但是如果由於語言的障礙，缺乏數學同儕的審核，這些論文還是「正確」的嗎？我們如何面對無法審查的正確證明呢？

望月在網頁放了有心解釋論文結構的「小論文」，至少他有自信看待自己的結果，數學界也不乏有興趣理解這個證明的人。也許雙方終究有辦法跨出這個難局。

編輯室

「安全性證明」不保證安全

密碼學不僅應用於軍事，在現今網路環境已經深入日常生活。每天打開電腦或智慧型手機，瀏覽器自動以公鑰（public-key）密碼系統驗證網站。若需登入帳戶、進行轉帳或購物，則通訊與儲存設備再以對稱式加密、數位簽章、雜湊函數等各式密碼演算法與協定來保障資訊安全。

密碼學牽涉電機、資訊、數學三大領域。以晶片等硬體實作演算法，需電機背景；寫程式實現密碼的則需資訊人才。推導演算法的複雜度，亦屬資訊領域的計算理論。除了破解或分析密碼演算法，需機率統計及較深的抽象代數外，全世界廣泛使用的密碼系統，大量使用了下述代數工具。

先進加密標準（AES）是對稱式，將位元組視爲有限體 GF(2^8) 的元素，加解密均操作加法、乘法、與乘法反元素。美國國家安全局規定AES必須搭配迦羅瓦計數模式，運算 GF(2^{128}) 加法與乘法，保護政府敏感文件的完整與可鑑別。

RSA公鑰應用初等數論，安全性基於因數分解的計算困難度；橢圓曲線密碼（ECC）安全性基於橢圓曲線群上離散對數問題的困難度。近年美國國家安全局與北約組織逐漸淘汰RSA，分別以建構於384與256位元質數體 p 上的ECC，對政府極機密和機密文件的傳遞，進行密鑰協議與數位簽章。

橢圓曲線的研究超過150年，內涵豐富；柯博立茨（N. Koblitz）引入橢圓曲線，對現代密碼學有直接貢獻。柯博立茨出身數學，所受訓練與資訊或電機學者不同，一起投入密碼學研究，難免於論證嚴謹度或思考模式產生分歧，因而出現柯博立茨在 *Notices* 撰文批評部分理論密碼學研究，被指名道姓者紛紛反擊的衝突。

2007年9月柯博立茨文章前段，敘述密碼學自1970年代快速進展以來，數學的有趣應用及諸多良性互動。例如爲了隨機生成安全的橢圓曲線（群階最好是夠大的質數），必須研發快速計算群階的演算法。最初有修夫（R. Schoof）使用特定多項式的算則，新方法則利用模形式與 p 進（p-adic）技術（臺灣也有數學系學生寫程式實作並移交政府運用）。接著柯博立茨話鋒一轉，開始批評令人不滿的現狀，尤其是研究安全性證明（proof of security）的新興子領域「可證明安全性（provable security）」。

提出新密碼演算法或協定，若能證明「破解它」和「解決一項公認的計算難題」難度等價，是最理想的。例如已嚴格證明「破解拉賓（Rabin）公鑰密碼系統等價於因數分解」，因此學界對拉賓公鑰的信任甚於RSA。但欲證明這種等價關係通常極困難，導致安全性證明最常見論述是「若Y是計算難題，則系統可抵擋X類型攻擊」；論證工具來自計算複雜度理論的歸約（reduction）概念，以及數學模型的建立與演繹。

顯然，此類論述無法充分保障安全性，因爲

+ 新出現的Y不見得眞的是計算難題，或許認眞研究後就被解決了。
+ 雖然X類型攻擊無效，但另一攻擊可能奏效。

柯博立茨認爲這些論文，「定理」和「證明」的寫法太氾濫，容易誤導非專業人士產生不切實際的過度信任。至今有一些宣稱具備安全性證明的系統已經被攻破，讓不少學者也感到不安。*Notices* 2010年又刊登一篇柯博立茨的文章，指出基於不穩固假設所推導的安全性證明，將使得若干著名密碼協定暴露於風險中。

圖靈獎是資訊科學界的最高榮譽，2012年頒給密卡力（S. Micali）和郭德瓦瑟（S. Goldwasser），表彰兩位麻省理工學院教授在「可證明安全性」的先驅研究。在「安全性證明不能保證安全」的亂象消失前，是否適合如此頒發大獎？密碼學界部分學者對2012圖靈獎頗不以爲然。

無論如何，在這個子領域發展成熟前，許多專家的看法傾向「雖然不能因爲它有『安全性證明』就信任其安全性，但有證明總比沒有好。」

編輯室

2013年阿貝爾獎與沃爾夫獎

兼談數學界的諾貝爾獎

一般人知道的數學諾貝爾獎是國際數學聯盟頒發的費爾茲獎，這是數學家的桂冠。但是費爾茲獎和諾貝爾獎有根本的不同。

諾貝爾獎接近終生成就獎，但費爾茲獎只獎勵年齡不超過40歲的年輕數學家，這激勵了許多年輕人的鬥志，從得獎史也可以見到許多年輕的見證者。但這個條件也造成誤導，以爲數學家年齡一過四十就江郎才盡，和實情相去甚遠。

其次是獎金。費爾茲獎的獎金是15,000美金，諾貝爾獎依最近的行情則是得獎者合得約1,200,000美金。雖然「富貴非所求」是好事，不過這也加強費爾茲獎是年輕人獎的印象，不足以彰顯得獎人成就之偉大。還有一個差別是頒發的時間，費爾茲獎配合國際數學家大會四年一頒，而諾貝爾獎則是年年頒獎，大大增加了該獎的媒體能見度。

因此有很長的時間，足以媲美諾貝爾獎的數學獎，除了費爾茲獎之外，一般認爲就是由沃爾夫基金會頒發的沃爾夫獎。沃爾夫獎沒有年齡限制，涵蓋了農業、化學、數學、醫學、物理、藝術六大領域，的確有第二諾貝爾獎的架勢，也是數學界受人矚目的大獎。

不過沃爾夫獎號稱每年頒發，但卻常有變動（進入21世紀，就有兩次兩年合頒，三次從缺），獎金100,000美金，遠高於費爾茲獎，但是仍遠低於諾貝爾獎。再加上物理、化學不但有沃爾夫獎，還有諾貝爾獎，感覺上數學比別人矮了個頭。這些都讓人期待眞正的數學諾貝爾獎。

有趣的是早在19世紀末，挪威數學家李（S. Lie）就曾經因爲諾貝爾獎獨缺數學，倡議設立阿貝爾獎，一方面慶祝挪威數學家阿貝爾（N. Abel）1902年的百年誕辰，並可做爲數學的諾貝爾獎。可惜這項計畫雖然獲得挪威王室的支持，卻在1899年李過世後胎死腹中。

結果在千禧年與阿貝爾兩百年誕辰的雙喜時刻，2001年挪威政府重提此議，決定設立數學家專屬的阿貝爾獎。阿貝爾獎的格局和諾貝爾獎相當，目標放在獎勵長年與跨領域的研究者，每年一頒，獎金高達1,000,000美金。2003年第一屆得獎者是塞爾（J.-P. Serre），他將在七月來臺參加世界華人數學家大會。

今年的阿貝爾獎和沃爾夫獎都已經宣布。阿貝爾獎2013年的得主是普林斯頓高等研究院的比利時數學家德利涅（P. Deligne）。而沃爾夫獎的共同得主是美國數學家耶魯大學的莫司特（G. Mostow）與麻省理工學院的亞丁（M. Artin）。

德利涅是代數幾何大師格羅騰迪克（A. Grothendieck）的傑出弟子，也是新代數幾何的宗師。他完成格羅騰迪克未竟之志，完整證明了跨越幾何和數論的威伊猜想（Weil conjecture）中最深刻的部分，他因此獲得1978年費爾茲獎，並成爲法國高等科學研究院（IHÉS）最年輕的終身成員。之後他仍然持續研究代數幾何、數論、表現論等深刻議題。

莫司特最知名的貢獻是他的剛性定理（rigidity theorem），證明了維度大於2的閉雙曲流形，其幾何性質由其基本群所決定，建立了拓樸與幾何的深刻關係。他的「無窮遠作用」觀點，影響了許多數學領域的發展包括微分幾何、低維拓樸與克萊恩群、幾何群論。另外他曾經與德利涅合作研究低維複雙曲空間的非算術格理論。

亞丁和德利涅一樣，都是格羅騰迪克學派的大將，新代數幾何的大師。他和格羅騰迪克共同發展的平展上同調理論（étale cohomology）是代數幾何的基本工具。另外他發展了代數空間、代數堆（algebraic stack）與變形理論，成爲探討代數幾何模空間與相交理論的根本概念，其中包括他知名的「逼近定理」與「存在性定理」。

關於亞丁、德利涅、格羅騰迪克的故事可以參看本期86頁〈宛如來自空無的召喚〉。

編輯室