數學近貌 序言

石厚高

Lynn Arthur Steen所輯的Mathematics Today：Twelve Informal Essays（Springer-Verlag，1978）一書共收集了十二篇文章，是當代著名數學家所寫的有關理論數學及應用數學的散文。其目標是要把數學觀念中的某些性質、發展以及數學觀念的應用——尤其是那些在現代科學研究已經應用的數學——傳達給非數學家專業人士。

選輯這一本書的構想至少要回溯到1974年，那時有三個團體在研商：American Mathematical Society的Joint Project Committee for Mathematics（JPCM）、Mathematical Associatiation of America以及Society for Industry and Applied Mathematics。JPCM把出版此書列爲首要計畫，並委請Conference Board of the Mathematical Sciences（CBMS）向National Science Foundation提出支助。

這本書分四個部分：

一、數學——人類無形的文化*。

二、數論、羣與對稱、宇宙的幾何、氣象的數學，及四色問題。

三、組合式安排理論、計算是什麼、了解經濟靠數學、生物繁衍之數學觀。

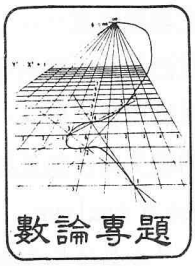
四、數學的關聯。

本系列專欄即選譯自Mathematical Today這本書，希望透過它，能讓大家有機會一窺近世數學的概貌。

最後，我要向本欄的諸位審稿人致最高的謝忱，由於他們的潤色並改正謬誤，使本欄增色不少。

---

*第一部分已分別由朱建正、林聰源兩位教授譯出，刊登於本刊四卷一、二期和五卷一期。



數學近貌：數　論

石厚高　譯
Lan Richards　著

數論所關注的是整數的性質。它是數學中最古老的兩個分支之一，幾何是另一支。但古典的“圓與三角形”的歐氏幾何對研究科學而言本質上已經是槁木死灰，而數論仍然有很多沒有解決的問題。說實話，它的某些最有吸引力的問題要回溯至歐氏的時代。

讓我們從一些已經解決的問題開始。考慮質數P（質數就是除了1以外不能被比它小的任何數整除的數）。就拿這個三十九位的質數

$$P = 170,141,183,460,469,231,731,687,303,715,884,105,727,$$

來說吧，它是現代電腦來臨之前已知的最大質數。假設我們把比$P-1$小的所有數全部乘起來（P就是上面所說的最大質數）：那就是說，我們把1乘以2再乘以3一直乘到$P-2$。這個結果叫作“$P-2$的階乘”〔寫作（$P-2$）!〕。我沒有算過這個數，任何人都沒有算過，電腦也是一樣。甚至於把它寫下來所用的紙也比世界上所有圖書館的圖書還要多；就算是電腦能計算它（而它不能），世界上也沒有足夠的紙把答案印出來。可是這種數必定存在，因爲我們能合理的給它定義，也能對它作各種考慮。

好了，假設我們現在把“$P-2$階乘”這個數除以P，結果就得了某個商數與餘數（正如我們拿72除以7得到了商數10而餘數爲2）。當然啦，理由如前述，從來沒有人作過這個除法。可是我們知道這個餘數應該是多少。它應該是1。我們是從一個叫作“威爾遜（Wilson）定理”理論的結果知道的。

威爾遜是十八世紀的英國學者，從來就沒有人以這麼少的理由而不朽。他並沒有把他的“定理”證出來，而較早另外有個人，忘了是在什麼地方的什麼文章裡曾經眞正的說了出來並證明了這個定理（我忘了原來的作者；歷史眞是殘酷的！）。威爾遜的“發現”被一個阿諛的朋友所出版，他預言這個定理永遠不會被證明——眞的是永遠不能被證出來——因爲人類沒有好的記號來對付質數。這個值得注意的聲明被高斯（Gauss）知道了——一直被很多人公認爲最偉大的數學家（想要知道高斯的更多事跡，請參閱第4頁方塊）。高斯進行“威爾遜定理”的證明時，只獨自思考了五分鐘，高斯就對威爾遜下評論說“他不需要記號，他需要觀念”。

傳統的說法（也許是神話）是數學家必須“對於數字算得很快”。這是不對的——數學所包括的主要是直觀與掌握理論觀念的能力。如果一個數學家有這些才能，他就不再需要什麼別的東西了。可是高斯是個例外。他樣樣精

通！他是個語言大師，他記得全部的對數表——並且他是個數學家。和很多偉大數學家一樣他是早熟的。在十七歲之前他解決了“三等分一角”的老問題，證明它是不可能的。當他二十四歲（1801）的時候出版了數論上第一篇有系統的論文，一本叫作Disquisitiones Arithmeticae的書。在這本書的開宗明義第一頁他列出了他認爲的數論先進；恰巧是四個人——費馬（Fermat）、尤拉（Euler）、拉格蘭自（Lagrange）與勒尖得（Legendre）。此外，高斯讓讀者毫不懷疑他認爲自己在同儕中名列第一。例如，在討論某個結論的時候（今日稱之爲“**二次相互律**”，“**law of quadratic reciprocity**”）在他之前已經有人發現了，而高斯第一個把它證了出來，他這樣寫着：

> 基本定理〔那就是指相互律〕必須確實被認爲是它那一類中最漂亮的一個。到目前爲止還沒有人用像我們作得這麼簡單的形式把它呈現出來……。更讓人吃驚的是尤拉已經知道與它有關的其它命題，應該導致它的發現……尤拉之後，著名的勒尖得在他最好的論文“Recherches d'analyse indéterminée',……”中熱忱的作同樣的努力……勒尖得嘗試了一個證明，因爲它很巧妙，我們會在下一節把它講得相當詳盡。可是因爲他先作了很多假定而沒有證明（他自己本身也承認……）……他所著手的途徑似乎導致了僵局，所以我們的證明應該被認爲是最先的。下面我們就要對這個最重要的定理提出兩種其他的證明，它們彼此互異也與以往的完全不同。

換言之，其他的人都不能證明的，高斯證明了一次以後，又作了兩次較好的改正。

高斯

（Carl Friedrich Gauss）

1785年某天，一個德國數學教師爲了要他的學生保持安靜，就告訴他們把1到100的數全部加起來。這位老師知道有個公式可以用來作這一題。當然啦這些學生並不知道（他們是“二年級生”），所以老師就能保證有一小時的安靜了（那個時代學校是有些規矩的）。可是其中有個學生名叫高斯（Carl Gauss）立刻走到教室前面提出了正確答案5050。高斯也知道這個公式！

數學的歷史是幸運的，這位老師絕對能體會到某些特殊的事要發生了。高斯沒有受過教育的雙親能教給他這個公式嗎？絕對辦不到：他一定是自己發現的。由此就開始了公認爲亘古以來最偉大數學家的生涯。

這裡沒有篇幅來談高斯的研究，或是分析一下他的複雜而時常矛盾的個性。他是個怪人，有的時候冷漠而無情，他也是個最難取悅的標準知識份子。今天他的大名出現在數學以及數學應用的每個角落：只舉一個例子，有種電磁單位被稱作“高斯”。

對於Disquisition Arithmeticae 的一個現代繼承者是1975年英國年輕數學家Alan Baker所出版的一本書。（事實上，貝克是從引用Disquisitiones 開始了他的書）。貝克的研究是在“超越數”以及“Diophantine 方程式”的範疇，曾導致數論的一次革命，我們以後會對它的發展詳加討論。

整數(Whole Numbers)

Diophantine 方程式以古代希臘數學家叫作Diophantine 的爲名，關注於方程式的整數解，限制爲整數，才能使它成爲“數之理論化”而不是一個純計算問題。因爲一個方程式可以有很多解，只有在特殊情形下這些解才會是整數。所以看看下面的例子：

$$x^2 = 2y^4 - 1$$

這個方程式有 x 與 y 都是正整數的解。說得更明確一些它恰有兩個這樣的解。有一個很容易看得出來：$x = 1$ 與 $y = 1$。可是，或許沒有人能很快的找到第二個。它是 $x = 239$，$y = 13$。而挪威數學家W.Ljunggren在1942年證明了別無它解。（公平說來我應該補充說明，這個結果是如此的特殊與奇異，在數論中它並不是特別重要。我在這裡提它，也只不過是爲了好玩罷了。）

另外一個Diophantine 問題有非常豐富的歷史，那就是把某一個整數寫成若干個整數的平方和。平方數就是小學生都知道的1，4，9，16，……。其他的數例如6，不是平方數，可是它們能寫成平方數之和

$$6 = 4 + 1 + 1$$

到現在爲止諸事順遂，可是下一個問題較爲困難。假設我們要把任何整數寫成若干整數的平方和（例如我們剛剛看到了6是三個平方數之和4，1與1）。一般來說，我們需要多少個？三個夠嗎？我們需要四個嗎？或五個嗎？或隨意選取的非常大的數，就說它是

$$5,149,176,235,882,197,318,266,512$$

吧，我們需要把很多個平方數加起來得到這個數，這是可能的嗎？答案如下：四個平方數就夠了，三個平方數有時是不行的。古希臘人發現了很多數學上的事實，這一件也是其中之一。可是數論不同於幾何，希臘人很少能證明他們的發現。這種尖銳的對比——輕鬆的道來定理內容，而無法證明它——是數論吸引數學家的事物之一。我們有個簡單的命題，就像是：

每個正整數是四個較小的平方數之和。

好啦，你也許會說你不在乎。那是完全合理的。可是你確實了解這個命題。還有呢，或許你我在一千年內都證不出來。

這種誇大有點瘋狂，可是有一點正確的主張必須要指出來——我們了解某事物的意義並不意味我們一定能把它作出來。說得具體些，攀登額非爾士峯（Mt. Everest），每個人都能直觀的了解到這一點。我們大多數都是對於能爬上峯頂的人吝於表示尊敬。可是對我的胃口來說“四平方數定理”（four-squares theorem）更饒趣味。這個定理在有人能了解它欣賞它之前，在金字塔造成之前就已經爲眞了。此外，當我們剛發現它的時候（一如古希臘人），它像個臆測：它似乎是眞的，可是我們不能證明。它似乎是眞的，因爲不管我們怎麼試它都正確，或許我們測驗數千次，如果我們有個當代的電腦也許作它幾百萬次。因爲它畢竟是個數學問題，不論我們測試多少次，還是有無限多次沒有作——其中可能有一次例外摧毀了這個規則。只有邏輯的證明能同時包含這些無數的個案，彌平了臆測與眞理建立的鴻溝。

有很長的一段時間（沒有人能預言有多長），這個“發現”僅僅保持着一種臆測狀態。最後是某個人證明了它——或證明它不眞。至

尤拉

（ Leonhard Euler ）

你很難想像一個人怎麼可能寫出一百本書來，可還是有人作到了。但是在歷史上只有一個人寫了那麼多數學。尤拉（ Leonhard Euler 1707 — 1783 ）是有史以來最偉大的五、六位數學家之一。他生於端士的Basel附近。大部分生活與工作在柏林（ Berlin ）與彼得斯堡（ St. Petersburg ）。他的“尤拉特徵”（ Euler characteristic ）是拓撲學中的前所未有的發現，第一個發現，有時用來在高級中學教那些資優生；今天所寫的每一本微積分都是尤拉所寫的一篇論文的直接後裔。可是他所研究的其他部分是太前進了，直到現在他們也不過是僅僅了解而已。完成這個工作的尤拉是個熱愛家庭的人，也是個虔誠的基督徒。他是個眞正謙虛的人，有的時候甚至取回他的論文，讓更年輕的人可以先發表同樣的結果。更有趣而值得大書特書的是——就像歷史上某些偉大人物一樣，他的眼睛瞎了以後仍然繼續工作。

少我們希望會有這種事發生。在四平方數定理的個案裡確實發生了這種事，在大約二千年之後：這個臆測被證明爲眞。十八世紀兩位最偉大數學家中之一，尤拉，一生之中斷斷續續的在作這個問題。可是他的對手拉格蘭自找到了證明（尤拉與拉格蘭自更多的資料請參閱本頁與第20頁方塊）。自此之後其它證明就層出不窮（奇怪的是，第一種證明仍然是最簡單的），這些證明中有些包括預料不到的附加物——數學物理。（這些附加物是藉着所謂的橢圓函數“ elliptic functions ”而來的）。我們說現代數學中有段豐富的內涵是拜四平方數定理所賜是很公平的。

對人類的意志來說有件奇怪的事實——掌握人們想像力的事物比任何實際目標更能使人們爲之努力不懈。最近由威斯康新大學數學研究中心（ Wisconsin's Mathematics Research Center ）的J.B.Rosser，L.Schoenfeld與J.M.Yohe所主持的計畫說明了這一點。這三位數學家用一部電腦獲得了有利於某個數論臆測（ number-theoretic conjecture ）的證據。這個臆測被稱爲“里曼假說”（ Riemann Hypothesis ），它的說明須要些技巧。我們在這裡所要說的只是它的特點。可是，對我們目前的目標來說那已經足夠了；稍後我們要更詳盡的討論此一假說。

質數的理論導致了某個“複變數函數”的“里曼ζ函數”（ Riemann zeta-function ）。問題本身是關注於這個函數的“零”（那就是使函數等於零之點）。據了解——除了某些我們能區分的不重要的例外——所有的這些“零”都在二維平面某個無限的長條區域之內部。同時也知道“零”是有無限多個的。里曼假說主張所有這些“零”都在長條區域的中心線上。這個假說是由德國數學家里曼在1859年作的，直到今天仍然沒有證出來。它是數學上最

里曼

（Bernhard Riemann）

有句陳腔爛調是說“一個藝術家必須受苦”。對里曼（Bernhard Riemann）來說確實如此，他一生多在受苦。這並不因爲他是默默無聞之人。事實上他被認爲是個天才。他只不過沒有職業罷了。更糟的是，他家中有幾個人依賴他的供養。所以里曼以微薄收入養家並挨餓工作。他在數學上的研究幾乎影響到了數學的每一分支。只舉一個例子，愛因斯坦（Einstein's）的一般相對論奠基於里曼所發展的數學。包含里曼假說（Riemann Hypothesis 本文曾特別提及）的八頁論文是數論中曾經發表過的最重要的論文。

最後在1859年里曼轉運了。他在哥丁根（Göttingen）得到一個教授的職位，三年後結婚有了個女兒。噩運仍然如影相隨，1866年三十九歲時死於肺結核。

著名的未解決問題之一，直到今天爲止質數中未決定的理論大部分與它有關。（想對里曼有更多的了解，請參閱本頁方塊。）

Rosser，Schoenfeld，與Yohe在他們研究里曼假說時用一部電腦展示了ζ函數的最初三百萬個“零”確實是在長條區域的中心線上。當然啦，這種資訊並沒有建立一種證明——電腦的資料很少有能作到的——因爲“零”有無限多個，而我們只考慮了它們之中的最初三百萬個。可是，三百萬件個案中無一例外似乎也是強勁的證明了。不過數論的歷史有過先例，這種有限的推論是十分不可靠的。曾有過這麼個例子，在1914年英國數學家J.E.Littlewood發現了某個方程式對於所有直到X的數都爲眞（X是個非常大的數，今日稱之爲“Littlewood 常數”），可是在這個數值之外有無數個數使方程式不能成立。到今天爲止Littlewood常數的最佳估計是超過了10^{100}——那就是一個1後面跟着100個零——一個很容易大於宇宙中可見的原子數的數量。

對於Rosser，Schoenfeld，Yohe的研究，另有個有趣的啓示。純數學家有點懷疑電腦，因爲電腦是個機器，而機器會犯錯誤。如果機器確實犯了個錯誤，你怎麼會知道呢？從電腦中得來的結果一般是必須有信心接受的。了解到這一點，所以Rosser，Schoefeld，與Yohe對他們的工作非常小心的研究；他們把程式以宗教家的熱誠檢查了又再檢查。在檢查中他們發現電腦本身的內部邏輯會有一些錯誤。電腦被用了很多年沒有任何人發現這個事實。更確切的說，這些錯誤是非常微妙的，或許沒有影響到計算的常規。不過，三個人在數學最飄渺的領域中研究一個不切實際的問題探出這個錯誤來，還是破天荒的第一次。

質數(Prime Numbers)

一個比1大的整數，除了1以外不能被比

它小的任何整數整除，就把它叫作“質數”。質數很重要，因爲它們是用乘法建立某些數的“原子”。例如

$15 = 3 \cdot 5$ 而 $8316 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 \cdot 11$

（小圓點是表示乘法；對於“3・5”來說是讀作“3乘以5”）對於其它含質數的例子以及與其它各數之間的關係，請參閱本頁之方塊。

不論它們的定義是多麼單純，令人吃驚的是對質數了解得太少。我們知道在現代算術與代數中它們是非常基本的。可是掌管它們的分布的定律我們知道得很少。這並不是由於疏忽：質數理論吸引了現代最優秀的數學家中某些人的注意。或者是數學中任何範圍都沒有包括這麼多沒有證出來的臆測。

我們對於質數知道些什麼？好啦，歐基里德證明了質數的個數是無限的，在以後的兩千年中雖然作了很多臆測，這種證明可就是此一主題中的唯一定理，例如：古代記錄中有很多“雙生質數”（twin primes）的個案，那就是說一對連續奇數而又都是質數，諸如

17，19 或 29，31 或 41，43

古人臆測這種雙生質數有無限多個。可是這個臆測仍然沒有證出來。不過，最近中國數學家陳景潤把它證了一下（雖然說是勁道不太夠，總也算是具體而微了）：他證明了有無數對的成對奇數，P與$P+2$，其中前者是個奇數，後者$P+2$至多有兩個質因數。（在“雙生質數”中我們需要P與$P+2$二者都是質數；現在我們能說P是質數可是$P+2$只不過是個“幾乎是質數”。）

不論這個結果有幾分不完整的性質，陳氏定理是被當作主要成就而叫好。一則沒有人能知道還要等多久才能有人作得更好。再則陳氏的證明幾乎把質數理論上所作過的每一件事都用到了：要把它們用不是專門研究這個問題的數學家能了解的形式寫下來，那就需要每册約三百頁的書兩册。我的意思是說在了解陳氏定理之前這兩本書的整個內容都要精通——六百

質數與合成數

數學家把正整數分成三類：

單一數1：它被稱爲單位。乘以1不產生任何效果，例如$3 = 3 \cdot 1 = 3 \cdot 1 \cdot 1 = 3 \cdot 1 \cdot 1 \cdot 1$等等。

質數：那就是除了1與本身外不再有任何因數的正整數。所以17是一個質數，而$15 = 3 \cdot 5$則否。

合成數：就是比1大而不爲質數者。例如，$4 = 2 \cdot 2$，$6 = 2 \cdot 3$，而$9 = 3 \cdot 3$都是合成數。小於一百的質數有二十五個，那就是：

2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97

（質數中除了2以外都不是偶數，因爲每個偶數都有2作爲因數）。任何數都可以經由乘法從原子——質數——建立起來。例如，$12 = 2 \cdot 2 \cdot 3$，而$210 = 2 \cdot 3 \cdot 5 \cdot 7$，沒有別的方法能把12或210寫成質數之積。（當然啦，我們忽略了各因數間不關緊要的次序，例如寫下$12 = 3 \cdot 2 \cdot 2$而不用$2 \cdot 2 \cdot 3$）同樣的敍述適用於任何數，而“整數質因數分解的唯一性”這個事實，形成了理論算術的基礎。

頁的方程式與論述，用這樣的文體能使希臘幾何的畢氏定理用大約四行證明完畢。（我偶然想起確實有這兩本書。第一本也許任何一册載有幾篇質數的標準論文，而第二本是H. Halberstam與H.-E. Richert所著書名Sieve Methods的一本書，陳氏定理的說明是該書的最高潮。）

換個不同的問題來談談：我們如何知道某個數是質數？原則上我們知道如何去作。就拿 n 來說吧。如果 n 不是質數，那麼 n 就有某個較小因數，像2或3或4……所以我們能用比 n 小的數來試除看看它是不是質數。可是有些較快的方法，其中最有名的是厄拉多塞氏之篩（Sieve of Eratosthenes）（參閱圖1）。

一個有關連的問題就是在某範圍之內找出所有的質數。對這個目的來說厄拉多塞氏之篩也一樣管用：所以我們在圖1中產生了小於二十的全部質數。在這一方面的研究收獲頗豐。例如，美國數學家D.N.Lehmer在電腦來臨之前於1914年算出了一千萬以內的全部質數。

在我們的討論中考慮一下Lehmer是如何作的會有益處。首先他從1至一千萬的數開始。他從列出全部這些數的表中立即消去了個位是2，4，6，8或0的數，因爲這些數都是偶數，所以不是質數。同樣的消去所有個位是5的數，因爲它們能被5除盡。（當然啦，個位是0的數也能被5除盡，可是它們已經被消去了。）從現在開始，這份差事愈來愈難了。因爲要知道一個整數能不能被三或七或十一等等除盡並不是一件很容易的事。Lehmer的方法與圖1所示是一樣的：從1開始，消去每三個一數的第三個數，再來是第七個，然後是第十一個，等等。爲了有助於他的工作，他發明了很多種機械輔助設備——本質上是迷你電腦（mini-computer譯者按：當然不是今天的迷你電腦）；這些可能是最早的曾經有效使用的計算機器之一。（電腦的觀念是很古老的，可是很多種早期的模式都沒有脫離設計板的窠臼。）

厄拉多塞氏之篩在作計算時是有價值的，而數世紀來在理論上是被認爲無用的。它的困擾在於連續的消去似乎是太隨便而無法預知。在1920年挪威數學家 Viggo Brun 介紹了一

厄拉多塞氏是古希臘的一位數學家，他發明了一種方法“顯”（screen）出數字，從合成數中挑出質數。他的方法被叫作“篩”，因爲它依賴連續消去的方式。我們要展示一下“篩”法如何用來產生小於二十的全部質數。當然啦，同時也要把這些小於二十的數一個一個道來，它是質數或者不是：

1	②	③	4	⑤	6	⑦	8	9	10	⑪	12	⑬	14	15	16	⑰	18	⑲	20
	–		2		2		2		2		2		2		2		2		2
		–			3			3			3			3			3		

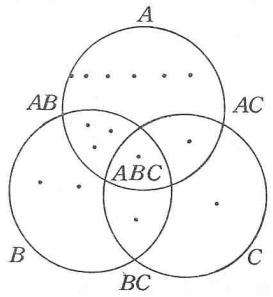
我們所作的就是消去2或3（或2與3）的倍數；畫有圓圈的數仍然是質數。例外：1這個特別的數被叫作“單位”是不算在內的，而2與3本身是質數沒有被消去。

只檢查2與3的倍數的理由如下：如果一個整數 n 有任何因數（那就是說，如果 n 不是質數），那麼某個因數是要小於或等於 $\sqrt{n}$；因爲若 $n = a \cdot b$，那麼 a 或 b 必須小於或等於 $\sqrt{n}$。還有，任何 n 的因數必須包含更小的質因數，所以只有質因數需要考慮。對於 $n = 20$ 或更小的數，$\sqrt{20} < 5$，比5小的質數只有2與3：就是我們所用的那些！

圖1 厄拉多塞氏之篩

種新方法以後，情況有了改變，它是奠基於“包容與排斥原理”。這個原理簡單得令人着迷，讀者如欲追根究底可參考本頁之方塊。在我們想像它竟然是這麼簡單之前，我就要請你來就Brun的位置坐下。我們有個問題：找出一個理論上的方法，不能一個一個的數，但能說出來某個區間的質數有幾個。這個區間可能會太大而無法計算。例如，我們可能會問：小於十億個十億個十億的質數有多少個？如果我們不能精確的計算這個數（沒有人能夠），我們至少能作個估計吧？答案的結果爲“是”，而Brun之篩提供了最主要的方法之一來解決這種問題。現在，如果你看看本頁方塊，Brun的作法，我想你會發現一開始的某些步驟十分令人驚訝。從質數的問題開始，Brun發展了一種新的方法，它所涉及的數學，有一部分通常是和資訊理論與語言學有關。在長途迂迴之後，他的方法最後又捲土重來解決了本來的問題。（實際上，它只部份的解決了這個問題，可是Brun的理論以及它的擴充仍然是我們所知道的最好方法。）這種獨創力就使一代宗師由泛泛之輩的從業人員中脫穎而出。

Brun之篩與包容排除律



設以上各區域皆含有限個元素：

A = 上方圓中點的個數 = 10

B = 左方圓中點的個數 = 7

C = 右方圓中點的個數 = 4

AB = 左方“橄欖球”中點的個數 = 4

AC = 右方“橄欖球”中點的個數 = 2

BC = 下方“橄欖球”中點的個數 = 2

ABC = 中央“三角形”中點的個數 = 1

（“橄欖球”是兩個區域的交集；“三角形”是三個區域的交集。）假設我們要計算三個圓合併後的總數（= 14）。我們可以取

$$A+B+C=21 \text{，可是它太大} \qquad (1)$$

（因爲AB，AC與BC都被計算過一次以上）。我們可以取

$$A+B+C-AB-AC-BC=13 \text{，可是它太小} \qquad (2)$$

（因爲三個區域的交集被減了太多次）。最後，如果我們取

$$A+B+C-AB-AC-BC+ABC=14 \qquad (3)$$

就得到了正確的答案。

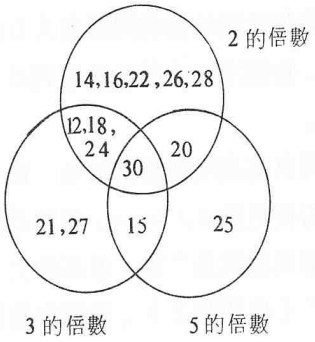
理由非常簡單；(3)式左邊計算的結果是每個點被包容與排斥的次數是正好那麼多次。一個明顯的原則是說：正確的計算一個集合就是把每個元素只算一次。而這裡就是每個點最後正好被計算了一次。例如，考慮在中央的ABC裡面的點。再來看看

$$A+B+C-AB-AC-BC+ABC$$

這個集合中的每個點在$A+B+C$中被計算了三次，然後在$-AB-AC-BC$中被排除了三次（到目前爲止總次數 = 0）；最後這個點又在ABC中出現了。所以，其它的點也是一樣的。

如果我們用包容與排除律來計算某區間的質數（就說是11到30吧），那麼與以上討論有關的篩問題就變得明朗了。實際上我們是要計算合成數（那就是非質數），然後用減法來導出質數的個數。首先我們觀察到這個區間共有二十個數11，12，……，30。在這個範圍中的每個合成數必須至少被質數2，3，5中之一整除（當然也可能被幾個整

除）：這一點對下一個質數 7 來講也是成立的，而最小的合成數（只有 7 或較大質數作爲因數）是 $49 = 7^2$。現在，我們就有了與前面三個圓圖形酷似的模式：



（當然啦，21也是 7 的一個倍數；可是我們沒有地方來安置這一類）。在 11 到 30 之間有十四個合成數，而全體共有二十個數，所以必須有六個質數。實際上是有六個：它們是 11，13，17，19，23，29。

而這種過程似乎是比一個一個的數也好不到那裡去，可是在大區間一個一個的數是不切實際時，這個邏輯原理就派上用場了，就好像是從九十億到一百億的區間。它的觀念是這樣的，注意，“ 2 的倍數 ”之圓總共含有十個點，這可不是偶然的：從 11 到 30 共有二十個數，其中一半是偶數！“ 5 的倍數 ”之圓也一樣，含有 $20/5 = 4$ 個點。“ 3 的倍數 ”之圓含有七個點，而 $20/3 = 6.6666\cdots$（多出來的是怎麼回事？）

現在我們來想想 Brun 方法中最令人驚訝的部份。讓我們再一次考慮我們所發展的公式(1)，(2)與(3)中在圓的重疊部份所計算的點數。再回想一下，公式(3)是恰好正確，而(1)與(2)分別是太大與太小。Brun 的妙訣是避免用(3)而以(1)與(2)來代替。他的理由是這樣的，雖然說公式(1)與(2)並不是恰恰好，可是它們比(3)要簡單，並且它們帶來了合理的近似值。實際上，要了解到，我們必須假定有好幾千個集合而不是 A、B、C 三個集合（如上圖所示）。所以組合個數的增加，超越了所有的理性界限（多於太陽系的原子數——就像那一類的東西），把這個數減少便是 Brun 所主要關注的事。

讓我們回到這個問題：你如何知道一個指定的數是不是質數？就原理而論，我們已經了解厄拉多塞氏之篩帶來了答案。我說“ 就原理而論 ”是因爲如果這個數太大，這個篩的方法可能就十分的不切實際。結果發現某些特殊的數有較快的方法。偉大的波蘭數學家 Hugo Steinhaus 的書 Mathematical Snapshots 中有下列刺激的命題：

含七十八位的數

$$2^{257} - 1 = 231,584,178,474,632,390,847,141,970,017,375,815,706,539,969,331,281,128,078,915,168,015,826,259,279,871,$$

是合成數；它能被證出來是有因數的，可是不知道它們是什麼。

這本書是我一度收到的耶誕禮物。我的父親——是個有點一板一眼的人（一個生物學家），他不以爲然的說：Steinhaus 的命題似乎是荒謬的，你如何知道一個數有因數而又不知道它們是什麼？我也不了解，可是我想它是相當巧妙的！事實上，這個“ 無法肯定 ”的定理（其中某人證明了有個數存在，而無法把它找出來）是我在 Steinhaus 的書中能記得的最重要的一件事。數年前我有個構想，這些事情是如何完成的。方法大概是這樣的：有個明顯的原理是說，如果你把七份印刷品放進六個信箱，那麼至少有一個信箱必須包含兩份或兩份以上的印刷品。換句話說，如果某個足球場有 100,000 個座位，而每個座位都坐了人，可是只賣出了 99,999 張票，那麼一定有某個人沒買

票溜了進來（設法把他找出來）。所以用“數”（ㄕㄨˋ）的方法常常能決定某事的存在性，而要把它找出來勢必需要一個澈底的搜索。事實上，如果所牽涉的數足夠大（就說是七十八位吧），那麼“澈底的搜索”就變成了“荒謬的搜索”——太陽系也沒有那麼多的原子！可是一個聰明的數學家也許就能“數”（ㄕㄨˋ）了；當然啦，不是一次一步的作，而是用“算術”。那就是在本質上，數學家對於他們不能眞正找到的數如何證明它們的存在性。

質數定理

直到現在我們考慮了主要的尚未解決、或部份解決、或偶然解決了的問題。讀者可能會懷疑這個主題中解決了什麼事。其中的巧妙的勝利成果之一現在把它叫作“質數定理”。追踪這個問題的歷史是很有趣的。它的題目是：求從0開始直到某個指定正數 x 的區間內質數的平均密度。例如，小於100的質數有25個。同樣的，我們能計算小於1000或小於1,000,000的質數個數等等。如果我們這樣作，我們就會發現質數的平均密度在減小。由此可得小於一百、一千、一百萬的質數個數是：

	質數 <100	質數 <1000	質數 <1000000
質數個數	25	168	78498
質數百分率	25%	16.8%	7.8%

就只看這個表，高斯與勒尖得在1800年左右作了不平常的臆測。他們注意到在不同區間內質數的個數似乎與函數 $\log x$ 有關，在那個時代似乎是種完全不能解釋的關係。

函數 $\log x$，有時稱之爲“自然對數”，起源於微積分中涉及成長與衰變有關的問題。例如，設有一筆利息爲100%之貸款，用複利計算，所以它就連續的成長（事實上100%的利息是高利貸，我們不必爲它煩惱）。於是 $\log x$ 代表了一元變成 x 元時所必須經過的年數。數學家把這種金錢在複利之下增加的過程叫作“指數成長律”（law of exponential growth）。把這種過程的描述稍加改變，就能合用於諸如此類的種種問題如人口成長，放射線衰變，物體冷却（甚至於複利以合理的利率計價）。

勒尖得與高斯所觀察到的是：比 x 小的質數的個數約接近於 $x/\log x$。這個近似值用百分率的術語來說就是“當 x 愈來愈大，成長得愈來愈好”（參閱圖2）。我們注意到甚至於 x 是十億時，錯誤的百分率仍然相當大。不過，高斯不僅僅是個數論家。他也建立了數學家的統計領域，把它應用到不同的問題上，如天文學與質數個數的計算。高斯用今天統計學家所謂的最小平方法來分析估計質數個數的誤差。他所得到的結論是 x 接近無限大時，誤差最後會趨近於零。

x	質數個數 $<x$	$x/\log x$	錯誤百分率
一千	168	144.8	16.0%
一百萬	78,498	72,382	8.4%
十億	50,847,478	48,254,942	5.4%

圖2 小於 x 的質數個數

這個“質數臆測”（它是個1800年的臆測）帶給數學家最不平常的衝擊。方程式的一邊是質數的個數；而另一邊的函數 $\log x$ 來自微積分，與人口成長有關。這是離散（discrete）與連續（continuous）的結合。

經過50年，沒有任何人能在高斯—勒尖得臆測的證明方面有任何進展。第一個這樣作的人是俄國數學家謝比雪夫（Pafnutii Chebychev），時間在1850年左右。他得到了部份結果，然後他的觀念被其他的人所模倣。可是最後發現他的方法不能再有大的進展，他們就放棄了。在1859年，一個德國科學院（Germany Academy of Sciences）新進人員里曼（Bernhard Riemann）利用了會員的一項特權——在院裡的雜誌發表論文（雖然他只不

過三十出頭，可是數年後就去世了）。他的八頁論文標題是“談談小於某定數的質數個數”，這篇論文非常的不完整，論據也有很大的漏洞，很少有肯定證明的部份。可是幾乎質數理論中所作過的每件事，自此之後都受到這篇論文的影響。

約有三十年之久，其他的數學家都想要證明里曼論文所宣佈的——可是並無所獲。最後在1894年（里曼論文出現之後三十五年），法國數學家阿達馬（Jacques Hadamard）獲得一次重要突破。然而高斯與勒尖得的最初臆測仍然沒有解決。可是沒有再持續多久，兩年之後，在1896年阿達馬與布松（de la Vallée Poussin）各自獨立的研究，證明了質數定理。

他們的證明（二人都是以里曼的研究爲基礎）用的是非常間接的方法。這些方法來自複變數函數論（高等微積分的一支），它用“虛”（imaginary）數。事實上，阿達馬在作以上的突破時，發展了某些新的複變數技術，並且這些技術以後被發現可以應用在無線電波動的理論上。他們能被用來證明一個濾波器（它是種設備，用以除去無線電信號中的靜電）是否可能毀掉信號中的資訊。

從一種成長中科學的觀點來看一切都十分美好。可是某些數學家感到不滿意。質數定理的證明太繞彎了，沒有人眞正了解它。他們對證明中的一步又一步都能了解——它是正確的——可是要說它與質數有什麼關係似乎是非常不容易發現的。又有數年人們尋求“基本”的證明，那就是只用質數的基本性質，而避免這些神秘的方法，諸如複變數與波動分析。這種發展又花了很長一段時間，可是大家所想要的那種形式的證明，最後在1948年被Atle Selberg與Paul Erdős發現了。無論如何，這種新的證明一如舊的證明，很難以了解。就“每一步都是基本的”的意義而論，它的技巧是“基本的”。可是有這麼多的步驟，把它們拼在一起的方式又這麼複雜，沒有出現一種簡單的生動描寫。或許說這是不能避免的。似乎有個“困難不滅”（conservation of difficulties）原理，一個難的定理就是難，不論你如何研究它。

里曼假說
(The Riemann Hypothesis)

我們的下一個例子比前面幾個要更爲技術性，爲了討論它我們必須要用幾個技術名詞。此外，由於它的重要性，省略它的話是很可惜的。里曼在前述1859年的論文中作了一個從未解決的臆測。這個臆測現在被叫作里曼假說，已經成了個陳腔爛調。它被當作非常困難或非常值得要的數學結果之標準模式。例如，當我是個大學生時，一度有個小小的研究合約。我表示了對自己能力的懷疑，是否能作出點任何有意義的事。我的指導教授對我保證說：「放心，他們並不指望你解出一個里曼假說來！」

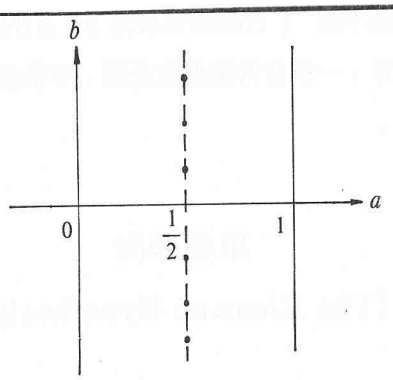
最初一眼瞥去，這個假說看起來是解除了武裝般的單純。它包括了某個方程式的很多解。對一個非專業人員來說，這個方程式似乎是複雜了些；而對學過微積分的大二學生來說，可以說是件件都很熟悉。我們可以很容易的寫下這個方程式，而沒有人知道如何解它。這裡是其中的形式之一：

$$1-\frac{1}{2^s}+\frac{1}{3^s}-\frac{1}{4^s}+\cdots\cdots=0$$

方程式中的未知數 s 是被假定爲複數，那就是說

$$s=a+ib\ ,\text{式中}\ i=\sqrt{-1}$$

里曼假說主張（有些著名的特殊例外）這個方程式的解都在複數平面的同一條直線上，其中 $a=\frac{1}{2}$（參閱圖3）。它的證明會自動包含對很多有關質數問題已知結果的劇烈改進。德國著名的數論家蘭杜（Edmund Landau）



$s = a + ib$ 代表了二維平面上某個位置。

• = 對里曼方程式解答的臆測。

里曼假設牽涉里曼方程式

$$1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots\cdots = 0$$

的解。已經知道的是（除了某些無關緊要的例外）這些解全部在陰影部份“重要的長條區域”內，並臆測它們全在這個長條區域的中心線上。這個臆測的證明對質數理論影響深遠。不過，自從 1859 年里曼作了這個臆測，到現在仍然沒有證出來。

圖3 里曼假說

認爲此事非常重要，1927年在他有名的著作 Vorlesungen über Zahlentheorie 裡，有一整章標題是“在里曼假說的假設之下”。在這章裡，他並沒有證明任何定理，只不過是告訴大家，那些“定理”可從里曼假說導出。

里曼方程式有無限多個解——對它所知就這麼多——其中重要的都在複數平面上某個無限長的長條區域內。里曼假說主張這些解都在此一長條區域的中心線上。稍早我們特別提到威斯康新大學三位數學家，用一部電腦證實了這一點對最初的三百萬個解是正確的。可是前面我們也特別指出，在電腦搜索範圍之外的無限多個解，這種電腦的結果是什麼也證明不了的。

從純理論來說有另外一個觀點。因爲解答是限制在一個無限的長條區域內，我們能想到它們是以一定的次序開始的，就像公路上的汽車一樣。用這個方式來看此一問題，我們要問是否能（因爲我們不能證明里曼假說）至少證明這些解答的正百分之幾在這條重要的直線上。這是 1942 年 Selberg 所完成的。不過 Selberg 所能建立的百分比極端小——一個極小分數的百分之一。在 1974 年 MIT 的 Norman Levison 成功的證明了全部解答至少有三分之一在這條重要直線上。

Levinson 早期的工作並不是數論，而是常微分方程式，是與數學的物理領域有關連的。他於致癌去世前不久才開始研究里曼假說。因而是在他長而傑出的生涯的末期才得到這項極了不起的成就。這個事實應該有助於驅散一個觀念：數學是年輕人的競技。

方程式的整數解

還記得前面我們考慮過的方程式 $x^2 = 2y^4 - 1$ 嗎？它恰有兩個正整數解，那就是 $x = 1$，$y = 1$，與——頗爲有趣的——一對數值 $x = 239$，$y = 13$。

只用整數解方程式的理論叫作“Diophantine 方程式”以紀念古希臘的 Diophantus，是由他創始的。因爲命題本身固有的單純，從古代直至目前，這個理論仍然是數論的中心。數學家的感覺是既然這個方程式看來這麼簡單，就應該能解它們！不過，就像讀者現在可以猜得到的：通常這是辦不到的。我們再次邂逅了——敍述單純而證明困難到幾乎無法克服——的對照，就是這種對照使數論一直保持爲一種繼續活動的研究科學。

我們的第一個方程式只有兩個解（它的意

義當然是指整數解），而問題自然就來了：這些Diophantine 方程式全都是只包含有限個解嗎？如果是的話，是不是有某種方法把它們找出來？

第一個問題的答案爲否。例如，方程式

$$x^2 - 2y^2 = 1$$

有無限個正整數的解。最初幾個是 $x = 3$，$y = 2$；然後是 $x = 17$，$y = 12$；然後是 $x = 99$，$y = 70$；……。讀者可能會奇怪這些解答是如何發現的。實際上它們有個公式，在下面的方塊中曾予討論。

一個Diophantine 方程式的解

解方程式

$$x^2 - 2y^2 = 1$$

我們有個一般的公式。它是這樣的：
若 x，y 爲一組解，那麼用下列公式

$$x' = 3x + 4y$$
$$y' = 2x + 3y$$

得到一組新的解。例如，設 $x = 3$，$y = 2$（它滿足原來的方程式，$3^2 - 2 \cdot 2^2 = 1$），得 $x' = 17$，$y' = 12$；這一組解也能奏效，因爲 $17^2 - 2 \cdot 12^2 = 289 - 288 = 1$。爲了驗證這一招是否永遠管用，只要把以上公式代入 $x'^2 - 2y'^2$ 中計算一下就行了。

所以，某些Diophantine方程式只包含有限個解，而其它的有無限個解。它們的差別在那裡？在任何肯定的答案出現之前，人類對這一點困惑了很久。費馬（Pierre de Fermat），在1600年左右是第一個證明 Diophantine 方程式有什麼意義的人。

這裡有個旁白：費馬有個惱人的習慣，那就是從不寫下證明。因此他的後繼人如尤拉，必須把一切重行來過。於是問題就來了：既然他從來就沒有把它們寫下來，我們又如何知道費馬眞正的證明了他的命題？好啦，他說他作過了，而他是個很聰明的人。還有，他確實對他的方法作了某些提示。最後，幾乎他所說過的每件事以後都被證明爲眞（只有一樣重要的例外）。這個例外是著名的“費馬最後定理”。它主張若 x、y、z 均爲異於零之整數，若整數 $n > 2$，則方程式

$$x^n + y^n = z^n$$

無解。如果讀者曾讀過其它的任何數論報告，他或許看過這個方程式——那是標準的話題之一。所以在這一節我們要讓費馬最後定理站一邊去。沒有人曾經把它證出來（除非費馬自己作過）。

過了很長的一段時間，沒有眞正的所謂 Diophantine 方程式論這種玩意兒。每個單獨的方程式，如果它最後是能解的，都只需要與該方程式有關的特殊理論。一個方程式——一種理論，最後逐漸令人厭倦，在十九世紀末葉 Diophantine 方程式不再受到歡迎。

然後在 1909 年，挪威數學家 Axel Thue 宣佈的結果，爲這個主題展開了一種完全不同的方式。再來回憶一下我們較早的問題：爲什麼有些 Diophantine 方程式只有有限個解，而其它的却有無限個解？Thue 的結果本質上回答了這個問題。第一個方程式

$$x^2 = 2y^4 - 1$$

只有有限個解，因爲它是“4次”——意思是說有一項 $2y^4$ 指數是 4。Thue 證明（我們略去了某些技巧的限制）了含兩個未知數 x、y 而次數爲 3 或更高次的方程式只有有限個解。（另一方面來說，二次方程式——如 $x^2 - 2y^2 = 1$ —— 就的確有無限個解。）

Thue 的定理是 Diophantine 方程式領域中第一個眞正的普遍結果——因爲它應用於多種的方程式，而不是只針對一個特殊的方程式

。可是，它有個主要的毛病。它的證明並不是邏輯上的“有效”（effective）。這是什麼意思？爲了探討這個觀念，我要開始提到另一個最近解決的著名問題。

高斯在他著名的Disquistiones Arithmecae書中介紹了某種類的數。不必管它的定義。高斯認爲它們是重要的，我們就把它們叫作“高斯數”。高斯成功的找出了九個這種數；它們是

$$1, 2, 3, 7, 11, 19, 43, 67, 163$$

他推測一共只存在着九個這種數，可是他不能證明。從1800年到1934年別人也證不出來。然後在1934年H. Heilbronn與E.H. Linfoot證明了至多只有十個高斯數！高斯找到了九個，而Heilbronn與Linfoot證明最多只有十個。可是對於這第十個：到底它存在不存在，Heilbronn與Linfoot的證明並沒有留下線索。如果它是存在的，他們並沒有說明把它找出來的方法；如果你沒有找到，他們也沒有一種肯定的方法來告訴你，它不在你計算範圍之外的某個地方。這個“第十個高斯數”可能存在也可能是個孤魂野鬼。

這就是我們所謂的邏輯上的“無效”證明。

最近Diophantine方程式的進展，絕對多數是包括了把以前無效的討論轉換成有效的。高斯問題是在1966年被美國數學家Harold Stark解決了。他證明了只有九個高斯數；第十個並不眞正存在——這是自始至終每個人都相信的。而就在同時，英國數學家Alan Baker給了Thue理論一個“有效”的基礎。這一點有很廣泛的影響，而結局尚難預料。我們只提出Baker理論的一種應用作爲結束。由此，在荷蘭的Tijdeman最近在解決一百歲的Caltalan問題上有了實質的進步。他證明的是，除了有限個可能的例外情形，只有兩個整數的乘冪——平方，或立方或四次冪等等——相差恰巧是1。它們自然是3^2與2^3，那就是9與8。（右側的方塊更爲仔細的研究Tijdeman定理。）

Catalan問題的Tijdeman近似解

Catalan問題所關注的是整數的乘冪，那就是

平　方：1, 4, 9, 16, 25, ……

立　方：1, 8, 27, ……

四次冪：1, 16, ……

等等。

（我們沒有把一次冪算在內，因爲每個整數都是一次冪，也就乏善可陳了。）

一百多年以前，Catalan推測兩個整數的乘冪，相差恰巧是1的只有3^2與2^3，那就是說9與8。最近R. Tijdeman在荷蘭用英國數學家A. Baker的觀念幾乎證明了這個推測，只有有限個情況未處理。

〔“例外情形”的個數雖然是有限的，用電腦來解決是太大了，在Catalan問題完全被解決之前需要另一種觀念。數論中出現的幾個不規則的大數例子，在本文中其它各處可以看到。〕

對於Catalan推測看得更仔細一些是很有趣的。我們回想一下，它包括了所有整數的乘冪（平方、立方等等）。經過檢查，我們發現有的整數乘冪相差是1：

9與8　（那就是$3^2 - 2^3 = 1$）

有的是2

27與25　（那就是$3^3 - 5^2 = 2$）

有的是3

128與125　（那就是$2^7 - 5^3 = 3$）

有的是4，它有兩種方式：

125與121　（那就是$5^3 - 11^2 = 4$）

8與4　（那就是$2^3 - 2^2 = 4$）

這要到何處停止呢？並且在那種情況有好幾個解？Catalan的推測說，相差爲1時，只有9與8這一組解。

舊的與新的

在這最後一節裡，我們要描述數論中最古老的結果之一，最近如何在電子計算機程式設計中發現了一項應用。這個古老的結果叫作“中國餘數定理”；它被古代中國人用來預言天文學週期的一段共同週期。這個對程式設計的應用包括了獲得“雙倍精確”（multiple precision）的意願——那就是說要機器求出比它正常設計的更爲精確。

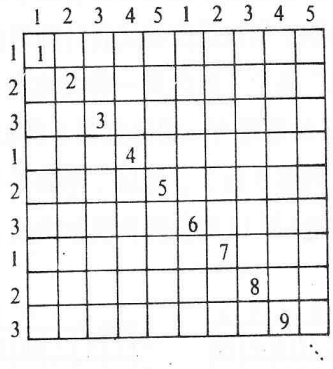
從一些老生常談的事情開始：每個人都知道“單與雙”的觀念——兒童玩石子遊戲時用它，並且在澳洲人們解決爭論時會說“讓五是雙的”（意思是說“你願意怎麼辦就怎麼辦，我可不願意爲了它打一架”）。當然啦，“單與雙”的觀念必須用到2這個數。有個較少爲人所知的事實是：類似於“單與雙”的觀念，它應用於3以及更大的數。就拿3來說吧。假想要把一群學生分成三隊；典型的作法是老師要學生排成一列並要他們報數：“一，二，三，一，二，三，一……”學生們就被分成三組了，而這種處理是循環的——“一”跟着的是“二”再跟着的是“三”再回到“一”。（注意，如果不用“單與雙”，學生報數用“一，二，一，二，一，二……”時的關係又如何呢？那時所有的“一”都要在單的位置——第1，第3，第5，等等。——而所有的“二”都在雙的位置。）

把這種觀念擴展到三的週期就叫作“模3的同餘”，並且較長的週期也是可能的。好啦，週期的事件是一直會發生的：星期，年，月的盈虧，等等。古代中國人在研究天文學上的週期導致下列問題：當你把兩個週期事件合併的時候會發生什麼事呢：就說是星期與年吧。然後這種模式的出現是十分值得注意的。有幾個例子展示了不同的可能性，見本頁之方塊。

中國餘數定理

我們要以週期爲3與5的個案來說明這個定理。注意3·5＝15。中國餘數定理說，1，2，3，……15等十五個數如果用某種方式安排，就會填滿一個3×5的方塊：

	1	2	3	4	5
1	1	7	13	4	10
2	11	2	8	14	5
3	6	12	3	9	15



下邊的圖形有很多個3×5的方塊，如果我們把對應圖案附加上去，就得到了上邊的圖形。它相當像一個有技巧的攝影師慣於作出多重畫面。在這兩個圖形中我們的計算都是從上而下從左而右。它的意思是說垂直與水平的位置（“模3”與“模5”）在每一進程都是前進一步。注意，從“3到4”的移動次序是如何從左上往右下而失去踪影，又再度出現於上方的。當然啦，在下方的圖形中，4是在一個不同的方塊中。

中國餘數定理所說的只不過是小的矩形中全部空間都填滿了。這種事一定會發生是明顯的嗎？讓我們看另外一個個案，“週期”是4與6：

	1	2	3	4	5	6
1	1		9		5	
2		2		10		6
3	7		3		11	
4		8		4		12

1

13要去的空間已經被1填入了，所以只有一半的正方形被填滿了。這是那裡不對勁兒了？麻煩是在於4與6都是公因子2的倍數。在這種情況下，就會有麻煩；然而在矩形兩邊沒有公因子時，就諸事順遂，一如它們在第一個圖形中的表現。（有一種方法可以保證沒有公因數，就是讓兩個邊都是質數；因爲質數除了1與本身之外別無其它因數。）

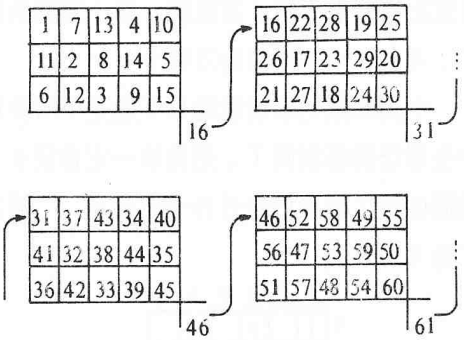
現在來談談電子計算機：假想一個“嬰兒電子計算機”，它只能應付1至5這幾個數（當然啦，這應該是個相當笨的電子計算機）。假設有個程式設計師用這部機器，需要1到15這幾個數。這個機器喜歡小的數而拒絕大的數。所以這位程式設計師用兩個小的數（或“碼”）來代表一個大的數。每個從1至15的數都有一定的位置（例如，10是在第1列第5行）。所以，兩個不大於5的數足夠把1到15的任何數表示出來。

	1	2	3	4	5
1	1	7	13	4	10
2	11	2	8	14	5
3	6	12	3	9	15

	1	2	3	4	5
1	1	4	7	10	13
2	2	5	8	11	14
3	3	6	9	12	15

A碼“CRT”碼　B碼　較爲笨拙的碼

此外，多疑的讀者也許會問：爲什麼要這麼麻煩？爲什麼不用一種較容易的碼，就如“B碼”中所示。這個問題的答案之一由下圖間接表明。



CRT在程式中設計時有用的理由是：對於加法與乘法的基本運算它表現得很“一致”。爲了瞭解這個概念，假設我們把注意力集中在其中兩行，就說是第2行與第3行吧。從這兩行中隨機選出兩個數，它們是2與13。然後2·13＝26的乘積就在第一行（在它自己的方塊中）。不論我們選那一個數都有這種結果，只要它們是來自第2行與第3行的。

再試試看，仍然用第2行與第3行的：取12與3。然後12·3＝36仍然是在第1行（雖然是在一個不同的方塊內）。

再多試一次：取12·13＝156，它脫離了方塊的範圍，可是如果以上的圖案再繼續下去，156會落在第1行。

對其它行來說類似的事一樣可行。對於列來說也是一樣。例如，第2列任意二數之積會在它那個適當方塊中第1列出現。（例：2·14＝28）

這裡就是電子計算機如何利用這些性質作計算。就說是電子計算機必須把2與8相乘吧。電子計算機讀這些數是這樣的

2：第2列，第2行
8：第2列，第3行

我們已經了解，所以說

（第2列）·（第2列）＝（第1列）
（第2行）·（第3行）＝（第1行）

所以2·8應該在第1列第1行。而事實上確實如此：2·8＝16，而16在它那個方塊中的第1列，第1行。

“呆板的”B碼沒有這種性質。

我們要談一點這些“古代智慧”如何產生了現代電子計算機程式設計的一種應用。電子計算機是作成能處理某種大小的“字”（words）的。當然啦，設計電子計算機的人要選出合理的“字長”（word length，這是個電子計算機的行話，它是電子計算機能指揮管理

的數的位數：例如，21有兩位，而4,172,316有七位）。如果數的位數太小，機器就沒有用處，而位數太多又造成浪費。正常情況下位數允許有十五位左右。可是有的時候我們需要更多的位數。因爲電子計算機是內部設計好，只處理某種長度的“字”，如果你要改變字的長度是會惹火它的。當一個程式設計師需要較大的位數，他時常會發現不要碰機器硬體——也就是說——在軟體上動點手脚。

來談談它的概念，假想一部電子計算機能指揮管理的數可以十五位。現在，假設我們需要三十位。這部機器喜歡“小的”數（十五位），拒絕大的數。所以程式設計師用兩個小的數來代表（或寫碼code）一個較大的數。它的作法有很多種。最簡單的就是只把這個大的數分成兩個較小的數（就像是把2143分成21與43）。可是這不是最好的方法。用這種粗枝大葉的方式來把一個數分成兩個，它的麻煩是導致了相當混亂的“計算”，何況，這部機器不一定要作得能處理這種混亂。（當然啦，程式設計師應該把它想清楚；問題在於如果程式設計師必須把它想清楚，他就要浪費很多時間。）非常奇怪的，對很多目標來說，這個上千歲的中國餘數定理，帶來了最有效的方法解決這個問題。

在結束這篇文章之時，我要對數論在數學中的地位以及它與應用科學的關係作一些觀察。數論被高斯叫作“數學的女王”，也被不喜歡它的人叫作“一種無用的科目”。關於這一點，也許我們注意到高斯也把數學叫作“科學的女王”，因爲所有的它種科學都是從它萌芽的。很明顯的，數的觀念存在於數學的核心；問題是對於數的有系統研究，其中有多少是有助於應用科學——又，在什麼方式下。

數論對其它科目的一些應用已在本文中提過。此外，電子計算機發展的趨勢，資訊理論與有關領域使我們想到數論在將來會應用得更爲廣泛。（一件很類似的事發生在五十年前一種叫作“群論”的科目上：這種以前的“純”領域——自1825年左右爲數學家所研究的——竟然成爲新量子力學的一項極重要工具。）

還有，假定這些應用是數學家研究數論的主要理由——就未免太天眞了。當我們要把很少的應用與從事增強此科目所作極大努力作相對的比較時，這一點就變得特別明朗。爲什麼有人作這方面的努力？爲什麼像尤拉這樣的偉大數學家——一個在數學每一分支實際都有貢獻的人，他的全集的貢獻超過了大英百科全書全部頁數——很多年來都花部分時間試圖證明四平方數定理（未能成功）？答案是這樣的，數學家是職業性的，以數學爲職志的數學家熱愛他們行業。

法國數學家Henri Poincare要把一流數學家與二流數學間的特徵加以區別，他說“有的問題是有人質問的，也有的問題是問題本身質問的”。無疑的本章所考慮的數論問題“自己質問本身”。極端單純的命題，結合了困難的證明，把它們標記爲眞正的問題。此外，這種問題的解導致了整體理論的發展。

一個好的定理對以後的數學發展幾乎永遠會有廣泛的影響，只因爲事實上它是正確的。因爲它是正確的，一定有某些理由使它正確；如果那個理由是深藏不露的，那麼這種理由的披露，通常是需要對它接近的事實與原理有較深的了解。就這方面來說，數論——數學中的女王——一直是個試金石，很多數學的其他分支上的工具都被拿來測試過。事實上，這就是數論影響純數學與應用數學的眞正方式。

進一步讀物建議

一般性：都有中譯本，

專門性：

H. Davenport，*The Higher Aritheme-tic*

這是一本吸引人的書，介紹關於較現代的代數數論，別被它的書名誤導了——這本

拉格蘭自——尤拉的主要對手，十八世記兩個最偉大數學家之一——拉格蘭自個性特異。尤拉是虔誠的，而拉格蘭自是懷疑論者，尤拉是難以置信的多產作家，而拉格蘭自只把他最光輝的觀念出版。可是二人在數學上所造成的衝擊幾乎相等。拉格蘭自是個慷慨的人，對一個時常竊取他的觀念的年輕數學家甚至到了原諒並要幫助他的地步。然而到了晚年他感到他的數學能力走下坡時就有憂鬱的傾向以致於絕望。（像片獲“Germanisches National Museum,”Nuremberg之同意）

書只有認眞的學生才能唸。

Godfrey. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*

除了前兩章外，這本書相當難。不過關於數論的書也沒有眞正容易的。這本書是經典之作，每章討論一個不同的題材，各章之間相當獨立。

A. E. Ingham. *The Distribution of Prime numbers.*

這是用英文寫的關於此題材最好的介紹，文體非常清晰。用小字印的章節非常好，它讓你明白一個好奇的人，在了解主要問題的解答後，怎樣去找新的問題。需要複變函數論的知識。

—本文作者現任教於台北市立建國中學—