高等学校教学用書

数論基础

И. М. 維諾格拉陀夫著

高等教育出版社

高等学校教学用書

数論基础

И. М. 維諧格拉陀夫著
裘光明譯

高等教育出版社

本書系根据苏联国立技术理論書籍出版社（Государственное издательство технико-теоретической литературы）1952 年出版的維諾格拉陀夫院士（Академик И. М. Виноградов）著"数論基础"修正第六版譯出的。原書經苏联高等教育部审定为綜合大学物理数学系的教本。

本書前出第五版譯本（由商务印書館出版）曾得到北京大学閔嗣鶴教授的帮助，同时，中国科学院数学研究所所長华罗庚教授为本書写了指导性的介紹，对讀者有很大的帮助。

数 論 基 础

H. M. 維諾格拉陀夫著

裘光明譯

高等教育出版社出版

北京琉璃廠一七〇号

（北京市書刊出版業營業許可証出字第〇五四号）

京华印書局印刷　新华書店总經售

書号13010·189　開本 850×1168 1/32　印張 6 5/16　插頁 2　字数 148,000

一九五二年三月商務初版（共印7,500）

一九五六年十一月北京新一版（修訂本）

一九五六年十一月北京第一次印刷

印數 0001—6,000（另平11,000）　定價（8）平1.20（精裝本）

介紹"数論基礎"

維諾格拉陀夫院士的"数論基础"是数論領域里不可多得的一本深入淺出的好書，譯成中文，对于大学数学系的学生和爱好数論的同志都是極有帮助的。

这本書是不能粗淺地閱讀的；特别是習題部分，其中包含着十分丰富的題材，特别是維諾格拉陀夫学派的基本技术。如果讀这本書而不看不做書后的問題，就好像入宝山而空返，把这書的最重要的部分忽略了；这些問題大部分都是有根据有源流的。很多是历史上的著名問題，或是維氏自己的研究工作。他精簡地叙述了，他巧妙地安排了，使讀者逐步做去，在不知不覚中間証明了历史上有名的定理。这些高度的技巧，可能是初讀者不易發現的，同时也誠恐国内很少人能够指明給讀者关于这些問題的出处。因此我不揣冒昧地，在这里介紹一番。

在第二章的習題中，一开始就談到兩个数論上十分重要而未解决的問題：

其中一个是有名的高斯（Gauss）的圓內整点問題。所謂整点是指兩个坐标都是整数的点。設 T 是以原点为中心，r 为半徑的圓內的整点的个数。換句話說，T 就是适合

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

的整数(x, y)的对数。經过第二章問題 1, c, 第三章問題 6, a, 逐步地証明了

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

这是历史上有名的伏乐諾依和謝尔品斯基（Вороной–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。

这是数論中一个十分困难的問題，近若干年来經过不少数学家的努力，逐步推进，整个的历史可以概括地叙述如下：

設 θ 是最小的正整数适合下面的条件：对于任意 $\alpha>\theta$，总有

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

謝尔品斯基証明 $\theta\leqslant\frac{1}{3}$；李特伍德(Littlewood)和瓦尔非兹(Walfitz)証明 $\theta\leqslant\frac{37}{112}$；臬蘭(Nieland)更証明 $\theta\leqslant\frac{27}{82}$；梯次馬虛(Titchmarsh)用双变数方次数函数和証明 $\theta\leqslant\frac{15}{46}$。而最好的結果則是 $\theta\leqslant\frac{13}{40}$。这是罗庚在1935年所証明的。但是这距离大家所猜測的 $\theta\leqslant\frac{1}{4}$ 还有些距离。另一方面已經証明了 $\theta\neq\frac{1}{4}$。如何来决定这个 θ 的数值，在数論中是一个难題。

接着圓內整点問題，維氏还提出狄里虛勒(Dirichlet)的約数問題。問題是这样的：求出适合

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

的整点的个数 T 来。經过第二章問題 1, d 和第三章問題 6, b, 可以証明

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

这是俄国大数学家伏乐諾依的結果。但是如果讀者把維氏的証明与伏乐諾依原来的証明比較一下，不难發現新的証法是便捷得多了。就像圓內整点問題一样，我們引进 θ，这个 θ 的历史是这样：万·德·考柏(Van der Corput)先后証明了 $\theta\leqslant\frac{33}{100}$ 和 $\theta\leqslant\frac{27}{82}$。最好的結果是迟宗陶同志的 $\theta\leqslant\frac{15}{46}$。他所用的方法是閔嗣鶴同志所提出的。

在討論上述兩个問題的过程中，維氏引入了一个十分重要的定理：（見第三章問題 5, a, 它前面一連串的問題都是幫助讀者来証明这个定理的。）

設 $A>2, k\geqslant 1$, 函数 $f(x)$ 在間隔 $Q\leqslant x\leqslant R$ 里有連續的二阶导数而且有条件

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

以 $\{f(x)\}$ 表示 $f(x)$ 的分数部分，則

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

这是一个十分重要的定理(非常有用的工具)。如果把这書中所安排着的証明和万·德·考柏的相当的工作比較一下，不难發現这里要簡捷多了。

在第二章的問題里，一連串地引进了不少关于素数分布的定理。特别是問題 9, 那是历史上有名的俄国数学大师車必奢夫(Чебышев)的工作。問題 16 是茂陛烏斯(Möbius)函数的若干重要性質，而且也是与素数分布基本上相通的。問題 17, a 中引入了一个重要的方法，这方法把"爰拉托散 (Eratosthenes) 的篩子"公式化了。这与問題 23, c 联系起来，就是素数論上常用的白潤(Brun)方法。也就是維氏著名工作"充分大的奇数是三个素数的和"的証明中用着的一端。問題 24 是这个方法的一个簡單的应用。

第五章的問題 11 討論了所謂高斯和数。他算出形式

$$\sum_{x=0}^{m-1}e^{2\pi i\frac{Ax^2+ax}{m}}$$

的和数的絕对值。在第六章問題 11 里更把这結果推进一步。他研究了

$$\sum_{x=0}^{m-1}e^{2\pi i\frac{ax^n}{m}}$$

的絕对值的上限。在問題 15, a 里更討論了

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{ax^n+bx}{m}}$$

的一个特例。由此引伸出来，我們就会發問：和式

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{f(x)}{m}}, \quad f(x)=ax^n+a_1x^{n-1}+\cdots+a_n$$

的上限如何？这一个历史上的問題，已經由罗庚解决了。

不要看輕第六章的問題 13，这是維氏的重要貢献之一。从第四章問題 11 就开始了 n 次剩余的討論，而第六章問題 13 則是关于 n 次剩余分布情形的优良結果。不等式中 p 的方次数 $\frac{1}{c}$（$c=2e^{1-\frac{1}{n}}$）是应当可以降低的。大家預測，可以用 p^{ε}（ε 是任意正数）来代替 $p^{\frac{1}{c}}$，但是这是一个迄未解决的問題。如果讀者能得出比 $\frac{1}{c}$ 小的数，也是值得發表的。而如果能解决这个問題，那对于数論的貢献是極大的。

同时第六章問題 12，e 也是維氏的重要貢献，罗庚曾經把它推进一步。問題 14 也是維氏自己的工作。

第五章問題 9 是苏联数学家高尔士可夫（Горшков）的結果，是普通書上所找不到的。我們知道，任意 $4m+1$ 形式的素数 p 一定是兩个平方数的和 x^2+y^2。但是究竟如何把 x 和 y 写出来？高尔士可夫回答了这个問題：

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

此处 $\left(\frac{r}{p}\right)=1$，$\left(\frac{n}{p}\right)=-1$，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引进了克魯斯脫曼(Kloostermann)和数,第五章問題10解决了沛勒(Pell)方程,第六章問題9引进了品格函数的基本性質,等等。仔細地看来,就不难發現維氏的惊人的技巧。他把这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,自己証明了这些結果。这是多么引人入胜的方法啊!

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(Иван Матвеевич Виноградов),生在1892年。他是苏联科学院院士,斯泰克洛夫数学研究所所長。他还是苏联的社会主义劳动英雄,1941年获得斯大林獎金,1945年得到列宁勛章。他对数論有划时代的光輝貢献。对于用"三角和式的估值"来研究数論上的問題这一方面,在世界上是首屈一指的权威。特别是关于瓦林(Waring)問題的不朽的工作,以及震惊全球的关于哥尔德巴哈(Goldbach)問題的貢献。他的成就証明了社会主义的优越性,这正象征着我們的明天。

华罗庚

目　次

第五版序

許多俄罗斯数学家，諸如車必奢夫(Чебышев)，科尔欽(Коркин)，佐罗泰辽夫(Золотарёв)，馬尔可夫(Марков)，伏乐諾依(Вороной)等等，都曾研究过数論。要知道这些著名学者的古典工作的內容，可以去看狄隆涅(Б. Н. Делоне)著的"数論的彼得堡学派"那本書。

苏維埃数学家在数論領域里工作，繼續着自己的先驅者的优良傳統，創造了新的强有力的方法，用来得出第一等的結果；在"苏联数学三十年"書上数論篇里，可以看到苏維埃数学家在数論領域里的成績，在那里还有着对应的文献篇目。

在我的这本書里，只是系統地叙述了大学課程范圍里数論的基础知識。書中大量的習題是为了把讀者引进数論領域的某些新观念的范圍。

这書現在的第五版与第四版有很大的不同。为了使叙述更簡單，在所有的各章里都作了很多的变动。特别大的变动是把原来的第四章和第五章合并成为新的第四章一章（因此章数减少到六个），同时关于元根的存在也有了新的更簡單的証明。

加在每章末尾的問題，都作了实質上的改編。現在問題引出的順序完全与理論材料安排的順序相配合了。引进了一些新的問題，但是問題的数目还是減去了不少。这是因为把原先独立的、然而按解决方法或者內容說是相近的問題，用 a, b, c, …記号把它們合并在一起了。重新修訂了全部的問題解答；好多地方这些解答簡化了或者用更好的代替了。在問題解答里变动得最利害的是关于 n 次剩余、非剩余和元根的分布，以及对应的三角和式的估值。

維諾格拉陀夫(И. М. Виноградов)

第一章　可除性理論

§1. 基本的概念和定理

a. 数論是研究整数的性質的。我們所說的整数不仅是自然数(正整数) $1, 2, 3, \cdots$, 还有零和負整数 $-1, -2, -3, \cdots$。

通常在作理論的叙述时，我們用字母表示的只是整数。当字母所代表的不是整数时，如果意义并不很明白，我們会作特别的声明。

兩个整数 a 和 b 的和数，差数和乘积仍然是整数，但是 a 被 b 除(假如 b 不等于零)所得到的商数，可以是整数，也可以不是整数。

b. 当 a 被 b 除得到的商数是整数时，假如把它記做 q，我們就有 $a = bq$，也就是說，a 等于 b 乘上一个整数。那末我們就說，a 被 b 除尽或者 b 除尽 a。这时 a 叫做 b 的倍数而且 b 叫做 a 的約数。b 除尽 a 这个事实，写做 $b \backslash a$。

下面的兩个定理成立。

1. 如果 a 是 m 的倍数，m 是 b 的倍数，則 a 是 b 的倍数。

实际上，从 $a = a_1 m$，$m = m_1 b$ 推出 $a = a_1 m_1 b$，这里 $a_1 m_1$ 是整数。这就証明了定理。

2. 如果在等式 $k + l + \cdots + n = p + q + \cdots + s$ 中，除掉某一項以外，所有的項都是 b 是倍数，則这一項也是 b 的倍数。

实际上，設这一項是 k，則因为

$$l = l_1 b, \quad \cdots, \quad n = n_1 b, \quad p = p_1 b, \quad q = q_1 b, \quad \cdots, \quad s = s_1 b,$$

所以

$$k=p+q+\cdots+s-l-\cdots-n=$$
$$=(p_1+q_1+\cdots+s_1-l_1-\cdots-n_1)b.$$

这就証明了定理。

c. 在一般情形下，包括 a 被 b 除尽的特殊情形在内，我們有下列定理：

每一个整数 a 可以唯一地通过正整数 b 而被表示成

$$a=bq+r;\qquad 0\leqslant r<b.$$

实际上，取 bq 等于不超过 a 的 b 的最大倍数，我們得到 a 的这种形式的一个表示式。假定还有 $a=bq_1+r_1$, $0\leqslant r_1<b$, 我們得到 $0=b(q-q_1)+(r-r_1)$，由此推出 $r-r_1$ 是 b 的倍数(b, 2)。但是由于 $|r-r_1|<b$, 所得結果只在 $r-r_1=0$, 即 $r=r_1$ 时才可能，于是还得出 $q=q_1$。

数 q 叫做 a 被 b 除的不完全商数，数 r 叫做 a 被 b 除的余数。

例子 設 $b=14$, 我們有

$$177=14\cdot12+9,\qquad 0<9<14;$$
$$-64=14\cdot(-5)+6,\quad 0<6<14;$$
$$154=14\cdot11+0,\qquad 0=0<14.$$

§2. 最大公約数

a. 以后我們只討論数的正的約数。同时除尽整数 a, b, $\cdots$, l 的每一个整数都叫做它們的公約数。公約数中最大的一个叫做最大公約数而且用符号 $(a, b, \cdots, l)$ 来表示。由于公約数的个数是有限的，最大公約数显然存在。如果 $(a, b, \cdots, l)=1$, 則 a, b, $\cdots$, l 就說是互素的。如果数 a, b, $\cdots$, l 中的每一个都与别的每一个互素，則 a, b, $\cdots$, l 叫做兩兩互素的。明显地，兩兩互素的数一定也互素；而对于兩个数来說，"互素"和"兩兩互素"的概念是一样的。

例子 数 6, 10, 15, 由于(6, 10, 15)=1, 是互素的。数 8, 13, 21, 由于 (8, 13)=(8, 21)=(13, 21)=1, 是兩兩互素的。

b. 我們先来研究兩个数的公約数。

1. 如果 a 是 b 的倍数,則数 a 和 b 的公約数的集合与單独一个 b 的約数的集合重合; 特别地,$(a, b)=b$。

实际上,数 a 和 b 的每一个公約数都是單独一个 b 的約数。反之,因为 a 是 b 的倍数, 所以(§ 1, b, 1) b 的每一个約数也都是 a 的約数, 这就是說它們都是数 a 和 b 的公約数。因此数 a 和 b 的公約数的集合与單独一个 b 的約数的集合重合。而因为数 b 的最大的約数是 b 自己,所以$(a, b)=b$。

2. 如果
$$a=bq+c,$$
則数 a 和 b 的公約数的集合与数 b 和 c 的公約数的集合重合; 特别地, $(a, b)=(b, c)$。

实际上,上面所写的等式表明,数 a 和 b 的每一个公約数也除尽 c (§ 1, b, 2), 因而也是数 b 和 c 的公約数。反之, 这一个等式又表明,数 b 和 c 的約数除尽 a. 因而也是数 a 和 b 的公約数。因此数 a 和 b 的公約数与数 b 和 c 的公約数是相同的一些数; 特别地,这些公約数中最大的也应該相同,即$(a, b)=(b, c)$。

c. 为了求出最大公約数,也为了获得它的最重要性質, 用到下面叙述的欧几里得(Euclid)算法。設 a 和 b 是正整数。按照 § 1, c, 我們求得一串等式

$$\left.\begin{aligned}
a&=bq_1+r_2, && 0<r_2<b,\\
b&=r_2q_2+r_3, && 0<r_3<r_2,\\
r_2&=r_3q_3+r_4, && 0<r_4<r_3,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{n-2}&=r_{n-1}q_{n-1}+r_n, && 0<r_n<r_{n-1},\\
r_{n-1}&=r_nq_n,
\end{aligned}\right\} \qquad (1)$$

这串等式当我們得到一个 $r_{n+1}=0$ 时才終止。这后一点是必然的，因为 $b, r_2, r_3, \cdots$ 是遞減的正整数列，不能包括多于 b 个的正整数。

d. 自上而下来看等式組(1)，根据 b，我們可以肯定，数 a 和 b 的全体公約数与数 b 和 r_2 的全体公約数重合，也与数 r_2 和 r_3 的，数 r_3 和 r_4 的，$\cdots$，数 r_{n-1} 和 r_n 的全体公約数重合，最后就与單独一个数 r_n 的全体約数重合。同时我們还有

$$(a, b)=(b, r_2)=(r_2, r_3)=\cdots=(r_{n-1}, r_n)=r_n.$$

于是我們得到了下面的一些結果。

1. 数 a 和 b 的公約数的集合与它們的最大公約数的約数集合重合。

2. 这个最大公約数等于 r_n，也就是等于欧几里得算法最后的不等于零的余数。

例子 应用欧几里得算法求(525, 231)。我們求得(輔助的計算写在右边)

$$\begin{array}{r|l} 525 & 231 \\ \hline 462 & 2 \end{array} \qquad 525=231\cdot 2+63$$

$$\begin{array}{r|l} 231 & 63 \\ \hline 189 & 3 \end{array} \qquad 231=63\cdot 3+42$$

$$\begin{array}{r|l} 63 & 42 \\ \hline 42 & 1 \end{array} \qquad 63=42\cdot 1+21$$

$$\begin{array}{r|l} 42 & 21 \\ \hline 42 & 2 \end{array} \qquad 42=21\cdot 2$$

这里最后的正余数是 $r_4=21$。所以$(525, 231)=21$。

e. 1. 設 m 表示任意的正整数，我們有 $(am, bm)=(a, b)m$。

2. 設 δ 表示数 a 和 b 的任意公約数，我們有$\left(\frac{a}{\delta}, \frac{b}{\delta}\right)=\frac{(a, b)}{\delta}$；特别地，我們有$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right)=1$，这就是說，兩个数

被它們的最大公約数除所得的商数是互素的。

实际上，等式組(1)逐項地乘上 m，我們得到新的等式組，在其中代替 $a, b, r_2, \cdots, r_n$ 的是 $am, bm, r_2m, \cdots, r_nm$。所以 $(am, bm) = r_nm$，因此命題 1 成立。

应用命題 1，我們求得

$$(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta;$$

由此推出命題 2。

f. 1. 如果 $(a, b) = 1$，則 $(ac, b) = (c, b)$。

实际上，由于 (ac, b) 除尽 ac 和 bc，按照 d, 1 它也除尽 (ac, bc)，后者根据 e, 1 等于 c；而 (ac, b) 又除尽 b，所以它也除尽 (c, b)。反之，(c, b) 除尽 ac 和 b，所以它除尽 (ac, b)。因此，(ac, b) 和 (c, b) 互相除尽，因而它們就相等了。

2. 如果 $(a, b) = 1$ 而且 ac 被 b 除尽，則 c 被 b 除尽。

实际上，由于 $(a, b) = 1$，我們有 $(ac, b) = (c, b)$。但是因为 ac 是 b 的倍数，所以按照 b, 1 我們有 $(ac, b) = b$，这說明 $(c, b) = b$，即 c 是 b 的倍数。

3. 如果 $a_1, a_2, \cdots, a_m$ 中的每一个与 $b_1, b_2, \cdots, b_n$ 中的每一个互素，則乘积 $a_1a_2\cdots a_m$ 也与乘积 $b_1b_2\cdots b_n$ 互素。

实际上，从定理 1，我們有

$$(a_1a_2a_3\cdots a_m, b_k) = (a_2a_3\cdots a_m, b_k) = (a_3\cdots a_m, b_k) =$$
$$= \cdots = (a_m, b_k) = 1,$$

然后，簡写 $a_1a_2\cdots a_m = A$，用同样的方法我們求得

$$(b_1b_2b_3\cdots b_n, A) = (b_2b_3\cdots b_n, A) =$$
$$= (b_3\cdots b_n, A) = \cdots = (b_n, A) = 1.$$

g. 求兩个以上的数的最大公約数的問題，可以化成求兩个数的公約数的問題。那就是說，为了求得数 $a_1, a_2, \cdots, a_n$ 的公約数，

我們写出下列的一串数:

$$(a_1, a_2)=d_2, \qquad (d_2, a_3)=d_3, \qquad (d_3, a_4)=d_4,$$
$$\cdots, (d_{n-1}, a_n)=d_n.$$

数 d_n 就是所有已知数的最大公約数。

实际上，根据 d, 1 数 a_1 和 a_2 的全部公約数与 d_2 的全部約数重合; 所以数 a_1, a_2, a_3 的全部公約数与数 d_2 和 a_3 的全部公約数重合，即与 d_3 的全部約数重合。然后我們肯定，数 a_1, a_2, a_3, a_4 的全部公約数与 d_4 的全部約数重合，等等，最后，数 $a_1, a_2, \cdots, a_n$ 的全部公約数与 d_4 的全部約数重合。而因为 d_n 的最大約数是 d_n 自己，所以它就是数 $a_1, a_2, \cdots, a_n$ 的最大公約数。

看一下上面所引的証明，我們肯定定理 d, 1 对于兩个以上的数也对。定理 e, 1 和 e, 2 也是对的，这是因为用 m 去乘或者用 δ 去除所有的数 $a_1, a_2, \cdots, a_n$, 正像所有 $d_2, d_3, \cdots, d_n$ 都被 m 乘或者被 δ 除一样。

§3. 最小公倍数

a. 所有已知数的每一个整倍数都叫做它們的公倍数。最小的正的公倍数叫做最小公倍数。

b. 我們先来研究兩个数的最小公倍数。設 M 是兩个整数 a 和 b 的任意公倍数。因为它是 a 的倍数，所以 $M=ak$, 这里 k 是整数。但是 M 又是 b 的倍数，所以

$$\frac{ak}{b}$$

也应該是整数。假定 $(a, b)=d$, $a=a_1d$, $b=b_1d$, 上面的整数就可以表示成 $\frac{a_1k}{b_1}$, 这里 $(a_1, b_1)=1$ (§ 2, e, 2)。所以 k 应該被 b_1 除尽 (§ 2, f, 2), $k=b_1t=\frac{b}{d}t$, 这里 t 是整数。由此