蘇聯科學專著譯叢

數論基礎

維諾格拉陀夫著
裘光明譯

商務印書館

蘇聯科學專著譯叢

數論基礎

維諾格拉陀夫著
裘光明譯

商務印書館

И. М. ВИНОГРАДОВ

ОСНОРЫ ТЕОРИИ ЧИСЕЛ

蘇聯科學專著譯叢

數論基礎

裘光明譯

★版權所有★

商務印書館出版

上海河南中路二一一號

新華書店總經售

商務印書館北京廠印刷

(55046)

1952年3月初版 1954年5月4版

印數 6,501—7,500 定價¥14,900

華　序

遠在 1946 年春季，我訪問莫斯科的時候，維諾格拉陀夫院士送我這一本小書。我當時就決定了要把它譯成中文。於是就利用舟車上的間隙，約會中間的餘暇，從事翻譯這書的工作。終於在 1946 年 7 月在昆明完成了初稿。但是經過幾次間接的問訊，知道若干著名的書店，都無意於刊印，所以一直十分遺憾地掛在心頭。

直到去年再度去歐洲，在匈牙利知道這本書已經譯成匈牙利文字。因爲這本書的俄文簡潔，他們還用這本書作爲學習數學俄文的讀本。因之，我決定在回國以後就整理舊稿出版。但在一回來之後，就立刻知道這書已由清華大學數學系助教裘光明同志翻譯出來了。這對我是一個十分可喜的消息。積壓在心頭已久的願望，已由裘同志償還了！

他譯的是 1949 年新版，無疑地就版本講是會還優於我的舊譯的。譯文也由清華大學教授閔嗣鶴同志負責看過。我深信一定比我在忙亂中的翻譯，來得高明。

但這本書是不能粗淺地閱讀的！特別是習題部分，其中包含着十分豐富的題材，特別是維諾格拉陀夫學派的基本技術。如果讀這本書而不看不做書後的問題，就好像入寶山而空返，把這書的最重要

的部份忽略了！這些問題大部份都是有根據有源流的。很多是歷史上的著名問題，或是維氏自己的研究工作。他精簡的敍述了，他巧妙地安排了，使讀者逐步做去，在不知不覺中間證明了歷史上有名的定理。這些高度的技巧，可能是初讀者不易發現的，同時也誠恐國內很少人能夠指明給讀者關於這些問題的出處的。因此我不揣冒昧地，在這序言裏介紹一番。

在第二章的習題中，一開始就談到兩個數論上十分重要而未解決的問題：

其中一個是有名的高斯 (Gauss) 的圓內整點問題。所謂整點是指兩個坐標都是整數的點。設 T 是以原點爲中心，r 爲半徑的圓內的整點的個數。換句話說，T 就是適合

$$x^2 + y^2 \leqslant r^2$$

的整數 (x,y) 的對數。經其第二章習題 1，C，第三章習題 6，a，逐步地證明了

$$T = \pi r^2 + O(r^{2/3} \ln r),$$

這是歷史上有名的伏樂諾依和謝爾品斯基 (Voronoï–Sierpinski) 的結果。而所謂高斯問題，就是要求出 $T - \pi r^2$ 的最好的上限。這是數論中一個十分困難的問題，近若干年來經過不少數學家的努力，逐步推進，整個的歷史可以概括地敍述如下：

設 θ 是最小的正整適合下面的條件：對於任意 $\alpha > \theta$，總有

$$T = \pi r^2 + O(r^{2\alpha}).$$

謝爾品斯基證明 $\theta \leqslant \frac{1}{3}$；李特伍德 (Littlewood) 和瓦爾非茲 (Walfitz) 證明 $\theta \leqslant \frac{37}{112}$；臬蘭 (Nieland) 更證明 $\theta \leqslant \frac{27}{82}$；梯次馬盧 (Titchmarsh) 用雙變數方次數函數和證明 $\theta \leqslant \frac{15}{46}$。而最好的結果則

是 $\theta \leqslant \frac{13}{40}$。這是羅庚在 1935 年所證明的。但是這距離大家所猜測的 $\theta \leqslant \frac{1}{4}$ 還有些距離。另一方面已經證明了 $\theta < \frac{1}{4}$。如何來決定這個 θ 的數值，在數論中是一個難題。

接着圓內整點問題，維氏還提出狄里盧勒 (Dirichlet) 的除數問題 (Divisor problem)。問題是這樣的：求出適合

$$xy \leqslant n, \quad x > 0, \quad y > 0$$

的整點的個數 T 來。經過第二章問題 1, d 和第三章問題 6, b, 可以證明

$$T = n(\ln n + 2E - 1) + O(n^{\frac{1}{3}}(\ln n)^2).$$

這是俄國大數學家伏樂諾依的結果。但是如果讀者把維氏的證明與伏樂諾依原來的證明比較一下，不難發現新的證法是便捷得多了。

就像圓內整點問題一樣，我們引進 θ，這個 θ 的歷史是這樣：萬·德·考柏 (Van der Corput) 先後證明了 $\theta \leqslant \frac{33}{100}$ 和 $\theta \leqslant \frac{27}{82}$。最好的結果是遲宗陶同志的 $\theta \leqslant \frac{15}{46}$。他所用的方法是閔嗣鶴同志所提出的。

在討論上述兩個問題的過程中，維氏引入了一個十分重要的定理：(見第三章問題 5, a，它前面一連串的問題都是幫助讀者來證明這個定理的。)

設 $A > 2$, $k \geqslant 1$, 函數 $f(x)$ 在間隔 $Q \leqslant x \leqslant R$ 裏有連續的二階微商而且有條件

$$\frac{1}{A} \leqslant \left| f''(x) \right| \leqslant \frac{k}{A}$$

以 $\{f(x)\}$ 表示 $f(x)$ 的分數部分，則

$$\left| \sum_{Q < x \leqslant R} \{f(x)\} - \frac{1}{2}(R-Q) \right| \leqslant (2k^2(R-Q)\ln A + 8kA)A^{-\frac{1}{3}}。$$

這是一個十分重要的定理(非常有用的工具)。如果把這書中所

安排着的證明和萬·德·考柏的相當的工作比較一下，不難發現這裏要簡捷多了。

在第二章的問題裏，一連串地引進了不少關於素數分佈的定理。特別是問題9，那是歷史上有名的俄國數學大師車必奢夫(Chebishev)的工作。問題 16 是茂陛烏斯 (Möbius) 函數的若干重要性質，而且也是與素數分佈基本上相通的。問題 17, a 中引入了一個重要的方法，這方法把 "愛拉托斯散納 (Eratosthenes) 的篩子" 公式化了。這與問題 23, C 聯系起來，就是素數論上常用的白潤 (Brun) 方法。也就是維氏著名工作"充分大的奇數是三個素數的和"的證明中用着的一端。問題 24 是這個方法的一個簡單的應用。

第五章的問題 11 討論了所謂高斯和數。他算出形式

$$\sum_{x=o}^{m-1} e^{2\pi i \frac{Ax^2+ax}{m}}$$

的和數的絕對值。在第六章問題 11 裏更把這結果推進一步。他研究了

$$\sum_{x=o}^{m-1} e^{2\pi i \frac{ax^n}{m}}$$

的絕對值的上限。在問題 15, a 裏更討論了

$$\sum_{x=o}^{m-1} e^{2\pi i \frac{ax^n+bx}{m}}$$

的一個特例。由此引伸出來，我們就會發問：和式

$$\sum_{x=o}^{m-1} e^{2\pi i \frac{f(x)}{m}}, \qquad f(x) = ax^n + a_1x^{n-1} + \cdots + a_n$$

的上限如何？這一個歷史上的問題，已經由羅庚解決了。

不要看輕第六章的問題 13，這是維氏的重要貢獻之一。從第四章問題 11 就開始了 n 次剩餘的討論，而第六章問題 13 則是關於 n 次剩餘分佈情形的優良結果。不等式中 p 的方次數 $\frac{1}{c}$ $(c=2e^{1-\frac{1}{n}})$ 是應當可以降低的。大家預測，可以用 p^{ε}（ε 是任意正數）來代替 $p^{\frac{1}{c}}$，但是這是一個迄未解決的問題。如果讀者能得出比 $\frac{1}{c}$ 小的數，也是值得發表的。而如果能解決這個問題，那對於數論的貢獻是極大的。

同時第六章問題 12，c 也是維氏的重要貢獻，羅庚曾經把它推進一步。問題 14 也是維氏自己的工作。

第五章問題 9 是蘇聯數學家高爾士可夫 (Gorshkov) 的結果，是普通書上所找不到的。我們知道，任意 $4m+1$ 形式的素數 p 一定是兩個平方數的和 x^2+y^2。但是究竟如何把 x 和 y 寫出來？高爾士可夫回答了這個問題：

$$p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2,$$

此處 $\left(\frac{r}{p}\right)=1$，$\left(\frac{n}{p}\right)=-1$，而且

$$S(k)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right)。$$

此外像第四章問題 7 引進了克魯斯脫曼 (Kloostermann) 和數，第五章問題 10 解決了沛勒 (Pell) 方程，第六章問題 9 引進了品格函數的基本性質，等等。仔細地看來，就不難發現維氏的驚人的技巧。他把這許多重要的結果分成若干問題，使讀者按步就班地，用做習題

的方式，自己證明了這些結果。這是多麼引人入勝的方法啊！

維諾格拉陀夫院士的全名是伊凡·馬脫維也維赤·維諾格拉陀夫（Ivan Matveevich Vinogradov），生在 1892 年。他是蘇聯科學院院士，斯泰克洛夫數學研究所所長。他還是蘇聯的社會主義勞動英雄，1941 年獲得斯大林獎金，1945 年得到列寧勳章。他對數論有劃時代的光輝貢獻。對於用"三角和式的估值"來研究數論上的問題這一方面，在世界上是首屈一指的權威。特別是關於瓦林（Waring）問題的不朽的工作，以及震驚全球的關於哥爾德巴哈（Goldbach）問題的貢獻。他的成就證明了社會主義的優越性，這正象徵着我們的明天。

華羅庚序於清華園

1951，5，30.

翻譯者的話

這本書是蘇聯大數學家維諾格拉陀夫寫了作爲大學裏數論課程的教本用的。譯者是根據一九四九年出版的第五版翻譯的。因爲它是基礎課程的教本，內容很淺，加上敍述又很清楚，所以讀者只要學過中等的數學，即使沒有人指導，大概也可以看得懂。大家看了以後就會知道這的確是一本極好的入門書。

這本書的最大優點是在於每一章的最後附有大量的問題。這些問題，據著者在序言裏說，是爲了把讀者引進數論的新的領域裏去。他的確很好地做到了這一點。本來在數論這一門課程裏就有着一個很難處理的問題：怎樣把基本數論（普通數論）和較高深的數論（分析數論、代數數論等）密切連繫起來？這本書裏的這些問題就是配合着書內理論的進展有系統地介紹了許多分析數論的內容和方法，使讀者對於數論能夠有比較深入的了解。

當然這些問題的內容比較地深了一些。但是好在書的最後附有問題解答。所以對於學過微積分的讀者，只要認眞地依着次序學習下去，一定可以完全懂得的。

譯者翻譯俄文書，這還是第一本。由於學識不夠，俄文程度又差，錯誤一定難免。原書排印錯誤的地方很多，譯者看到的都已經把

它改正過來了。但是恐怕還有沒有能看出的地方。譯者覺得理論性的科學文章，也與文學作品一樣，應該用最接近口語的白話文來寫，在這本書裏就是希望能做到那樣。只是譯者運用中國文字的能力很差，這方面可以參考的東西又很少，現在雖然盡自己的能力用白話文字來表達數學上慣用的術語了。但是一定有很多地方，寫得非驢非馬很不通順的，這種種都希望讀者給與指教和改正。

因爲數學名詞的翻譯還不很統一，過去曾經一度審定過的也不很完備，這本書所用的名詞，一般地是按照最通用的翻譯，但是也有一些比較特別的譯法。爲了避免某些意義上的誤會，特地列了一個中、俄、英三種文字對照的索引，附在書的最後。

這本書的翻譯是在科學院編譯局的贊助和清華數學系各位先生的鼓勵和幫助之下進行的。譯者在這裏對他們表示感謝。特別應該感謝的是清華數學系的閔嗣鶴教授，他仔細地看了全部的翻譯稿子，對於名詞和用詞提供了許多寶貴的意見，還幫助譯者改正了一些錯誤和解決了好多疑難的地方。沒有這種種的幫助，這本書是不能夠呈現在讀者面前的。

裘 光 明

一九五〇年十一月於清華園

原　序

俄羅斯數學家車必奢夫（Чебышев），科爾欽（Коркин），佐洛泰遼夫（Золотарёв），馬爾可夫（Марков），伏樂諾依（Вороной）等等，是研究數論的。要知道這些著名學者的古典著作的內容，可以去看狄隆涅（Б.Н. Делоне）著的小書"數論的彼得堡學派"。

蘇維埃數學家在數論領域裏工作，繼續着自己的先驅者的著名傳統，創造了新的强有力的方法，用來得出第一等的結果；在"蘇聯數學三十年"書上數論篇裏，可以看到蘇維埃數學家在數論領域裏的成績，那裏面還有着相當的篇目資料。

在我的這本書裏，只是系統地敍述了大學課程範圍裏數論的基礎。書裏的大量的習題是要把讀者引進數論領域的某些新觀念的範圍裏去。

這書現在的第五版與第四版有很大的不同。在書的各章裏，爲了使敍述更簡單，順序多少有些變動。特別大的變動是把原來的第四章和第五章合併成爲第四章一章（因此章數減少到六個），同時關於元根的存在也有了新的更簡單的證明。

刊印在每章後面的問題，都已作了必要的改編。現在問題的順序完全與理論展開的順序相配合了。引進了一些新的問題，然而問

題的數目還是減去了不少。這是因爲把原先獨立的題目，照解決方法或者內容的相近，用 a, b, c, … 符號把它們合併在一個題目裏了。所有的問題解答，也照解答的難易的順序或者是最好的替換順序重新修訂過了。在問題的解答裏，特別大的變更是討論到了 n 次剩餘和非剩餘以及元根的分配，再有是對應的三角和式的計算。

維諾格拉陀夫 (И.М. Виноградов)

目　次

第一章　可約性理論

第二章　重要的函數

第三章 同 餘 式

第四章 一個未知數的同餘式

第五章 二次同餘式

第六章　元根和指數

問　題　解　答

數 論 基 礎

第一章 可約性理論

§ 1 基本的概念和定理

a 數論是研究整數的性質的。我們所說的整數不但有自然數(正整數)的敍列 1, 2, 3, …, 還有零和負整數 -1, -2, -3, …。

通常我們用小寫的拉丁字母來表示整數，而當字母所代表的不是整數時，我們會有特別的聲明。

兩個整數 a 和 b 的和數，差數以及乘積仍舊是整數。但是 a 被 b 除(b 不等於零)所得到的商數，可以是整數，也可以不是整數。

b 實際上如果 a 被 b 除得到的商數是整數，用 q 來表示，我們就有 $a=bq$, 也就是說，a 等於 b 乘上一個整數。我們就說，a 被 b 除盡，或者 b 除盡 a。並且 a 就叫做 b 的倍數，而 b 則叫做 a 的約數。b 除盡 a，寫做 $a\mid b$。

我們隨即有下面的兩個定理:

1 如果 a 是 m 的倍數，m 是 b 的倍數，則 a 是 b 的倍數。

證明 從 $a = a_1 m$, $m = m_1 b$ 推出 $a = a_1 m_1 b$, 這兒 $a_1 m_1$ 是整