数论讲义

上册

柯召　孙琦　编著

高等教育出版社

本书是根据作者多年教学经验和科研成果写成的。内容除通常的初等数论教材中所包括的基本内容外，还包括高次剩余，三次、四次互反律，代数数论初步，有限域上某些不定方程的基础知识等。作者在介绍熟知的经典结果时，也注意介绍新的证明方法和近代进展，并尽可能介绍它们的应用。

本书共分上、下两册。上册前五章可作为初等数论课教学内容，上册第六章及下册可作为选修课教学内容。

本书可供数学专业、计算机科学专业及数字信号处理、组合数学方面的学生和研究生用作教材或参考书。也可供从事上面这些方面的教学、科研人员参考。

数论讲义

上册

柯召 孙琦 编著

*

高等教育出版社出版

新华书店北京发行所发行

二二〇七工厂印装

*

开本 850×1168 1/32 印张 6.5 字数 156,000

1986 年 3 月第 1 版 1986 年 4 月第 1 次印刷

印数 00,001— 6,640

书号 13010·01232 定价 1.10 元

前　言

初等数论是主要用算术方法研究整数性质的一个数论分支，它是数学中最古老的分支之一．我们知道，公元前三世纪，古希腊数学家欧几里德(Euclid)证明了素数的个数是无穷的，并给出了求两个正整数的最大公因数的算法．我国古代的《孙子算经》中给出了解一次同余式组的算法，即著名的孙子定理，国外把它叫做中国剩余定理，这是初等数论中一个重要的定理．从十七世纪到十九世纪，费马(Fermat)、欧拉(Euler)、勒让德(Legendre)、高斯(Gauss)等人的工作大大发展和丰富了初等数论的内容．特别是1801年，高斯出版了著名的《算术探讨》(*Disquisitiones Arithmeticae*)．在这本书中，高斯证明了二次互反律、原根存在的充分必要条件等重要结果．以上这些工作大体上构成了通常初等数论教科书的基本内容．当然，初等数论所包含的内容远不止这些．随着初等数论的不断发展，它的内容也越来越丰富．在本书中，我们只是选取一些较重要的课题．

在数学发展史上，常常可以发现，对初等数论中某些问题的研究，曾促使数学中新分支的发展．例如对不定方程和高次互反律的研究，促进了代数数论和类域论的发展．近几十年来，初等数论在计算机科学、组合数学、代数编码、信号的数字处理等领域内得到广泛的应用，而且许多较深刻的结果(包括一些近代的结果)都得到了应用．本书注意到这些情形，除了包含通常初等数论教科书所共同具有的最基本的内容外，增加了许多新的内容，以适应不断发展的理论和应用方面的需要，特别是增加了高次剩余、三次和四次互反律、有限域上的某些不定方程的基础知识等重要内容．在介绍那些熟知的经典结果时，我们也注意介绍新的证明方法和近代的进展，并尽可能提到它们的应用．这就是我们编写这本书的主要意

图. 下面扼要介绍一下各章的内容，从中大体可以反映出本书的特点.

在第一章和第二章中，除了介绍整除和同余的基本内容外，还介绍了唯一分解定理的另一个证明，取绝对最小剩余的辗转相除法，乔拉(Chowla)等关于完全剩余系的定理，孙子定理的重要应用，以及覆盖同余式组等.

在第三章中，我们介绍了各种基本的数论函数的初等性质，并从狄利克雷乘积引出麦比乌斯反演公式，还给出了著名的公开密钥码 RSA 体制的一个严格证明.

在第四章和第五章中除了介绍二次剩余和原根的基本内容外，给出了高斯引理一个推广形式，以便把高斯引理推广到某些高次剩余的情形. 本章还介绍了二次剩余理论的某些应用，计算次数和原根的某些方法，以及原根在数字信号处理中的一个应用等.

在第六章中我们研究了模奇素数 p 的缩系 $g, g^2, \cdots, g^{p-1}$ 的等价类 $C_j=\{g^j, g^{j+k}, \cdots, g^{j+(q-1)k}\}$(其中 $p-1=kq$, g 是 p 的一个原根, $j=0,1,\cdots,k-1$)的有关理论，这实际上就是分圆数的理论，并以此为工具，给出高次剩余的一些重要结果，如 $\left(\dfrac{2}{p}\right)_3=1$ 的充分必要条件是 $p=u^2+27v^2$ 等. 此外，还介绍了高斯引理在某些高次剩余上的推广和应用，这也是近代数论中的一个重要的研究课题. 本章的内容对组合数学也很重要.

第七章主要介绍三类问题：一类是有理数域上多项式不可约的判别问题；一类是把通常的分圆多项式推广到二个变元的情形，即 a^n-b^n 的本原因子的理论，这是本世纪初皮克霍夫(Birkhoff)和范迪弗(Vandiver)的重要工作；另一类是有限域 F_p 上多项式的基本理论，这在代数编码中很重要.

第八章介绍 F_p 上的特征和及其在 F_p 上不定方程 $x^n+y^n=1$ 解的个数研究中的重要应用，这是有关韦伊(Weil)猜想的初步工作.

第九章介绍环 $Z[\omega]$ 和 $Z[i]$ 上的三次和四次剩余特征，并给出

三次和四次互反律，又一次给出$\left(\frac{2}{p}\right)_3=1$的充分必要条件的证明.

第十章将简要介绍不定逼近方面的基本结果和进展，以及复数的有理逼近问题.

第十一章介绍代数数域的基本算术理论，从理想数的唯一分解定理直到给出一般分圆域的基本性质.

第十二章介绍解不定方程的基本方法和技巧. 我们将看到本书前面诸章的许多结果在此得到了应用.

本书是我们通过多年教学和科研工作的积累写成的，其中许多章节曾先后给大学生、研究生以及在实际部门工作的同志讲授过,并在讲授的过程中不断补充新的内容.

鉴于编写本书的意图，我们认为本书的适应面是较广的. 除了数学系的大学生和研究生外,对于计算机科学、数字信号处理、组合数学等方面的大学生、研究生,本书均可作为教本和参考书. 本书还可供从事上述诸方面教学和科研的同志参考.

前五章的内容作为大学数学系一个学期的初等数论课，已经足够了. 如果再加一学期,那么八、九、十、十一、十二诸章或六、七十一诸章都可分别作为一个选修课的内容. 自然，本书也可作为研究生两个学期数论课的教材. 以上这些意见仅供参考，如何更好地组织教材，还需教师根据实际情况来决定. 本书每章附有一定的习题供选用. 本书假定读者具备高等代数以及群、环、域的基本知识,只在个别地方(第二章 §10 节和第七章 §2 节)用到一点复变函数的知识,如讲授时学生未学,可以删去. 某些小节和较难的习题,用星号“*”标志,以便读者选择.

后面所列书目，可供读者使用本书时参考. 我们在编写本书的过程中,也曾参考过这些书. 特别是,本书的第六章，第七章的§4、§5两节和第八、九、十一章的若干节，分别比较多地参考了[8]和[6]、[1]的有关章节.

陈重穆教授和潘承彪副教授对本书原稿提出过许多宝贵意见，作者特致深切的谢意.

限于水平，本书难免有缺点和错误，请读者批评指正.

作者

1984年8月于成都

参考书目

[1] 华罗庚,《数论导引》,科学出版社,1957。

[2] 闵嗣鹤、严士健,《初等数论(第二版)》,高等教育出版社,1982.

[3] 柯召、孙琦,《谈谈不定方程》,上海教育出版社,1980.

[4] 柯召、孙琦,《初等数论 100 例》,上海教育出版社,1980.

[5] 孙琦、郑德勋、沈仲琦,《快速数论变换》,科学出版社,1980.

[6] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1982.

[7] E. Hecke, *Lectures on the Theory of Algebraic Numbers* (英译本), Springer-Verlag, 1981.

[8] H. Gupta, *Selected topics in Number Theory*, Abacus Press, 1980.

[9] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

目　　录

第一章　整数的唯一分解定理

整数的唯一分解定理，又叫算术基本定理，它是初等数论中最基本的定理之一．本章将给出这个定理两种不同的证明，以及介绍与此有关的初等数论中最基本的概念和性质．

§1 整除性

两个整数的和、差、积仍然是整数，但是用一个不等于零的整数去除另一个整数所得的商却不一定是整数，因此，我们引进整除的概念．

定义　任给两个整数 a, b，其中 $b\neq 0$，如果存在一个整数 q 使得等式

$$a=bq \tag{1}$$

成立，我们就说 b 整除 a，记作 $b\mid a$，此时我们把 b 叫做 a 的因数，把 a 叫做 b 的倍数．如果(1)里的整数 q 不存在，我们就说 b 不整除 a，记作 $b\nmid a$.

由整除的定义出发，下面一些性质是明显的．

1. 如果 $b\mid a, c\mid b$，则 $c\mid a$.
2. 如果 $b\mid a$，则 $cb\mid ca$.
3. 如果 $c\mid a, c\mid b$，则对任意的整数 m, n，有
$$c\mid ma+nb.$$
4. 如果 $b\mid a$ 且 $a\neq 0$，则 $|b|\leqslant|a|$.
5. 如果 $cb\mid ca$，则 $b\mid a$.
6. 如果 $b\mid a, a\neq 0$，则 $\frac{a}{b}\Big| a$.

一般地，有下面的定理.

定理 1　设 a, b 是两个整数，其中 $b>0$，则存在两个唯一的整数 q 及 r，使得

$$a=bq+r,\quad 0\leqslant r<b \tag{2}$$

成立.

证　作整数序列

$$\cdots,-3b,-2b,-b,0,b,2b,3b,\cdots,$$

则 a 必在上述序列的某两项之间，即存在一个整数 q 使得

$$qb\leqslant a<(q+1)b$$

成立. 令 $a-qb=r$，则(2)成立.

设 q_1、r_1 是满足(2)的另一对整数，因为

$$bq_1+r_1=bq+r,$$

于是

$$b(q-q_1)=r_1-r,$$

故

$$b|q-q_1|=|r_1-r|.$$

由于 r 及 r_1 都是小于 b 的非负整数，所以上式右边是小于 b 的. 如果 $q\neq q_1$，则上式左边 $\geqslant b$，这是不可能的. 因此，$q=q_1, r=r_1$.

证完

定义　我们把(2)中的 q 叫做 a 被 b 除得出的**不完全商**，r 叫做 a 被 b 除所得到的**余数**，也叫做**非负最小剩余**，常记作 $\langle a\rangle_b=r$. 以后，我们总假定除数 $b>0$ 以及因数为正.

在不致引起混淆的情况下，$\langle a\rangle_b$ 中的 b 常略去不写. 我们有

定理 2　对于整数 a_1, a_2, b，其中 $b>0$，常有

$$\langle a_1+a_2\rangle=\langle\langle a_1\rangle+\langle a_2\rangle\rangle, \tag{3}$$

$$\langle a_1-a_2\rangle=\langle\langle a_1\rangle-\langle a_2\rangle\rangle, \tag{4}$$

$$\langle a_1 a_2\rangle=\langle\langle a_1\rangle\langle a_2\rangle\rangle. \tag{5}$$

证 设

$$a_1=bq_1+\langle a_1\rangle,\ a_2=bq_2+\langle a_2\rangle,$$
$$\langle a_1\rangle+\langle a_2\rangle=bq_3+\langle\langle a_1\rangle+\langle a_2\rangle\rangle,$$

故

$$\begin{aligned}a_1+a_2&=b(q_1+q_2)+\langle a_1\rangle+\langle a_2\rangle\\&=b(q_1+q_2+q_3)+\langle\langle a_1\rangle+\langle a_2\rangle\rangle.\end{aligned}\tag{6}$$

由定理 1，即得(3)式，类似地可证(4)和(5)。 证完

§2 最大公因数与辗转相除法

利用上节的定理 1，我们来研究整数的最大公因数的存在问题和实际求法.

定义 设 $a_1, a_2, \cdots, a_n$ 是 n 个不全为零的整数. 若整数 d 是它们之中每一个的因数，那么 d 就叫做 $a_1, a_2, \cdots, a_n$ 的**一个公因数**. 这时，它们的公因数只有有限个. 整数 $a_1, a_2, \cdots, a_n$ 的公因数中最大的一个叫**最大公因数**，记作 $(a_1, \cdots, a_n)$，若 $(a_1, \cdots, a_n)=1$，我们说 $a_1, a_2, \cdots, a_n$ **互素**. 我们有下面的定理.

定理 1 设 a, b, c 是任意三个不全为零的整数，且

$$a=bq+c,$$

其中 q 是整数，则 $(a, b)=(b, c)$.

证 因为 $(a,b)\mid a$, $(a,b)\mid b$，所以有 $(a,b)\mid c$，因而 $(a,b)\leqslant(b,c)$. 同法可证 $(b,c)\leqslant(a,b)$，于是得到 $(a,b)=(b,c)$.

证完

因为，显然有 $(a_1, a_2, \cdots, a_n)=(|a_1|, |a_2|, \cdots, |a_n|)$，又因为，一组不全为零的整数的最大公因数，等于它们当中全体不为零的整数的最大公因数，所以，不妨设 $a_i>0\ (i=1, \cdots, n)$. 我们先讨论两个正整数的最大公因数的求法，即**辗转相除法**，并借此推出最大

公因数的若干性质.

任给整数 $a>0, b>0$, 由带余数的除法, 有下列等式:

$$
\begin{aligned}
a &= bq_1 + r_1, 0<r_1<b,\\
b &= r_1 q_2 + r_2, 0<r_2<r_1,\\
&\cdots \quad \cdots \quad \cdots\\
r_{n-2} &= r_{n-1} q_n + r_n, 0<r_n<r_{n-1},\\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, r_{n+1}=0,
\end{aligned}
\tag{1}
$$

因为 $b>r_1>r_2>r_3>\cdots$, 故经有限次带余除法后, 总可以得到一个余数是零, 即(1)中 $r_{n+1}=0$.

现在我们证明

定理 2 若任给整数 $a>0, b>0$, 则 (a, b) 就是(1)中最后一个不等于零的余数, 即 $(a, b)=r_n$.

证 由定理 1 即得

$$r_n=(0, r_n)=(r_n, r_{n-1})=\cdots=(r_2, r_1)=(r_1, b)=(a, b).$$

证完

从(1)中 $r_n=r_{n-2}-r_{n-1}q_n, r_{n-1}=r_{n-3}-r_{n-2}q_{n-1}$, 得

$$r_n=r_{n-2}(1+q_nq_{n-1})-r_{n-3}q_n,$$

再将 $r_{n-2}=r_{n-4}-r_{n-3}q_{n-2}$ 代入上式, 如此继续下去, 最后可得 $r_n=sa+tb$, 其中 s, t 是两个整数. 于是有

定理 3 若任给整数 $a>0, b>0$, 则存在两个整数 m, n 使得

$$(a, b)=ma+nb.$$

显然有

推论 a 和 b 的公因数是 (a, b) 的因数.

例 用辗转相除法求 $a=288, b=158$ 的最大公因数和 m, n, 使 $ma+nb=(a, b)$.

由

$$288=158\cdot 1+130,$$

$$158=130\cdot 1+28,$$
$$130=28\cdot 4+18,$$
$$28=18\cdot 1+10,$$
$$18=10\cdot 1+8,$$
$$10=8\cdot 1+2,$$
$$8=2\cdot 4.$$

因此，$(288,158)=2$.

再由 $2=10-8\cdot 1=10-(18-10)=10\cdot 2-18$
$$=(28-18\cdot 1)2-18=28\cdot 2-18\cdot 3$$
$$=28\cdot 2-(130-28\cdot 4)3=-130\cdot 3+28\cdot 14$$
$$=-130\cdot 3+(158-130\cdot 1)14=14\cdot 158-17\cdot 130$$
$$=14\cdot 158-17(288-158\cdot 1)=31\cdot 158-17\cdot 288,$$

故 $m=-17,n=31$.

对于§1的(2)中的余数，如果不要求它是正的，那么，对于整数 a 和$b>0$，则存在整数 s, t，使 $a=bt+s$ 成立，其中$|s|\leqslant\frac{b}{2}$. 这是因为，当§1，(2)中的$r<\frac{b}{2}$时，取 $s=r$；当 $r>\frac{b}{2}$时，取 $s=r-b$；当 b 是偶数且 $r=\frac{b}{2}$时，则 s 可取$\frac{b}{2}$和$-\frac{b}{2}$两个数中的任意一个. 数 s 叫做 a 被 b 除所得到的绝对最小剩余. 如果我们在(1)的计算过程中，都取绝对最小剩余，并设最后一个不为零的余数为 s_m，则由定理1，仍然有$|s_m|=(a,b)$. 仍用前例说明：

$$288=158\cdot 2-28,$$
$$158=28\cdot 6-10,$$
$$28=10\cdot 3-2,$$
$$10=2\cdot 5,$$

与一般的辗转相除法相比较计算步骤由 7 次减少为 4 次.

定理 4　若 $a|bc$, $(a,b)=1$, 则 $a|c$.

证　若 $c\neq 0$, 由 $(a,b)=1$ 知存在两个整数 m, n 使 $ma+nb=1$, 故 $mac+nbc=c$, 由 $a|bc$, 知 $a|c$; 若 $c=0$, 结论显然成立.

证完

现在来研究两个以上正整数的最大公因数. 设 $n>2$, $a_1>0$, $a_2>0$, $\cdots$, $a_n>0$, $(a_1,a_2)=d_2$, $(d_2,a_3)=d_3$, $\cdots$, $(d_{n-1},a_n)=d_n$, 那么有下面的定理.

定理 5　若 $a_1,\cdots,a_n$ $(n>2)$ 是 n 个正整数, 则

$$(a_1,a_2,\cdots,a_n)=d_n.$$

证　由 $d_n|a_n$, $d_n|d_{n-1}$, $d_{n-1}|a_{n-1}$, $d_{n-1}|d_{n-2}$, 可得

$$d_n|a_{n-1},\quad d_n|d_{n-2}.$$

由此类推, 最后得到

$$d_n|a_n,\quad d_n|a_{n-1},\cdots,d_n|a_1,$$

因此有 $d_n\leqslant(a_1,\cdots,a_n)$. 另一方面, 设 $(a_1,\cdots,a_n)=d$, 由定理 3 的推论可得

$$d|d_2,\ d|d_3,\cdots,d|d_n,$$

故

$$d\leqslant d_n.$$

于是得到 $(a_1,a_2,\cdots,a_n)=d_n$.　　证完

由定理 5 可推出

定理 6　设 a_1, a_2, $\cdots$, a_n 均为正整数, $n>2$, 则存在整数 $x_1,\cdots,x_n$ 使得

$$a_1x_1+\cdots+a_nx_n=(a_1,\cdots,a_n)$$

成立.

§3 最小公倍数

定义 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数($n\geqslant 2$),若 m 是这 n 个数中每一个数的倍数,则 m 就叫做这 n 个数的一个**公倍数**. 在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中最小的正数叫做**最小公倍数**,记作 $[a_1, \cdots, a_n]$.

因为乘积 $|a_1||a_2|\cdots|a_n|$ 就是 $a_1, \cdots, a_n$ 的一个公倍数,故最小公倍数是存在的.

由于任何正整数都不是零的倍数,故讨论整数的最小公倍数时,总假定这些整数都不是零.

和最大公因数一样,显然有 $[a_1, \cdots, a_n]=[|a_1|, \cdots, |a_n|]$,所以只需对正整数讨论它们的最小公倍数.

我们先研究两个正整数的最小公倍数.

定理 1 设 a, b 是任给的两个正整数,则

① a, b 的所有公倍数就是 $[a, b]$ 的所有倍数.

② $[a, b]=\dfrac{ab}{(a, b)}$.

证 设 m 是 a, b 的任一公倍数, $m=ak=bk'$,令 $a=a_1(a, b)$, $b=b_1(a, b)$,代入 $ak=bk'$ 得 $a_1k=b_1k'$,因为 $(a_1, b_1)=1$,故 $b_1|k$. 因此

$$m=ak=ab_1t=\frac{ab}{(a, b)}t, \tag{1}$$

其中 t 满足等式 $k=b_1t$. 反之,当 t 为任一整数时, $\dfrac{ab}{(a, b)}t$ 为 a, b 的一个公倍数,故(1)可以表示 a, b 的一切公倍数. 令 $t=1$,即得最小的正数,故 $[a, b]=\dfrac{ab}{(a, b)}$,这便证明了定理 1 中的②. 又由(1)式定理中的①也得证.