十二年國教，高中數學腰斬

2 月 10 日，國家教育研究院主導訂定的十二年國教總綱草案終於出爐，隨即在臺灣數學界投下震撼彈。

數學號稱是國家科學與科技發展的基本工具，但總綱小組在沒有數學界參與的情況下，閉門造出令人驚訝的結果。前國科會科教處處長林福來指出：「本來高中數學從高一到高三每學期 4 學分，共 24 學分。現在總綱明載只剩高一到高二，每學期 3 學分，共 12 學分，整個腰斬 50%。」

但是大學端並沒有課程異動的可能，24 個數學學分的內容也不可能濃縮成 12 個學分，因此直接受害的就是運用數學工具的大學科系。中華民國數學會前理事長張鎮華說：「大學生的數學程度已經日漸低落，現在更是雪上加霜，令人無法再容忍。」

總綱小組打的如意算盤是準備大力推行揚才適性的選修課程。他們認為只要高中開出恰當的選修課程，學生「理論」上還是可以學到恰當的數學內容。

2 月 27 日中研院院士林長壽在《中國時報》發表〈十二年國教的矛盾與綱要理念的迷失〉指出「在臺灣考試影響課程進行至巨，如今總綱不談大學考試與十二年國教如何接軌，不要求大學端入學考試的改革，反而讓高三課程規劃一片空白，令人憂心日後如何與大學入學做合理的銜接。」

中華民國數學會理事長陳榮凱說：「所謂『國民基本教育』，必須保障學生學習足夠和基礎的知識，不管教育改革理念如何，必要的部分就必須明文刊列，這是常識。」令人好奇的是，這些選修課還需要綱要嗎？還有教科書嗎？大學入學怎麼辦？

熟悉臺灣教育生態的人都知道，沒有清楚的課綱做引導，高中現場根本開不出和大學接軌的數學選修課程，因此幾乎所有高中必然會回歸舊高中課綱與課本，教育部根本白忙一場。

但是放任高中開設選修課的訊息影響十分深遠，家長將對一般學校更失去信心，投入更多個人社經資源到孩子身上，像是轉讀私校、聘請家教、上補習班等，擴大貧富差距的影響，嚴重扭曲基本教育的公平性。

中央大學單維彰 3 月在《科學月刊》的專欄〈數學教育的罪與罰〉中指出，PISA 國際評量，已經把臺灣列為數學教育機會最不公平的國家。4 月，中研院英美研究所黃敏雄研究另一項國際學生成就測驗 TIMSS 的數據，也指出類似的現象。PISA 和 TIMSS 是測驗原理和目標很不一樣的兩項國際重要評量，卻不約而同得出相同結果，對臺灣是一項很大的警訊。

臺灣大學翁秉仁補充說：「最令人訝異的是總綱沒有改革九年一貫的缺失。國小與國中數學教學時數不足，早就是這幾年數學教育界以及現場老師的共識。總綱整個反向操作，對弱勢家庭的影響，難以想像。」

3 月初，中華民國數學會提出《十二年國民基本教育中數學課程的主張》寄給國教院，林長壽和同事更當面向教育部長蔣偉寧指陳缺失，獲得保證處理之回應。4 月 22 日，成功大學理學院院長柯文峰發動校內連署，呼應數學會的主張，一星期內便獲得 300 多位教師熱烈回應。

沒想到國教院 5 月 5 日開記者會，說明總綱修正草案高中數學必修仍維持 12 學分，只說明自然組學生如何在高中自訂之加深加廣選修數學課程補足 24 學分，究其實質，和 2 月公布之草案完全沒有改變。

目前數學界已針對國教院的無感回應，積極擴大全國連署，至截稿日已約 3000 人。5 月 16 日，中華民國數學會與多位數學系主任召開媒體記者會，反對教育部總綱草案之修正案。痛陳總綱只顧理想、不顧現實與可行性的弊病，將導致大學的數學教育無法銜接。

此外，18 位中央研究院院士也隨後聯名發起院士連署，目前已有近百名中研院院士參與連署，並於 6 月 4 日召開記者會，宣告其共同主張為：每位高中學生每學期必修數學四學分；高中數學應規劃兩套課程綱要，供學生適性選擇；小學和國中每天應有一堂數學課；國家應積極建立長久性的師資再訓練制度，確保數學教學品質。

希望在這些壓力下，終能讓教育部懸崖勒馬。

編輯室

掃描數學家的腦

看到數學之美

數學美嗎？

許多人覺得你在開玩笑，數學無感的冰冷符號，怎麼可能比得上蘇打綠和吉米，或者莫札特和梵谷。

但是就算無緣見識數學老師眼中的熱情，書市幾年就會出本討論最美公式的科普書，網路上更不乏推薦最美公式的網頁、甚至排行榜。英國哲學家羅素甚至說：「從正確的角度觀視，數學不只真，而且極美。」

在聽音樂時，有人聆賞旋律直接的感動。但也有人殺風景，說如果會演奏樂器或讀懂樂譜，才真正理解音樂的美。這種觀點的極致體現，就是數學。數學的美必須伴隨著數學的理解。

例如歐拉的$e^{i\pi}+1=0$ 是公式排行榜的常勝軍。但是如果不知道這些符號的數學基本特性、不理解i、e、π的意義與重要性，或者不能體驗複數冪次的驚奇，就無法理解這個公式的美。而且隨著你愈清楚複數冪次在數學、量子力學、工程中的威力，就愈讚嘆這公式懾人之美。

數學的美，和音樂、繪畫的美是一樣的嗎？這個哲學問題在今年二月迎來一個科學答案。知名英國數學家阿提雅（Atiyah）和英國認知科學家在《人類神經科學前沿》期刊，發表了一篇論文〈數學美感經驗與其神經關連〉試圖回答這個問題。

倫敦大學的哲吉（S. Zeki）在過去幾年的實驗中，以功能性核磁共振造影（fMRI）證實，音樂、繪畫能夠激發腦部前眼窩前額皮質（mOFC）A1 區的「美感情緒」。因此他和合作者沿用過去的實驗方法，轉而針對數學的抽象理性之美（如果存在的話），探討這個問題。

但是比起音樂或繪畫，數學實在太高深了。於是這個實驗需要數學家提供被鑑賞的「作品」，需要數學家來受測，才能測試數學之美。阿提雅的任務就是提供 60 個包含許多領域的數學公式，當然這些可能不全是阿提雅心目中的重要公式。

受測的 16 位數學家都是倫敦大學研究所或博士後（有一人因服藥最後遭剔除）。在進行腦部掃描前，16 位受測人先在名為「數學之美：方程式」的問卷上，分別對 60 個公式打分數，從醜到美給出 -5 到 +5 的分數。研究者依據各人給分，客製四組公式做為腦部掃描的資料。每組 15 個公式美、中、醜各五，並交錯排列其順序，讓美感體驗不受無謂干擾。

兩個星期後等大家淡忘答案，16 位受測者到實驗室進行腦部掃描，他們分四階段看完自己的四組公式，並判斷見到的公式為美、中、醜。

幾天後受測者另填寫問卷，逐題回答對公式的理解（從不懂到非常懂，給 0 到 3 分）。另外再回答一些與實驗相關的問題。

論文中說明實驗分析的結果，顯示數學或抽象公式不但激發美感，而且它所觸發的仍然是 mOFC 的 A1 區，和藝術共享相同的美感情緒。這個初步的結果，將可以做為未來相關研究的基礎。

另外這個實驗也提供這些公式的數學家排行（很有限的代表性）。最高分果然是歐拉公式，最低分的醜公式則是拉曼努真的$1/\pi$公式：

$$\frac{1}{\pi}=\frac{2\sqrt{2}}{9801}\sum_{k=0}^{\infty}\frac{(4k)!(1103+26390k)}{(k!)^4 396^{4k}}$$

另外在試後問卷中，許多人抱怨某些美麗公式沒有出現，例如愛因斯坦方程、柯西積分公式、諾特守恆性定理等。受測人可能真以為自己在參與票選公式的活動吧。

這個實驗引發更多的問題，拉曼努真的公式被認為最醜令人意外（事實上另一個意外的醜公式是黎曼假說相關的泛函方程）。在數學中驚奇、難度、影響性、優雅、簡明都有可能造成美感。美比想像中複雜，並不是單純的愉悅即可，就像現代音樂、藝術電影也有小眾的美感，而且言人人殊。

美真的這麼簡單嗎？

編輯室

論文見 http://journal.frontiersin.org/Journal/10.3389/fnhum.2014.00068

外包給大眾做數學

小屁孩的玩意還是數學的未來

自然科學論文的作者一向很多，但沒有實驗室制度的數學界，論文作者通常都是小貓兩三隻。但近年網路興起，透過電子郵件與視訊，團隊合作的比例逐年增加。但到了 WEB2.0 甚至 3.0 的時代，大眾外包（crowdsourcing）的概念甚囂塵上，科技的進步是否終將改變數學研究的思考與研究方式呢？

2009 年 1 月，劍橋大學曾獲數學界最高榮譽費爾茲獎的高爾斯（T. Gowers），在部落格文章發起一項實驗——「多工數學計畫」（polymath project），目的是用嶄新的方式解決數學問題。他希望開放給全世界部落格讀者，藉由自發性網路合作來解決這個難題，並以多工數學部落格（polymath blog）及多工數學維基（polymath wiki）做短期的工作紀錄及評論，可以讓大眾見證或參與這段創作與發現的歷程。

結果六週問題就解決了。高爾斯將分散在幾百帖讀者回應裡的論證，綜合寫成一篇傳統論文，2009 年 10 月發表在網路論文集散站 arxiv.org，2012 年更正式刊於頂尖數學期刊 *Annals of Mathematics*。論文作者用的是筆名波里馬斯（D. H. J. Polymath），其中 D. H. J. 是定理名稱的縮寫。

不過，這個計畫真的外包給大眾了嗎？從結果看多少有點可疑，因為大部份的研究出自六個人，這些人都是職業數學家或匿名專家，其中還包括另一位費爾茲獎得主陶哲軒。這和透過電話或郵件的「傳統」方法有實質的差異嗎？

這個想法持續進行五年來，產生了九個多工數學計畫，有些成功，有的暫時停滯。這段過程逐漸讓參與者摸索出合作的模式。例如提案應簡短易懂、先備知識門檻低，而且適合多工合作，以擴大網眾的參與基礎；應提供可行的策略；不應與進行中的研究或博士論文題目重疊；計畫提案人應擔任執行及協調者的角色，敦促部落客以基本網路禮儀參與合作。另外，論文發表一律署名波里馬斯。

陶哲軒遺憾的指出，多工數學迄今的計畫皆屬數論與組合學，但強項在於能非常迅速的反應數學界發生的熱門事件。

2013 年 4 月，華人數學家張益唐證明有無窮多組質數對彼此距離不超過 70,000,000（見本刊上期專題）。陶哲軒隨即在同年 6 月 4 日啟動多工數學第八計畫（Polymath 8），希望了解並改進張益唐的估計手法（張益唐本人並未參與）。7 月 26 日，團隊便成功將距離降低到 4,680。2014 年 2 月，波里馬斯完成 163 頁的傳統論文，發表在 arxiv.org 並投稿到 *Algebra and Number Theory*。

2013 年 11 月，加拿大蒙特婁大學博士後研究員梅納德（J. Maynard）獨立將估計推進到不超過 600。多工數學 8b 計畫立即開展，希望結合張益唐與梅納德的方法將估計推到更小，這次梅納德決定參與。

根據陶哲軒 5 月 17 日的部落文，多工數學 8b 計畫即將收尾，準備整理發表，最新結果是波里馬斯已經將質數距離驚人的縮小到 246。透過部落格回應，也可以聽到參與人（包括梅納德）既興奮、但也疑惑該如何評價個人建樹的心聲。他們提醒有興趣參與的人，這不是數學家正常合作的模式。

數學界對多工數學意見分岐。普林斯頓高等研究院的沙納克（P. Sarnak）雖然致賀計畫成功，卻質疑研究數學的目標豈在最短時間內解答最多問題？他也對多工數學能否證明重要定理持保留態度，更質疑青年數學家一旦擁抱多人線上合作，將失去以獨自研究為數學帶來革命性改變的可能，最知名的例子是格羅騰迪克（A. Grothendieck）。沙納克的同事麥克弗森（R. MacPherson）則認為研究模式越多樣，對數學的發展越健康。

對於申請工作或晉職的年輕數學家，署名波里馬斯的論文應該如何計算學術貢獻呢？各數學系所可能要傷腦筋了。

編輯室

橢圓曲線：增強或減弱資訊安全的雙面刃

美國國家安全局 （NSA） 成立於冷戰時期，以保障政府通訊安全與國外情報蒐研為兩大職掌。雖然後來蘇聯解體，但像 911 事件的攻擊事件使得情蒐需求有增無減，而防止類似恐怖攻擊的最佳對策是「了解所有正發生的事情」。藉由「愛國者法案」的推波助瀾，NSA 廣募科技與數理人才，打造網路為監聽平台，企圖秘密監聽全世界。

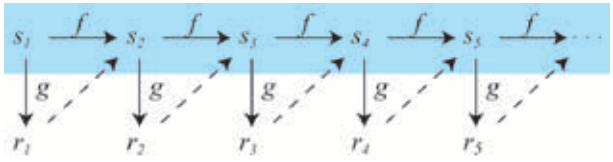
根據 2013 年史諾登 （Edward Snowden）向媒體揭露的文件，NSA 有數以百計的情蒐計畫代號，其中在學術界引起軒然大波的是 Bullrun 計畫。它在加密產品或相關演算法標準之中，植入僅 NSA 知道的後門 （backdoor），削弱安全強度，代表作是利用橢圓曲線產生亂數的 Dual_EC_DRBG，其中 EC 是橢圓曲線的簡寫。

2005 年美國的國家標準與技術研究所（NIST）公布 Dual_EC_DRBG 初稿，稍後成為國家與國際標準，RSA 公司與全球各地密碼產品相繼採用。2007 年微軟研究人員率先發現，Dual_EC_DRBG 有機會被暗藏後門。2013 年 9 月紐約時報更指出，NSA 確實掌握其後門。

亂數 （randomness，或稱「隨機數」） 在密碼學或維護資訊安全的系統中，角色舉足輕重；它產生加解密所需的密鑰 （secret key），並提供眾多其他用途。亂數值的產生若遭到成功預測，可能導致加密的文件被破解、網路上的身分或訊息來源被仿冒。

另一方面，橢圓曲線密碼 （ECC） 應用日趨廣泛，提供密鑰協議與數位簽章等功能。它的安全性建立在「離散對數問題」困難度上：給定一條「安全」曲線與其上兩點P與Q；欲解出t滿足$Q = tP$，所需複雜度超過2^{128}，計算上不可行。

亂數產生器的基本架構如圖示。Dual_EC_DRBG 以遞迴式 $s_{i+1} = f(s_i) = x(s_iP)$ 更新內部狀態，其中s_iP是橢圓曲線上固定點P的s_i倍，$x()$函數取其x坐



標。輸出函數$r_i = g(s_i) = x(s_iQ)$，外界不知Q是P的幾倍，無法經由曝光的r_i逆推得知內部狀態。NSA 曉得滿足$Q = tP$的t，可從r_i算出s_{i+1}，進而預測所有後續亂數。

雖然完整 Dual_EC_DRBG 較複雜，若能獲得連續 32 位元組 （byte） 輸出值，仍不難逆推取得內部狀態；但實務上發生機會極低，通常僅能獲得連續 16 位元組，無助於破密。再者，如果更換曲線，或不換曲線但更換曲線上的P或Q，皆可避開 NSA 預埋的後門。據知臺灣政府相關單位早已注意到它可能存在後門，並不在任何政府機敏通訊或儲存設備之中使用它。

另從分析史諾登文件可知：NSA 尚無法直接破解 ECC、RSA、AES 等主要密碼系統，破密仍然幾乎全部是從實作上的漏洞著手。因此，善用數學、適當加密，仍可讓全球頂尖情報機構一籌莫展。

倒是此事件，已經讓部分數學家質疑學術界和國安當局的恰當關係。曾經為 KGB 所苦的俄國數學家如芝加哥大學數學家貝林森（Beilinson）更激進的說，應該排除與 NSA 合作的數學家。

但是回到現實層次，在網路科技已如飲水的現在，各種層級的安全科技正像軍事競賽演進，國家為了保護公眾安全，勢必需要能掌握尖端數學家投身這一「戰場」。

總之，數學用在保密是好的，用在情報和國安所需之破密也很必要。但若用在大規模監聽無辜人民，就有違道德和憲法賦予的秘密通訊自由。所以問題在國安當局如何使用數學，不能一味指責合作的數學家。

國安與自由不是零和的關係，但是該怎麼取得平衡，可不像數學家的橢圓曲線那麼容易解決。

編輯室