數學=證明?

蕭文強

什麼叫做數學證明? 大家對此當不感陌生, 毋庸多說。判斷命題“若p則q”正確與否, 其間只靠基本概念 (定義)、基本假設 (公理) 及以前已經證實爲正確的命題 (定理) , 而且推論手法必須合乎邏輯, 這個過程就是數學證明。

讓我舉一個典型例子, 那也是一條既古老又重要的定理, 即是 EUCLID 的“ELEME- NTS” 卷一第 47 條命題: 在直角三角形兩邊上的正方的面積之和等於斜邊上的正方的面積。讀者對於書上的證明 (很多幾何課本上也可以找到), 大抵已是耳熟能詳, 不必在這兒重複了。據云英國十七世紀哲學家 HOBBES 某天在朋友書房裡看到案頭有本打開的書, 剛好是翻到這一頁。當時他已經四十歲, 從沒讀過幾何。他不經意地瞧了那頁一眼, 對自己說 :“那怎麼可能呢?”爲了滿足好奇心他便讀下去, 看它如何解釋。但書上的證明用了前面另一條定理, 於是他又翻看那一條定理, 看它如何解釋。那條定理的證明, 又用了再前面另一條定理, 於是他繼續翻查下去。如此這般, 費了半天工夫, 他終於看明白了 ,對第 47 條命題深信不疑, 就是這樣他愛上了幾何!

像 HOBBES 那樣爲了演繹推理而愛上數學的人大抵不多, 但以爲數學就是演繹推理及繁複計算因而對數學敬而遠之的卻大不乏人!勿論喜愛數學也好, 厭惡數學也好, 一般人對數學證明的看法, 基本上跟 HOBBES 的看法無異: 從基本假設出發, 按照邏輯手法嚴謹地推導出要證明的結論來。更而甚者, 有些人還把數學與證明等同起來: 數學=證明!

形成上述看法的主要影響, 來自本世紀初關於數學基礎的爭論, 特別是邏輯主義與形式主義的觀點。在這兒我不打算討論這方面的因由, 讓我們只看看一些有關的話:

A. N. WHITEHEAD (1898) “就其最廣泛的詞意來說, 數學是全部形式化、必要和演繹式的論證。”

B. RUSSELL(1903)“純粹數學就是以下這種形式的命題的集合:p蘊涵q(若p則q),p和q 都是命題。”

L. WITTGENSTEIN(1956)“數學是各式各樣的證明技巧。”

B. PEIRCE (1881)“數學是產生必要的結論的科學。”

不過話得說回來, 這些哲學觀點是爲了特定目標——數學的相容性, 或稱無矛盾性——

爲數學作爲一門學科而下的界定, 倒不一定表達持這種觀點的人對數學作爲一項活動的看法。但它帶來的影響, 卻似乎超越了純學術討論的範圍, 形成一種普遍的看法, 尋且使人連起初的特定目標也忘記了!很多人便以爲數學家的主要工作就是證明定理 ,而所謂證明就是指文章開首提到的演繹功夫。

其實, 如果說數學家的工作就是證明定理, 那就有如說文學家的工作就是寫句子、音樂家的工作就是填音符、美術家的工作就是繪圖著色。於是, 李白的詩只是字句的組合、貝多芬的交響曲只是音調的組合、齊白石的畫只是線條的組合!既然文學作品、音樂作品、美術作品有所謂意念、意境, 那麼爲何數學作品沒有呢? 數學作品的意念、意境, 即是所謂 "數學之美"。但這點只能由每人自己體會,"如人飲水, 冷暖自知", 我遠未臻此境界作深入的探討, 以下我只打算把數學視作一項活動, 討論一下"數學=證明?"這個問題。

● 先從歷史的角度去看, 讓我回到文章開首的例子。EUCLID 在 "ELEMENTS" 上的證明, 是現尙存的文獻上記載的第一個關於勾股定理的證明, 但那是否等於說數學家到了那個時候 (公元前四世紀) 才懂得這個結果呢?

美國哥倫比亞大學博物館保存著一塊泥板, 稱作 PLIMTON 322, 估計書於公元前十九世紀左右的巴比倫時代, 較諸 "ELEMENTS" 早了一千五百多年。在1943年的博物館目錄上, 這塊刻了好幾行數字的泥板被列作"商業賬目", 但過了兩年後, 著名數學史家 NEUGEBAUER 和 SACHS 宣佈他們的驚人發現, 原來那幾行數字竟然是一系列的勾股數, 就是說三條邊都取整數值的直角三角形的邊長, 叫作 h、b、d, 其中$h^2+b^2=d^2$。泥板上只刻了b和d 的值, 並沒有h的值, 但最左邊那行卻刻了$(d/h)^2$ 的值, 而且每兩個相連的數相差約爲 0.03 (見圖1)。當你讀到像第四列那三個數 (13500,12709 ,18541) 的時候, 你還會認爲古代巴比倫人不懂勾股定理而僅憑摸索得到那些數據嗎?

$(d/h)^2$	h	b	d
1.9834027	120	119	169
1.9491585	3456	3367	11521(4825)
1.9188021	4800	4601	6649
1.8862478	13500	12709	18541
1.8150076	72	65	97
1.7851928	360	319	481
1.7199836	2700	2291	3541
1.6927093	960	799	1249
1.6426694	600	541(481)	769
1.5861225	6480	4961	8161
1.5625000	60	45	75
1.4894168	2400	1679	2929
1.4500173	240	25921(161)	289
1.4302388	2700	1771	3229
1.3871604	90	56	53(106)

圖1

又譬如看看我國古代文獻周髀算經(約成書於公元前一世紀), 裡面有說:"以爲勾廣三、股修四、徑隅五。既方之外, 半其一矩, 環而共盤, 得成三四五, 兩矩共長二十有五, 是謂積矩。··· 勾股各自乘, 並而開方除之。"它的意思可能是運用拼湊法給出一個勾股定理

的證明 (我是從李國偉先生學過來的): 把直角三角形環繞斜邊上的正方形的中心旋轉, 盤成四個 (見圖2), 不難見到

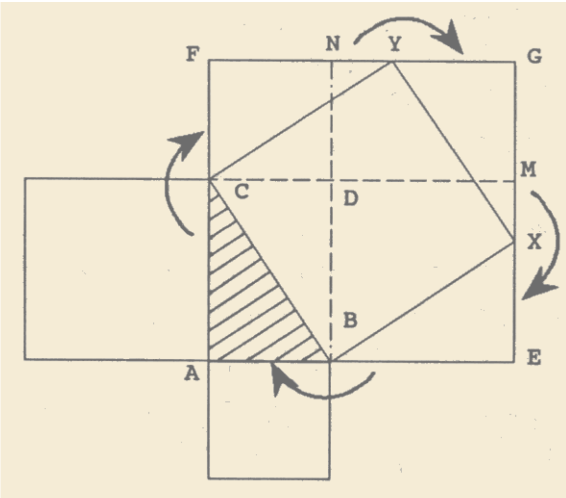

圖2

$$\square AFGE = \square CDNF + \square BEMD + 2\times\square ABDC$$

和

$$\square AFGE = \square BXYC + 4\times\triangle ABC$$

由此得到 AB 上的正方 $+AC$ 上的正方 $=BC$ 上的正方。

三國時吳人趙爽註周髀算經 提出了一個“勾股圓方圖”, 也用了拼湊法(見圖3a)。

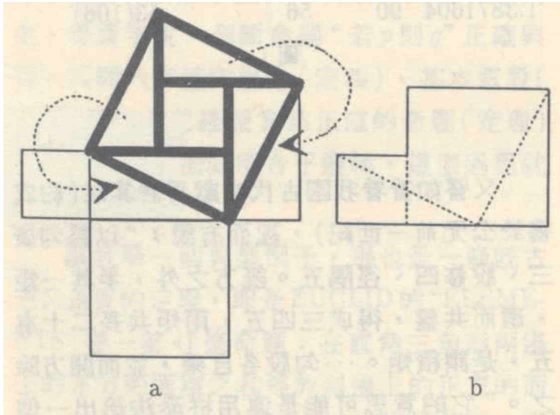

圖3

相同的圖也見諸於十二世紀印度數學家 BHA- SKARA 的著述 (見圖3b), 只是書上除圖以外單寫了一句“看呀!”。這些證明, 跟“ELEMENTS”卷一記載的的那個並不相同。

看來, 勾股定理包含的知識, 並不始於 EUCLID 的證明, 也不終結於 EUCLID 的證明。反過來說, 當人們掌握了這條定理的內容, 他們才逐漸找到嚴格的證明。類似的事例, 在數學史上屢見不鮮, 微積分的發展過程便是一個典型的例子。難怪十九世紀英國數學家 DEMORGAN 甚至說過:“數學的原動力是想像力而不是推理”。

● 為什麼人們相信未經嚴格證明的定理呢?

固然, 有些命題叫人一見到便深信不疑。例如: 三角形的兩條垂線必相交於一點; 兩實數的平方和不小於零; 對頂角相等; 空間兩直線同時與另一直線平行, 則該兩直線亦平行。也有些命題雖然不如上述那種命題那麼明顯, 但憑著足夠的觀察或試驗, 仍能入信。例如: 三角形的三條垂線共點; 兩實數的平方和不小於二乘它們的積。還有些命題, 雖看似抽

象, 但由於它有合理的物理意義, 也能使人入信。例如: 導數處處是零的函數是常數函數, 它的物理詮譯就是速度是零的點是不動點!但有更大一類的命題, 並不是有如上述的三種, 不靠證明又憑什麼教人相信它們呢?

不明顯的定理也有其由來, 往往某些側面的支持論據具有頗強的說服力。讓我只舉一個較容易敍述的例子, 讀者只用知道質數是什麼便成。質數的出現好像雜亂無章, 譬如問: 從 A 至 B, 質數在那兒出現? 有多少個? 出現的質數每兩個相隔多遠? 且看一些例子。從 0 至 99 這一百個整數中, 有二十五個質數, 其中八對僅相隔 1; 從 9,999,900 至 10,000,000 這一百個數中, 有九個質數, 其中兩對僅相隔 1; 但從 10,000,000 至 10,000,100 這一百個數中, 卻只有兩個質數, 它們相隔五十九。看似雜亂無章的質數分佈, 原來蘊藏著內裡玄機!十八世紀後期和十九世紀初期有些數學家 (如 LEGENDRE、GAUSS) 便看出苗頭來。讓我們也試觀察一些數據 (見圖 4), $\pi(N)$表示從 1 至 N 裡面質數的個數,

N	$\pi(N)$	$\pi(N)/N$
10	4	0.4
10^2	25	0.25
10^3	168	0.168
10^4	1229	0.1229
10^5	9592	0.09592
10^6	78498	0.078498
10^7	664577	0.0664577
10^8	5761455	0.05761455
10^9	50847354	0.050847354
10^{10}	455052512	0.0455052512

圖4

最右邊一列的 $\pi(N)/N$便表示質數密度了。把最右邊一列的數各乘以 1、2、3、4 $\cdots$ (亦即是 $\log N$), 得來的答案差不多都是一個在 0.4 至 0.5 之間的數, 而且趨勢是越來越接近某個常數 c。可以說 $\pi(N)/N \times \log N \sim c$, 或 $\pi(N) \sim c \times N/\log N$。置$c = \log e$, 便得 $\pi(N) \sim N/\log_e N$。從 c 的值推算 e 的值, 得 $e = 2.7182\cdots$, 就是今天我們熟悉的自然對數的基,$\log_e N$ 即是 N 的自然對數值了。這個猜測直至十九世紀最後幾年才給證明了, 叫做質數定理。既然我們對質數找不出局部規律, 卻找出如此優美整潔的全局分佈規律, 不如索性就當作質數按照這個頻率隨機地出現吧!意思是說: 擲一枚不均勻的銅板 N 次, 擲得人像的機率是 $1/\log_e N$,N 次中第 k 次擲得人像那一面表示 k 是個質數, 反之 k 是合成數。(嚴格地說, 這當然是荒謬的!k 只能是質數或合成數, 豈能憑擲銅板左右這個事實呢? 但請讀者忍耐一下讀下去吧。) 除 2 不計, 其餘質數都是奇

數, 相隔至少是1。相隔是1的一對質數叫做孿生質數, 例如3和5、5和7、11和13等等。關於孿生質數有一個著名的猜想: 有無窮多對孿生質數 (質數的分佈可非越來越疏)。讓我們用剛才擲銅板 的比喻揣摩一下這回事。我們問: 從1至 N 中兩個相隔是1的數都是質數的機會有多大? 或者說, 第 k 次和第 $k+2$ 次都擲得人像的機率是什麼? 粗略計算, 那是 $(1/\log_e N)^2$, 因此從1至 N中期望有 $N/(\log_e N)^2$ 對孿生質數。由於第 k 次擲得人像 (k 是質數) 和第 $k+2$ 次擲得人像 ($k+2$ 是質數) 並非眞正乃獨立事件, 計算機率時需要作些調整, 較精確的答案是$(1.32\cdots)\times N/\log_e N$ (細節略去)。利用這個式計算孿生質數對的個數, 對照眞正的答案 ,差別是非常微小 (見圖5)。這種叫人吃驚的吻合, 令人相信孿生質數對的分佈, 眞的有如以上所描述一般, 雖然還沒有人能證明該式是正確的!當 N 趨大時, $N/(\log_e N)^2$ 也趨大, 若分佈規律沒有錯, 那便證明了孿生質數猜想。

區間	孿生質數對個數	估計答案
10^9 至$10^9+150,000$	466	461
10^{10}至$10^{10}+150,000$	389	374
10^{11}至$10^{11}+150,000$	276	309
10^{12}至$10^{12}+150,000$	276	259
10^{13}至$10^{13}+150,000$	208	221
10^{14}至$10^{14}+150,000$	186	191
10^{15}至$10^{15}+150,000$	161	166

圖5

● 既然已經有很多證據支持命題, 爲何還得證明它呢?

不單一般人難以理解數學家對證明的重視程度, 即使別的科學家對這點有時也難以理解。數學家 HARISH-CHANDRA 年輕時任英國著名物理學家 DIRAC 的助手, 有一次他告訴 DIRAC 他感到十分苦惱, 因爲雖然他相信自己找著了正確的答案, 卻總沒辦法證明那答案是正確的。DIRAC 的回答是:“我不管什麼證明, 我只想知道眞相!”

通常的表面支持證據來自三方面: 幾何直觀、歸納數據、類比。讓我們逐項看看。

先看幾何直觀。KLEIN 在1908年提供了一個後來廣泛流傳的例子。他“證明”了任何三角形皆爲等腰三角形!把三角形 ABC的內角$\angle BAC$ 平分, 也豎立 BC 的中垂線, 角平分線 AO 和中垂線 DO 相交於 O(見圖6a)。從 O 構作垂直於 AB 和 AC 的線, 交 AB 於 E, 交 AC 於 F。利用全等三角形可知 $AE=AF$ 和 $BE=CF$, 故 $AB=AE+BE=AF+CF=AC$。有人會質疑:“角平分線及中垂線的交點可能落在 ABC 外面呀!”要是那樣, 我們類似地構作 OE 和 OF (見圖 6b), 依樣畫葫蘆, 可知 $AB=AE-BE=AF-CF=AC$, 結論是一樣。錯在什麼地方呢? 如果讀者仔細畫一幅精確的圖, 當能發現箇中蹊蹺。但歐氏幾何乃憑演繹推理獲得定理的公理系統, 理應對由直觀草圖提供的命題給予精確的證明, 不應對繪畫精確的圖形給予直觀的證明呀! 單憑歐氏幾何公理, 判斷不了圖形是那個樣子的。

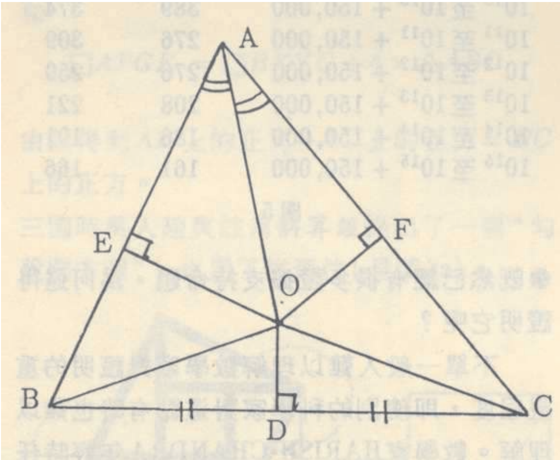

圖6(a)

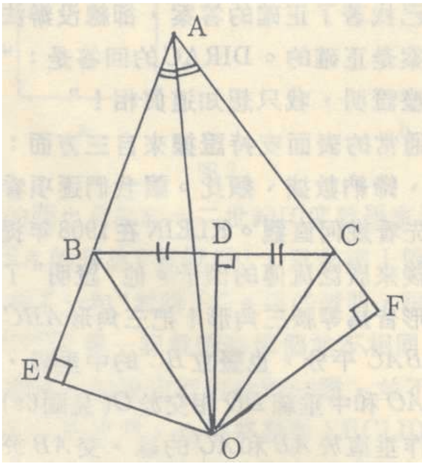

圖6(b)

再看歸納數據。有個這樣的問題: 除 $y=0$ 以外,$1+1141y^2$ 能否是平方數? 那等於解方程式 $x^2-1141y^2=1$, 求整數值的解。FERMAT 早在十七世紀已經討論這類方程式 ,後來 EULER 卻錯將賬記在英國數學家 PELL 的頭上, 今天我們習慣稱這類方程式作 PELL 氏方程式。如果你進行直接驗算, 即使你算至 y 是一百萬以至一千萬, 答案依然是否定。但其實數學家早證明了不單存在那樣的 x 和 y , 並且存在無窮多對那樣的 x 和 y 。不過最小的 y 已經極大, 是 30,693,385,322,765,657, 197,397,208~3×10^{25}, 相應的 x 是 1,036,782, 394,157,223,963,237,125,215~10^{27}。

最後看看類比。公元前三世紀 ARCHIMEDES 證明了橢圓面積公式,$A=\pi ab$,a 和 b 分別是橢圓的半長軸和半短軸。置 $a=b=r$, 橢圓化爲半徑是 r 的圓, 面積化爲 $A=\pi r^2$, 那是對的。考慮圓和它的外切正方形, 它們的面積之比是 $\pi:4$, 周長之比也是 $\pi:4$。若依類比, 既然橢圓和它的外切矩形面積之比是 $\pi:4$, 一個合理的推測是橢圓和它的外切矩形周長之比也是 $\pi:4$, 從而得到橢圓周長是$(\pi/4)\times 4\times(a+b)=\pi(a+b)$。置 $a=b=r$, 橢圓化爲半徑是 r 的圓, 周長化爲 $2\pi r$, 那是對的。十三世紀的意大利數學家 FIBONACCI 的確曾經提出了這樣的公式 ,但今天我們知道那是錯的。事實上橢圓的周長的計算絕不簡單, 根本不可能有一條簡潔的公式, 十九世紀後期的數學家才瞭解這回事。

● 證明又是否可靠呢?讓我說幾個小故事。

美國柏克萊大學的 BERLEKAMP 著的 代數編碼論 被公認爲這門領域的經典之作, 給譯成多國文字。在序言裡他許下諾言誰頭一個指出書裡任何錯誤, 勿論大小, 每條一律酬以美金一元!1978年冬我初讀此書, 發現第四章裡有條定理的證明錯了, 但可修補, 便寫信告訴作者。半個月後收到回信, 不出所料, 早於九年前他已經付出那一塊錢了。信內還附有一個勘誤表, 整整十三頁, 大大小小錯誤約有二百五十條, 作者還說這些年來他仍

得爲這項諾言每年支付三或四塊錢呢!但這些錯誤絲毫沒有減低大家對這本著述的評價。

1945 年時代周刊有一期報導了當時的一則轟動新聞, 美國數學家 RADEMACHER 宣稱證明了數學上一個極著名的猜想—— RIEMANN 猜想。1986 年春紐約時報報導了英國數學家 ROURKE 和葡萄牙數學家 REGO 解決了數學上另一個極負盛名的猜想—— POINCARÉ 猜想, 亦轟動一時。1988年三月時代周刊登載了一則新聞, 說日本數學家 MIYAOKA 證明了數學史上最大的懸案——“FERMAT 最後大定理”。後來這些定理的證明都被發現有紕漏, 而且無法修補。時至今日, 上述的三個難題依然懸而未決。但這些錯誤的證明並沒有使人看輕那幾位數學家的能力, 更沒有人會嘲笑他們的錯誤, 說不定日後發展說明他們的努力或者爲最終的解答作出貢獻。歷史上滿是這種事例, 就以“FERMAT 最後大定理”爲例,1847年三月一日法國數學家 LAMÉ 向巴黎科學院宣讀的錯誤證明對數論其後的發展有密切的關連。另一個著名例子是英國律師 KEMPE 在1879年爲前一年英國數學家 CAYLEY 提出的“四色問題”的解答 (原問題是先由一位年輕人 GUTHRIE 在1852年提出, 經由英國數學家 DEMORGAN 的介紹流傳開來)。雖然過了十一年後另一位英國數學家 HEAWOOD 發現證明當中有漏洞, 但其後的探討, 都是基於這種想法, 終於導致1976年的電腦證明, 運用當時的電腦計算一千二百小時後證明任何地圖均能以四種顏色著色。這證明也引起數學界爭論: 電腦證明是否算是數學證明?

還有一則“路邊社”消息:數學評論 的一位編輯說, 幾乎一半刊登了的證明是錯的 ,不過它們要證明的命題卻大部份是對的!

- 即使證明眞的無誤, 誰去判斷呢?

原則上每一門數學理論都可以給形式化, 意思是說, 基本概念轉換爲符號, 公理和命題轉換爲符號公式。例如 $1+1=2$ 變成

$$=(+(s(0),s(0),s(s(0))))。$$

證明轉換爲符號公式的有窮序列, 證明是否無誤等於鑑定從一道符號公式至下一道符號公式是否按照特定的准許的法則進行。如此說來, 毋須人的介入, 機器也能勝任這樁工作。從1920年至1930年間 HILBERT 提出了這項宏偉的計劃, 希望藉此解答數學是否相容 (亦即內部無矛盾) 這個問題。

實際上, 能否這樣形式化呢? 據云波蘭數學家 STEINHAUS 的一位學生試把勾股定理的證明基於 HILBERT 的幾何基礎裡面的公理系統全盤形式化 ,寫出來的符號公式充滿八十頁!但繁複猶是次要, 致命的一擊來自1931年奧地利數學家 GÖDEL 發表的兩條使人震驚的定理, 使整個企圖通過形式化去保證數學相容的美夢幻滅!他證明了:(1) 如果形式算術系統是相容的, 那麼它是不完全的, 即是說系統中有一命題, 既不能證明它是對的, 也不能證明它是錯的。(2) 如果形式算術系統是相容的, 那麼不能以系統內的形式方法證明它是相容的。

再回到數學家的日常工作看看, 他們證明定理豈是形式化的邏輯推導呢? 只是“指指點點”而已。固然, 指指點點當中必定包含不少符號和算式, 但那只是約定俗成的簡寫

吧, 與全盤形式化的證明相差不啻千萬里!既是指指點點, 自然涉及人的因素, 講解證明的是人, 理解證明的是人, 甚至接受證明與否的也是人。

有些證明既冗長又繁複, 有沒有人可以由頭至尾——包括證明裡面引用的定理的證明 ——核實全部細節呢? 即使有這種耐心的人, 又怎麼保證任何錯誤均難逃其鷹目呢? 有限群的分類問題是一個好例子, 就是問有多少個眞正不同的 N 元群表? 這個問題在1890年左右給提出後, 隔了幾乎一百年才算基本上被解決了。這個解答是衆多數學家在將近一個世紀以來累積的努力成果, 有關的文章、筆記、講義散見於各處。有人估計,要把這些成果集中起來整理, 少說也長達五千多頁!有幾人曾把這五千多頁的材料都通讀呢?

近十多年來, 更因電腦興起而產生所謂"電腦證明"。最早的著名例子是上述提過的1976年美國數學家 HAKEN 和 APPEL 在 KOCH 的協助下用了一千二百小時電腦計算時間解答了四色問題。最近關於十階有限射影平面的電腦證明, 使四色問題的計算時間變成小巫見大巫。1988年冬加拿大康哥迪亞大學林永康領導的研究小組宣稱他們證明了不存在十階有限射影平面, 他們借用美國國防分析研究所的 CRAY-1A 超級電腦工餘時間, 化整爲零配合他們自己大學的電腦, 花了整整三年完成二千多小時的計算。無人可確定電腦有沒有出錯, 出錯了又難以確定那是電腦本身的機器毛病抑或是計算方法上的紕漏。

● 上面好像說盡數學的壞話: 好些數學定理不必證明也可以入信!證明了的定理倒不一定可盡信!證明滲入過多的人爲因素!甚至數學本身具有先天的缺陷——GÖDEL 不完全定理!那麼說來, 數學證明是否還有功用呢?

數學證明的核實功用還是有它的地位。就數學內容結構而言, 正如近代著名數學家 WEYL 說過:"邏輯是數學家爲保持思想強健而遵守的衛生規則。"就學風而言, 正如另一位著名數學家 WEIL 說過:"嚴謹之於數學家, 猶如道德之於人。"

數學證明還有另一個功用, 甚至是更重要的功用, 即是增加理解。BOURBAKI 學派在一篇題爲數學的建築(1950年) 的文章裡說了這麼一段話:"每個數學工作者都知道, 單是驗證了一個數學證明的逐步邏輯推導, 卻沒有試圖洞察獲致這一連串推導的背後意念,那並不算理解了那個數學證明。"

有個這樣的小故事, 據說美國數學家 COLE 在1903 年十月給美國數學會作了一個"無言的 講演", 他在黑板上寫了兩個式子:

$$2^{67}-1=147,573,952,589,676,412,927$$

和

$$193,707,721\times 761,838,257,287 \qquad ,$$

然後把後式兩數相乘, 得到乘積正好是前式的數。換句話說, 他證明了 $2^{67}-1$ 是個合成數, 長久以來, 人們還以爲 $2^{67}-1$ 是個質數。整個過程中他不發一言, 寫完後放下粉筆, 全場報以熱烈的掌聲!後來有人問他, 這花去多少工夫, 他答道:"三年來的全部星期日。"我雖然佩服 COLE 的堅毅作風, 但我不認爲這個證明使人增加理解, 不

符合俄羅斯數學家 MANIN 的話:“一個好的證明應使我們更明智。”就如同前面我告訴過你 ,$\sqrt{1+1141\times(30,693,\cdots,208)} = 1,036,\cdots,215$, 但那可半點也沒有增 加你對 $x^2-dy^2=1$ 這種方程式的理解。

讓我舉出 GAUSS 關於二次互反律的證明經過爲例再強調這一點。讀者大可不必理會爲何這條定理如此重要, 總而言之,GAUSS 對它十分重視, 甚至曾稱它作“數論的寶石”。先弄清楚何謂二次剩餘。設 a 和 m 是互質的正整數, 若有正整數 x 使 a 和 x^2 以 m 除時有同樣的餘數, 便說 a 是模 m 的二次剩餘, 否則便說 a 是模 m 的非二次剩餘。例如 3 是 11 的二次剩餘, 因爲 3 和 $5^2=25$ 以 11 除時都餘 3; 但 11 是 3 的非二次剩餘, 因爲 3 除 11 餘 2, 但 3 除任何平方只餘 0 或 1。讓我們列一個表, 標以 a 的列和標以 m 的行的一格是黑表示 a 是 m 的二次剩餘, 那格是白表示 a 是 m 的非二次剩餘。(在 $a=m$ 的行列相交那格打個 $\times$, 可以不理。) 這兒的 a 和 m 只取奇質數值 (見圖7a)。看起來這個表好像沒有什麼規律可言, 但如果你把這個表的行列作適當置換, 把形如 $4t+3$ 的質數放在前面, 形如 $4t+1$ 的質數放在後面, 得來的表 (見圖7b) 有個規律: 除了左上角的方陣是“反對稱”以外, 其餘地方卻是“對稱”的。這就是二次互反律的優美內容。早在 1783年 EULER 已經提及跟這回事等價的定理, 但明確的表述及證明的嘗試應歸功於同時期的 LEGENDRE。不過他們兩人都沒有眞正成功證明了定理, 直至 1796年 GAUSS 才找到第一個證明。GAUSS 很重視這條定理, 後來陸續再發表另外五個證明, 最後一個 (第六個) 發表於1818年, 距第一個證明相隔超過了二十年了!通過不同的證明,GAUSS 揭示了這條定理不同的層面, 使人對數論有更深入的瞭解, 開啓了後世的研究方向。在1963年美國數學家 GERSTEN-HABER 寫了一篇一頁長的文章, 刊登於美國數學月刊 , 開玩笑地把題目定爲“二次互反律的第一百五十二個證明”。即使最近, 另一位美國數學家 SWAN 也寫了一篇半頁長的文章, 也是刊登於美國數學月刊, 題爲“二次互反律的另一個證明”。如果證明的功用僅供核實, 一個證明或者再多一個以供查驗便夠了吧, 何需對同一條定理證明了又證明呢?

• 以上拉雜談, 可以說試圖從側面說明數學是怎樣的一門人類文化活動。我並沒有也並不意圖給出一個答案, 但我希望能使讀者同意數學並不是乾巴巴的公式和邏輯而已。數學的眞正面目, 恐怕不容易說淸楚, 更且它

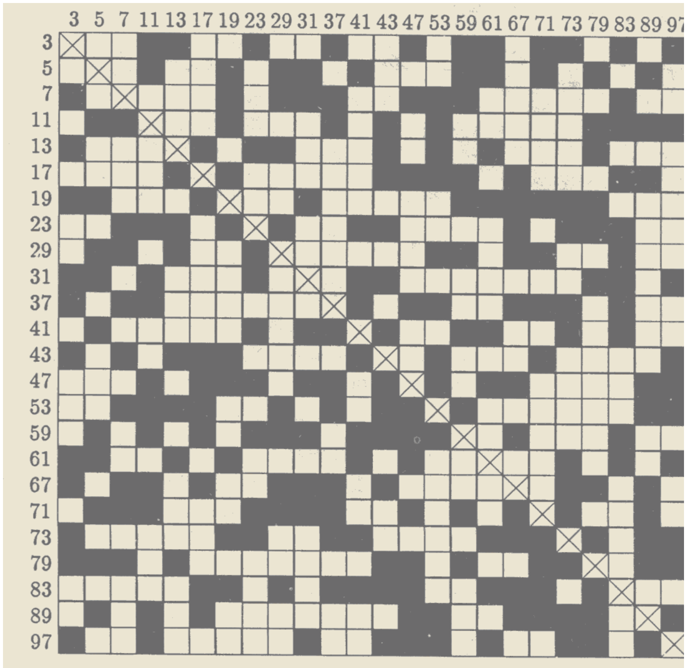
3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
3
5
7
11
13
17
19
23
29
31
37
41
43
47
53
59
61
67
71
73
79
83
89
97

圖7(a)

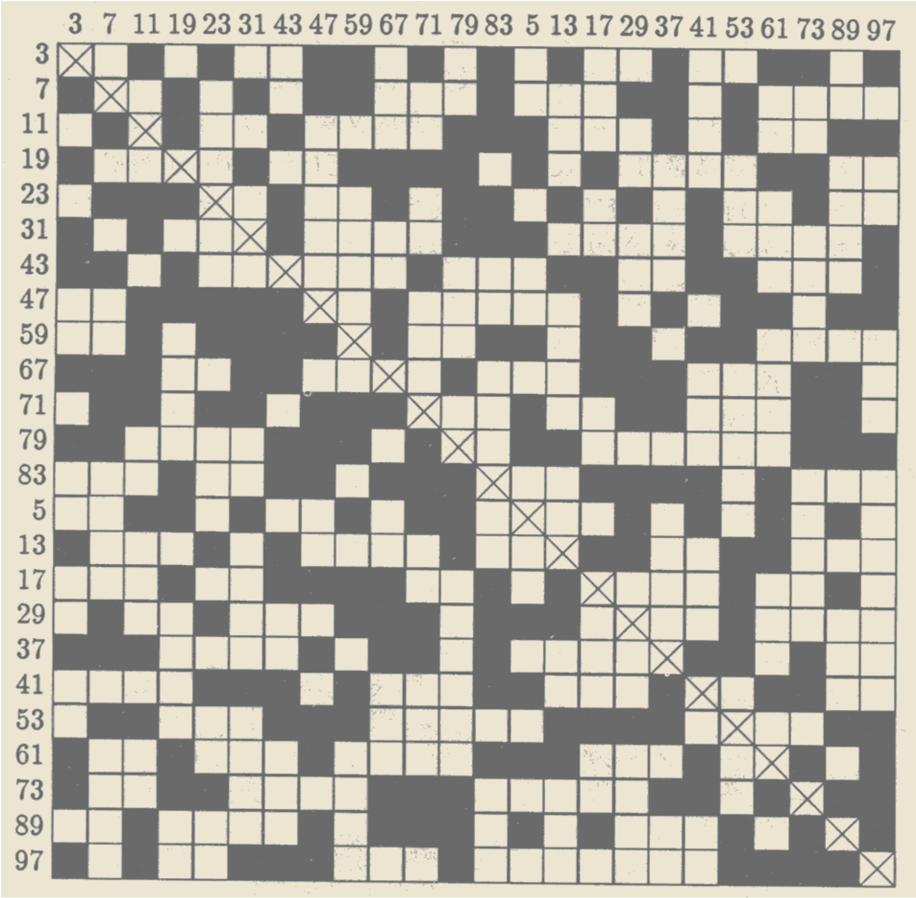

圖7(b)

因人而異, 每個人有每個人的不同體會, 這究竟是一個多元化的世界呀!或者讓我引用著名數學家數學教育家 POLYA 的一段話作結束:“ 數學思維不是純形式的, 它涉及的不僅有公理、定理、定義及嚴格的證明, 而且還有許許多多其他方面: 推廣、歸納、類推以及從一個具體情況中辨認出或者說抽取出某個數學概念等等。”

後記:這是 1992年元月我在中研院訪問期間到台灣師範大學數學系作的講演的講稿。當日有機會與師大洪萬生、林福來兩位老師交流意見, 並且有機會與師大的一群年輕研究生一起討論。這段愉快聚晤, 使我獲益良多, 謹在此向各位朋友致謝。同時也在此多謝中研院數學所所長李國偉先生的安排, 讓我有這個機會訪問臺灣的一些院校, 結識了不少同行的朋友。

—本文作者任教於香港大學數學系—