科技文化

僕人與皇后

——談談數論和它的應用

•王　元

一　數論是甚麼？

數論是研究數的規律，特別是研究整數性質的數學分支。它與幾何學一樣，是最古老的數學分支。從方法上講，數論可以分成初等數論、解析數論與代數數論。

數論的問題往往來自對於數的觀察，先根據一些感性知識，提出「猜想」，然後再通過嚴格的邏輯推導來論證它，被證明了的「猜想」就變成「定理」，但也有不少猜想被否定了。以下我們就數論中幾個重要領域來說明它所研究的問題。

甲　素數的分佈

自然數分成 1、素數與複合數三類。歐幾里德 (Euclid) 證明了「每個複合數均可以唯一地表示為素數的乘積」，這稱為算術基本定理。所以素數分佈的研究是最古老的數論研究課題之一。歐幾里德還證明了「素數有無窮多」這一重要定理。但也有些「猜想」被否定了。例如費馬 (P. de Fermat) 曾猜想形如 $F_n=2^{2^n}+1$ $(n=0,1,\ldots)$的數都是素數。當 $n=0,1,2,3,4$ 時，這一猜想是對的。歐拉 (L. Euler) 首先找出$F_5=4{,}294{,}967{,}297$的因子分解：

$$F_5 = 641 \times 6700417$$

所以費馬的猜想就被歐拉否定了。素數論中有所謂貝特朗 (J. Bertrand) 假設，即當 $x\geqq 1$ 時，在 x 與 2x 之間必定有一個素數。這一猜想是切比雪夫 (P.L. Chebysev) 證明的：以 P_n 表示第 n 個素數，那麼由貝特朗假設可以推出區間$[2^n, 2^{n+1}]$ $(n=0,1,2,\ldots)$中都有素數，所以素數有無窮多，而且 $P_n \leqq 2^n$。因此切比雪夫定理比歐幾里德定理深刻得多。但人們並不就此滿足，切比雪夫定理是說

$$P_{n+1} - P_n \leqq 3P_n$$

或用略不精密的語言將上述結論寫作 $P_{n+1}-P_n=O(P_n)$。人們猜想

$$P_{n+1}-P_n=O(P_n^{1/2}\log P_n)$$

這一猜想是尚未證明的黎曼 (B. Riemann) 的推論。

乙　不定方程組的解

數論另一個傳統領域是不定方程組的求解問題。所謂不定方程組是指方程的變數個數多於方程個數。我們要求方程組的整數解，或在整數的子集，例如全體素數上求解。中國古代的孫子定理(或稱中國剩餘定理)，即某種線性不定方程組的求解定理。數論也研究定義於自然數上的函數，即所謂數論函數的性質。例如命 $r(n)$表示 $u^2+v^2=n$ 的整數解個數，$d(n)$表示 n 的因子個數。則 $\sum_{n=1}^{x} r(n)$ 與 $\sum_{n=1}^{x} d(n)$ 分別表示圓 $u^2+v^2\leq x$ 與區域 $uv\leq x, u\geq 1, v\geq 1$中的格子點$(u,v)$的個數。粗略地說，可以用這兩個區域的面積來估計其中格子點的個數，但誤差是多少呢？猜想應該是 $O(x^{\frac{1}{4}+\varepsilon})$，其中 ε 為任意正數。這是兩個未解決的歷史難題。

丙　有理逼近

數論還有一個領域是實數組的有理逼近問題。例如中國古代的何承天與祖冲之分別建議用$\frac{22}{7}$(這稱為約率)與$\frac{355}{113}$(這稱為密率)來逼近π。又如命α為一個實代數數，即整係數代數方程的根。羅斯 (K.F. Roth) 證明了對於任意$\varepsilon>0$，皆有 $|\alpha-\frac{h}{q}|\geq c(\varepsilon)/q^{2+\varepsilon}$，其中 $c(\varepsilon)$為僅依賴於 ε 的正常數。這一歷史難題的解決使羅斯得到了1958年頒發的菲爾茲 (Fields) 獎。現在羅斯定理又由施密特(W.M. Schmidt) 推廣到聯立逼近情況。這樣看來，數論似乎純粹是出於數學家個人興趣與愛好而去研究的一門學問了。

二　數論和數學整體的關係

數論有用處嗎？誰也不懷疑，許多數學分支之所以存在，應該歸功於「現實世界」提出的問題，例如物理學、工程技術等提出的問題。熟知的例子有微積分，天體力學中需要的微分方程理論，以及流體力學中必不可少的偏微分方程，等等。但是，數論又怎麼樣呢？有一點是確鑿無疑的，就是費馬、歐拉 (L. Euler)、拉格朗日 (J.L. Lagrange)、勒讓達 (A.M. Legendre)、高斯 (C.F. Gauss) 等大師都是出自數論內在的趣味及其特有的優美而去探究人類知識這一領域的，他們確實毫不在乎那些優美的定理是否會有甚麼「實際的」應用。

圖 希爾伯特(左)、歐拉(右)。

高斯把數論置於科學之巔，他把數論描繪成「一座倉庫，貯藏着用之不盡的，能引起人們興趣的真理」。希爾伯特 (D. Hilbert) 則把數論看成「一幢出奇地美麗而又和諧的大廈」，「它有簡單的基本定律，它有直接了當的概念，它有純正的真理」。明可夫斯基 (H. Minkowski) 比喻數論「以柔美的旋律來演奏強有力數論音樂」。總之，對他們來說，數論是「純正潔白」的。高斯有如下名言：「數學是科學的皇后，數論乃數學之皇后。」

然而，隨着數學的深入發展，其他強有力的數學工具開始滲透到數論研究中去。由於數論問題的簡單明瞭，往往會導至研究深化。由此產生的概念、結果與方法對其他數學領域的影響也日見明顯。1900年，希爾伯特在第二屆國際數學大會的著名報告中，以「三體問題」與「費馬問題」作為例子來說明一個好的問題對於推動數學發展的作用。三體問題是天文學提出的最基本的自然現象問題，費馬問題如何能跟三體問題相提並論？所謂費馬問題是說，不定方程

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

當 $n\geqq 3$ 時沒有非尋常解：$x=0$，$y=z$，或 $y=0$，$x=z$ 稱為尋常解。這樣一個非常特殊、似乎不重要的問題，卻對數學產生了難以估量的影響。受這個問題的啟發，庫默爾 (E.E. Kummer) 引進了理想數，並發現分圓域的素理想數因子分解定理。這個定理又被戴德金 (D.W.R. Dedekind) 與克羅內科 (L. Kronecker) 推廣到任意代數數域，其意義已遠遠超出數論的範圍，而深入到代數與函數論的領域。

我們還可以舉哥德巴赫 (C. Goldbach) 猜想為例。所謂哥德巴赫猜想是說，不定方程

$$2n = p + q$$

有素數解 p, q，此處 $n\geqq 2$ 為任意給定整數。由於研究這一孤立問題，帶動了解析數論一些強有力的方法的產生與發展。例如哈代 (G.H. Hardy)、李特伍

德 (J.E. Littlewood) 與拉馬努揚 (S. Ramanujan) 的圓法；維諾格拉朵夫 (I.M. Vinogradov) 的素變數三角和估計方法；僕朗 (V. Brun)、賽爾伯格 (A. Selberg)、與陳景潤的篩法；列尼克 (YU. V. Linnik)、瑞尼 (A. Renyi)、潘承洞與朋比尼 (E. Bombieri) 的大篩法與素數分佈論。這些方法不僅是解析數論的強有力工具，而且對其他數學領域亦有應用與影響。

因此，數論不再是數學的一個孤立分支，這一觀點已成為共識。華羅庚在他的《數論導引》(北京科學出版社，1957)的序言中首先強調了這一論點：

「其一，希望能通過本書具體地說明一下數論和數學中其他部分的關係。」「但是在今天的數論入門書中往往不能看出這一關聯性，並且有一些『自給自足』的數論入門書會給讀者以不正確的印象：就是數論是數學中的一個孤立的分支。」「作者試圖在本書中就初等數論的範圍盡可能地說明這一點。例如素數定理與傅利葉 (J.B.J. Fourier) 積分的關係。因為受本書性質的限制，我們不能把素數定理和整函數的關係在本書中敍出：整數之分拆問題，四平方和問題與模函數論的關係；二次型論，模變換與羅巴切夫斯基 (N.I. Lobacevski) 幾何的關係等。」

其次，數論是研究整數規律的數學分支，它的概念與結果構成抽象數學的概念與方法的背景之一，而且也是促進數學發展的內部泉源之一。數論的這個功能也幾乎是共識的。在同一序言中華羅庚說：

「其二，從具體到抽象，是數學發展的一條重要大道，因此具體的例子往往是抽象概念的源泉，而所用的方法也往往是高深數學裏所用的方法的依據」。「從數學本身來說，它研究的最基本的對象是『數』與『形』。因此，『幾何圖形』所引出的幾何直覺，和由『數』而引出的具體關係和概念往往是數學中極豐富的源泉」。

中國大陸在文化革命結束前，發展數學的哲學思想是只承認數學發展的外部動力，而不承認其內部動力。這必然導至數學發展上的實用主義傾向，甚至

圖 華羅庚

發展到學術上的虛無主義，否定歷史上一切數學成果。因此，相當長時間中，數學的正常發展受到嚴重阻礙。

三　數論的實際應用

除了上述兩個功能外，數論有更直接的「應用」嗎？

50年代以來，電腦蓬勃發展，它的應用滲透到各個科學領域，大大開闊了人們的眼界，引起人們重新檢查過去積累的科技成果、方法直至觀念。數學除用於傳統學科，如物理學、力學、天文學與工程技術之外，在科學計算、生物科學、地學科學、計量經濟學、管理科學，乃至社會科學中都有應用。這些科學都需要從定性研究向定量研究深入發展。同時，離散數學顯得日益重要，它已逐漸取得與連續數學同等的地位。因此，在愈來愈多的場合，人們需要用數論的概念、結果與方法。事物總是由量變到質變的。數論的應用也由零散的應用達到系統應用，由應用數論的一般成果到應用最深刻的數論成果，甚至形成專門的數論應用分支。

甲　數值積分與近似計算

50年代末興起的近似分析中的數論方法，是以計算多重定積分為研究主題的。積分近似計算是一個古老的課題，它與微積分學同時誕生：牛頓 (I. Newton) 本人就是一位數值積分專家。著名的牛頓—柯斯 (R. Cotes) 公式包括了梯形公式 (trapezoid rule) 與辛卜生公式 (Simpson's rule) 作為特例：而車比雪夫 (P.L. Chebycev)、埃爾米特 (C. Hermite) 與高斯都曾對數值積分問題作過傑出貢獻。但他們的工作都是屬於一維數值積分的範疇。若將這些公式推廣到高維空間，則誤差將隨維數迅速增加，所以這些方法在高維空間都是無效的。直到50年代末，多維數值積分的論文還是寥若晨星。但原因並不是當時的純粹數學積累不够，不足以研究多維數值積分問題，關鍵在於計算工具落後，即使研究出新方法，亦無法進行實際使用，仍然是紙上談兵，引不起大家的興趣與注意。由馮諾依曼 (J. von Neumann) 與烏拉姆 (S. Ulam) 在40年代首創的所謂數值積分的蒙特卡羅 (Monte Carlo) 方法的要點，是將一個分析問題，如數值積分，化為一個有同樣解答的概率問題，如某隨機函數的數學期待值的計算，然後用統計模擬方法來處理後一問題。這就需要應用服從均勻分佈的獨立樣本，或稱隨機數(random number)。但隨機數如何產生？實際上所有產生隨機數的方法仍然是「確定性」的，即按一定數學程序來產生。數值積分中的數論方法就是給出一組在空間中均勻分佈的點列，用它代替真正的隨機數來構造多維求積公式。這組點列稱為「偽 (quasi) 隨機數」，而數論方法也稱為「偽蒙特卡羅方法」。

這一方法是成功的，求積公式的誤差主階與維數無關。首先是卡羅波夫(N.M. Korobov)在1957年給出了一個公式，他的方法基於完整三角和的估計。50年代末與60年代初，卡羅波夫、華羅庚、那夫卡 (E. Hlawka) 與哈爾頓 (J. H. Halton) 等先後發表了他們的方法。這些方法涉及到指數和估計、一致分佈論、丟番圖逼近論與經典代數數論的應用，甚至用到數論中最深刻的成果之一：吐埃—西革爾—羅斯—斯密特 (A. Thue, C.L. Siegel, K.F. Roth, W.M. Schmidt) 定理。現在人們正在嘗試用數論方法來處理插入公式、積分方程與偏微分方程的近似計算：並嘗試用之於試驗設計安排，最優化計算與統計模擬問題等，它已經逐步形成一個理論上與實際應用上頗有成效的新數學領域。

乙　密碼與「活板門函數」

數論另一個重要而饒有興趣的實用領域是密碼學(cryptography)。現在密碼問題已不再像過去那樣，僅僅用於軍事與外交等少數領域。隨着科學技術的不斷發展，在更廣大的領域，如財務、金融與銀行業務往來等方面都要用到密碼。因此密碼的設計不能像過去那樣採取事先約定的密約方式，而需要不太複雜的發碼與破譯手續。密碼最好是「公開的」的，但若接收者不掌握「破約」，則無法進行破譯。用這種思想設計的密碼理論稱為「公約密碼學」(public key cryptography)，這是70年代末開始的一門學問，至今才有十來年歷史。

公約密碼設計主要是倚靠一個「活板門函數」(trap-door function)。甚麼是活板門函數呢？它是這樣的：在一個方向很容易計算，但在反方向，則極難計算。例如，用電腦很快可以將兩個 1000 位數乘起來；反過來，如果已知一個 2000 位數是兩個約 1000 位的素數之積，要求出這兩個素數來，則除了某些簡單情形外，即使用最先進的電腦與程序，在今天仍然是遙不可及的事。用這思想構造出的一種公約密碼，稱為 RSA (L.M. Adleman, R.L. Rivest, A. Shamir) 密碼。它的原理是這樣的：

第一，發碼和收碼者先約定兩個「公開碼匙」，這是 n 和 s 兩個數，其中 n 是兩個極大(譬如上千位)素數 p, q 的乘積，而且 n, s **互素**：p, q 是不公開的，只有收碼者知道。第二，發碼者用公開而固定的方法把信息中的字轉變為數字M。例如用 0, 1, 2, … 25代表 a, b, … z 這二十六個字母，那麼 'YES' 這個字便可以用 $M=24q^2+4q+18q^0$ 代表，其中 q 是等於 26 的約定數。例如 q=26時，M=16346。

互　素　a, b「互素」即最大公約數是 1 的意思，一般以 (a, b)=1 表示，例如 (12, 25)=1。

同餘式　$a \equiv b \pmod{n}$ 即 a−b 可以被 n 整除，沒有餘數的意思，因此必然有整數 k 令 a=b+kn 成立。

n, M 一般也是互素的。第三，發碼者以 n 除 M^s，所得的餘數 C 就是代表 M 的密碼，這可以用「同餘式」表示：

$$M^s \equiv C(\text{mod } n)$$

密碼 C 是公開發給收碼者的，收到後便可以用下列辦法輕易解碼（見旁列的「說明方塊」）：以 n 除 C 的 t 次方，所得餘數便是代表信息的 M。即

$$C^t \equiv M(\text{mod } n)$$

上式中的 t 由「明匙」s, n 以及 n 的因子 p, q 決定：令 $\Phi=(p-1)(q-1)$，則 t 是適合

$$st \equiv 1(\text{mod } \Phi)$$

的數。旁人即使知道了明匙並且接到密碼 C，但倘若不知道 n 的因子，那麼以目前的數論積累和電腦技術來說，當 n 稍大時還是遠遠無法求出 p, q，以決定 Φ, t 去解碼的。

歐拉定理 (Euler's theorem)

若 $n=pq$，其中 p, q 是素數，而 $\Phi=(p-1)(q-1)$，那麼對任何滿足 $(a, n)=1$ 的數 a，

$$a^{\Phi} \equiv 1(\text{mod } n)$$

必然成立。例如 $p=3, q=5, n=15$，$\Phi=8$；若 $a=7$（它和15互素）則 $a^{\Phi}-1=7^8-1=576{,}480$，這是15的倍數。

文中解碼方法的證明

由 t 的定義可得 $M^{st}-M=M^{1+k\Phi}-M=M(M^{k\Phi}-1)\equiv O(\text{mod } n)$，最後一步即是由歐拉定理而來；另一方面，用普通的因子分解以及 C 的定義可得 $M^{st}-C^t=(M^s-C)\times$整數 $\equiv O(\text{mod } n)$。把上述兩式合併即得所求的 $C^t \equiv M(\text{mod } n)$。

另外一個活板門函數是「離散對數」，它也可以用來設計公約密碼。上面這些方法的破譯都歸結為如何快速有效地將正整數分解成素因子之積，因此，這個數論最古老、最基本的課題現在又熱起來了，在這一課題的最新研究中，甚至用到橢圓曲線 (elliptic curves) 的高深理論。

*　　*　　*

數論應用在近三十年來的發展，已改變了傳統對數論的看法，也改變了50年代對數論功能的認識。1990年，革萊姆 (R. Graham)在科羅拉多大學一次公開演講中宣稱：「現在，數論是最有用的數學分支」。這一斷言說明，數論是科學與數學最忠實而有用的僕人。數論由皇后變成僕人，或應該說，在皇后的寶座上同時又發揮僕人的功能，這標誌着科學技術發展的一個新里程碑，是值得我們為之熱情歡呼的！

附　錄

以下是文內提到的一些數值積分法的進一步說明。

命 $f(x)=a_k x^k+\ldots+a_1 x$ 為一個 k 次整係數多項式，q 為一個整數且與

$a_k, \ldots, a_1$ 沒有公因子。我們稱 $S(f(x), q) = \sum_{x=1}^{q} e^{2\pi i f(x)/q}$ 為完整三角和。高斯最先研究這個和當 $k=2$ 的特例，並證明了 $|S(x^2, q)| \leqq 2\sqrt{q}$。一般情況的最佳結果由韋依 (A. Weil) 與華羅庚得到。

我們假定 $f = f(x_1, \ldots, x_s)$ 各變數均有二階導數且有週期 1。卡羅波夫於1957年證明了求積公式

$$(1) \qquad \int_0^1 \cdots \int_0^1 f(x_1, \ldots, x_s)\, dx_1 \cdots dx_s - \frac{1}{p^2} \sum_{k=1}^{p^2} f\left(\frac{k}{p^2}, \frac{k^2}{p^2}, \ldots, \frac{k^s}{p^2}\right) = O(p^{-1}),$$

其中 p 為素數。事實上，將 f 展成傅利葉級數，則公式(1)的左端可以表示成一系列完整三角和，運用完整三角和估計即得(1)之右端。

卡羅波夫(1959)與那夫卡(1962) 獨立地證明了下面更強的結果：給予素數 p，皆存在整數矢量 $\mathbf{a}(p) = (a_1, \ldots a_s)$ 使

$$(2) \qquad \int_0^1 \cdots \int_0^1 f(x_1, \ldots, x_s)\, dx_1 \cdots dx_s - \frac{1}{p} \sum_{k=1}^{p} f\left(\frac{a_1 k}{p}, \ldots \frac{a_s k}{p}\right) = O(p^{-2} \log^{2s} p)$$

但這是一個「存在性」定理，給了 p 之後，需經 $O(p^2)$ 次初等運算才能得到 $\mathbf{a}(p)$。

華羅庚的數值積分方法(1960–1964)基於經典代數數論與丟番圖逼近論的應用。我們舉一個二維的例子。命 $\{F_n\}$ 為斐波那契 (L.P. Fibonacci) 序列，即由下面遞推公式定義的整數列：$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1} (n \geqq 1)$，則

$$(3) \qquad \int_0^1 \int_0^1 f(x, y)\, dx\, dy - \frac{1}{F_n} \sum_{k=1}^{F_n} f\left(\frac{k}{F_n}, \frac{F_{n-1} k}{F_n}\right) = O(F_n^{-2} \log F_n)。$$

這是一個完全「構造性」的方法。但當 $s > 2$ 時，需用分圓域，而且誤差比(2)大。

命 $r > 1$ 為整數，則任一正整數 k 皆可以唯一表示成 r 進位數：$k = a_0 + a_1 r + \ldots + a_m r^m, 0 \leqq a_i < r$。命 $\Phi_r(k) = \frac{a_0}{r} + \ldots + \frac{a_m}{r^{m+1}}$，則 $\Phi_r(k) \in [0, 1]$。命 $P_1, \ldots, P_s$ 為前 s 個素數，則得哈爾頓(1960)公式

$$(4) \qquad \int_0^1 \cdots \int_0^1 f(x_1, \ldots x_s)\, dx_1 \cdots dx_s - \frac{1}{n} \sum_{k=1}^{n} f(\Phi_{p_1}(k), \ldots, \Phi_{p_s}(k)) = O(n^{-1} \log^s n)。$$

王　元　是國際知名的數論專家，現任中國科學院數學研究所研究員，中國科學院數學物理學部委員，中國數學會理事長。王教授1930年生，江蘇鎮江人，1952年在浙江大學數學系畢業，其後一直在中國科學院從事數論及其應用之研究，著有《代數數域上的丟番圖方程與不等式》(1991)以及與華羅庚合作的《數論在近似分析中的應用》(1981)，都已譯成英文，由德國Springer-Verlag出版。王教授曾多次到外國及地區訪問，例如1985–1986年度任普林斯頓高等研究院客座教授及1991年任香港中文大學偉倫訪問教授。