叶景梅　楼世拓　吴茹玉　罗肇华
姚　琦　　李佛奇　　吴文昭

数论简明教程

宁夏人民出版社

ISBN7-227-00624-7/G·138

定价：3.50元

数论简明教程

叶景梅　楼世拓　吴茹玉　罗肇华
姚　琦　　李佛奇　　吴文昭　著

宁夏人民出版社

数论简明教程

叶景梅 等 著

宁夏人民出版社出版发行　　新华书店经销
（银川市解放西街105号）　　宁夏新华印刷厂印刷

开本：850×1168 1/32 印张：9.25　　字数：215千
印数：1——3,500册
1991年7月第1版　　1991年7月1次印刷

责任编辑：勉树人　责任校对：杨　力
封面设计：项玉杰　版式设计：勉树人

ISBN7-227-00624-7/G·138　　定价：3.50元

前　言

数论是研究整数性质的基础理论学科，是一个内容极为丰富的数学分支。历史表明，每一个重大的数论课题，都是在吸收了当时最新的数学成果，创造了极深刻的新方法之后，才获得进展的；反过来，数论研究的进展，也促进了数学其它分支的发展。因此，数论中的许多问题，都受到了大批杰出的数学家的重视。我国古代数学家在解不定方程、同余方程等方面，曾取得许多重大成果。在现代，华罗庚、闵嗣鹤等数学家及其学生更获得了数论的许多领先结果，为数论学科的发展作出了杰出的贡献。

数论的基本知识和技巧，对于提高解题能力和学习近代数学其它学科都是十分有用的。由于数论的初等内容和技巧与中学数学有着密切的关系，因而数论对于未来的数学教师来说，是一门有着重要意义的课程。正因为如此，许多高等院校，特别是高等师范院校，近年来相继开设了数论课程。

我国现有数论教材种类还很少，不能满足各种程度和不同学制的需要，为此，我们总结了自己的教学经验，编写本书，奉献给从事数论教学的师生和对数论知识有兴趣的青年读者。

本书共十章，划分成三个部分，适应三种不同教学对象的需要。

第一部分包括前五章，其内容与中学数学的教学和竞赛有密切的联系。其例题和习题有一部分选自国内外数学竞赛。这五章约需48教学学时，可作为专科院校数论课程的教学内容。

第二部分包括第六、七、八章，是前五章内容的继续，与中学教学仍有一定的联系。一至七章都属初等数论的范畴，而第八章则是代数数论的初步知识。一至八章约需80学时，可作为本科数论课程的教学内容。

第三部分包括第九、十章，是解析数论的入门知识，约需20学时，可作为数论课程后的选修内容。这部分内容在编写方法上与前面的章节不同，写得较为紧凑，以求用较小的篇幅介绍较多的内容。

本书前面章节的习题较多，希望读者能留心这些习题。除了选择一部分去独立完成外，其余习题可参考书末所附略解进行阅读和思考，从中体会数论的方法和技巧。

本书由浙江师范大学吴茹玉，上海师范大学罗肇华、吴文昭，上海科技大学楼世拓、姚琦，宁夏大学叶景梅，以及嘉应大学李佛奇等同志合作编写，叶景梅、楼世拓审定了全稿，并由叶景梅统一全文。限于编者的水平，在内容及题解上都可能出现错误。我们衷心欢迎读者的批评指正。

1989年

目　录

第一章　整数的整除性理论

整数是指集$Z=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$中的数。我们常用小写拉丁字母$a$，$b$，$c$等代表整数。

在中学数学中已经涉及整数的一些性质，如整数四则运算的一般性质，整数的有序性等等。此外，我们还将经常使用整数的如下重要性质——**最小整数原理：有下界的非空整数集必有最小元。**与上述原理等价的是**最大整数原理：有上界的非空整数集必有最大元。**

§1　整除与余数

众所周知，加、减、乘三种运算在集Z中是封闭的。也就是说，两整数的和、差、积仍是整数。然而，用一非零整数去除另一整数，所得的商未必是整数，因此有必要对整数的可除性问题进行讨论。

定理1　若$a,b\in Z$，$b\neq 0$，则存在唯一的整数对q及r，满足

$$a=bq+r,\quad 0\leqslant r<|b|. \tag{1}$$

证：首先讨论$b>0$的情形。作数列

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

由阿基米德公理知存在$q\in Z$，使

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

于是$0\leqslant a-bq<b$。若令$r=a-bq$，则$r\in Z$，且q，r满足(1)。

若设q_1、$r_1\in Z$也满足（1），即

$$a=bq_1+r_1,\quad 0\leqslant r_1<b,$$

则$bq_1+r_1=bq+r$，故

$$b\,|q-q_1|=|r_1-r|.\qquad(2)$$

但由$0\leqslant r<b$及$0\leqslant r_1<b$，可知$0\leqslant|r_1-r|<b$。若$q\neq q_1$，则有$|q-q_1|\geqslant 1$，故$b\,|q-q_1|\geqslant b$。于是由(2)即知$|r_1-r|\geqslant b$。但这是不可能的，故只能有$q=q_1$，进而$r=r_1$。

对于$b<0$的情形，由前述讨论可知存在q'，$r\in Z$，使

$$a=|b|\,q'+r,\quad 0\leqslant r<|b|.$$

故$a=b(-q')+r$。若取$q=-q'$，即知q，r'满足（1）。因q'，r是唯一的，故q，r也是唯一的。定理证毕。

定义1　（1）式中的整数q称为a被b除所得的不完全商（简称为商），非负整数r称为a被b除所得的余数。

从定理1的证明过程中可以看出，q，r的唯一性是在条件$0\leqslant r<|b|$下才成立的。如不作此限制，则满足$a=bq+r$的q及r不是唯一的。此外，余数必须非负且小于除数。例如，虽有$-81=-5\times 14-11$，但-11不是-81被-5除所得的余数，进而14也不是-81被-5除的商。

例1　求所有被4除余1的二位正整数之和S。

解：被4除余1的一切正整数是且仅是如下形式的数：

$$a=4q+1,\quad q=0,\ 1,\ 2,\ \cdots\cdots.$$

命题要求a是二位数，故$10\leqslant 4a+1<100$，于是

$$2\frac{1}{4}\leqslant q<24\frac{3}{4}.$$

显然q可取3至24之间的一切整数，由等差数列求和公式不难求得

$$S=\sum_{q=3}^{24}(4q+1)=1210.$$

（1）式的一个重要特例是$r=0$，这时有

定义2 设a，b，$q\in Z$，$b\neq 0$，若$a=bq$，则称a被b整除，或称b整除a，记作$b\mid a$；否则a就称不能被b整除，或称b不能整除a，记作$b\nmid a$。若$b\mid a$则称b为a的因数（约数），a为b的倍数。

易证整数间的整除性有下列基本性质：

1° 若$b\mid a$，则$\pm b\mid \pm a$。特别地，若$b\mid a$，则$|b|\mid|a|$。

根据这一性质，我们可以限制在正整数的范围内来讨论整除性问题，特别地，关于数的因数，我们也只需考虑正因数。今后，如无特别声明，本章中所用字母均代表正整数，但所得结论对于负整数仍然成立。

2° 若$a\mid b$，$b\mid c$，则$a\mid c$。

3° 若$a\mid b_i$，$i=1$，2，$\cdots$，k，则$a\mid \sum_{i=1}^{k} c_i b_i$。

4° 若a是任意整数的因数，则$a=\pm 1$。

5° 若a是所有整数的倍数，则$a=0$。

6° 非零整数同时是它自己的因数和倍数。

定义3 若$b\mid a$且$1<b<|a|$，则称b为a的真因数。

7° 若$b\mid a$，$a\neq 0$，则$|b|\leqslant|a|$。由此可知，非零整数只能有有限个因数。

例2 设整数a，b，c，d使方程组

$$ax+by=m,\quad cx+dy=n$$

对任何整数m，n都有整数解，试证$D=\begin{vmatrix} a & b \\ c & d \end{vmatrix}=\pm 1$。

证：显然a，b，c，d均不能是零。现证$D\neq 0$。事实上，若$D=ad-bc=0$，则$\frac{a}{c}=\frac{b}{d}$。因而只须取m和n，使$\frac{m}{n}\neq\frac{a}{c}$，则方程将无解，从而与题设矛盾。

其次，由方程解得

$$x=\frac{md-nb}{D},\quad y=\frac{na-mc}{D}.$$

取$m=1$，$n=0$和$m=0$，$n=1$，可得两组整数解：

$$\begin{cases}x_1=\dfrac{d}{D},\\ y_1=-\dfrac{c}{D};\end{cases}\qquad \begin{cases}x_2=-\dfrac{b}{D},\\ y_2=\dfrac{a}{D}.\end{cases}$$

于是

$$x_1y_2-y_1x_2=\frac{ad-bc}{D^2}=\frac{1}{D}$$

是一个整数，故$D\mid 1$，于是$D=\pm 1$。

在（1）式中，若取$b=2$，则有

$$a=2q+r,\quad 0\leqslant r<2.$$

因此只能有$r=0$，1。当$r=0$时，有$a=2q,q\in Z$；当$r=1$时，有$a=2q+1$，$q\in Z$。形如$2q$的整数称为偶数；形如$2q+1$的整数称为奇数。

例3 在三维欧氏空间中，任意给定九个整点（坐标均为整数的点），试证其中至少有两点，使得连接它们的直线段内也有整点。

证：依坐标的奇偶性，可将空间的整点分为八类，如(奇，奇，奇)，（奇，奇，偶）等等。显然，任给的九个整点中，至少有某两点P，Q属于同一类，即它们的相应坐标有相同的奇偶性，因而线段PQ的中点是一个整点。

例4 设m，n是任意正整数，试证$S=\sum_{i=0}^{n}\frac{1}{m+n}$不是整数。

证：因$m+i$（$i=0$，1，…，n）是正整数，故可设

$$m+i=2^{\alpha_i}a_i,\quad a_i,\ \alpha_i\in Z,\ \alpha_i\geqslant 0,\ 2\nmid a_i.$$

取$\alpha=\max\{\alpha_0,\alpha_1,\cdots,\alpha_n\}$，$a=a_0a_1\cdots a_n$，$c=2^{\alpha-1}a$。显

然，因$n\geqslant 1$，故m，…，$m+n$中至少有一个是偶数，故$\alpha-1\geqslant 0$，于是$c\in Z$。

现设$\alpha_k=\alpha$，则k是唯一的。事实上，若有$j\neq k$使$\alpha_j=\alpha$，不妨设$j<k$，则

$$m+j=2^{\alpha_j}a_j=2^{\alpha}a_j;\qquad m+k=2^{\alpha_k}a_k=2^{\alpha}a_k。$$

于是$a_j<a_k$。但a_j，a_k均为奇数，故存在偶数b，使$a_j<b<a_k$。于是

$$m+j=2^{\alpha}a_j<2^{\alpha}b<2^{\alpha}a_k=m+k。$$

显然存在$j<t<k$，使$m+t=2^{\alpha}b$，注意到b是偶数，$m+t=2^{\alpha_t}a_t$，因而$\alpha_t>\alpha$。这是与α的意义矛盾的。

现以c乘S，注意到$\dfrac{2^{\alpha-1}a}{m+k}$不是整数，而对于不等于$k$的其它$i$，因$\alpha_i<\alpha$，故$2^{\alpha_i}\mid 2^{\alpha-1}$。于是$\dfrac{2^{\alpha-1}a}{m+i}$都是整数，从而$cS$不是整数。进而推得$S$也不是整数。

习 题 一

1.分别举出使下面命题不成立的例子：

（1）若$a\mid b$，$b\mid a$，$a=b$.

（2）对于a，$b\in Z$，$a\mid b$，$a=b$，$b\nmid a$中至少有一个成立.

2.设d_1，d_2，…，d_n是正整数a的全部正因数，试证$(d_1d_2\cdots d_n)^2=a^n$.

3.设$(m-p)\mid(mn+pq)$，试证$(m-p)\mid(mq+np)$.

4.设a，b是两个不全为零的整数，记一切形如$ax+by(x,\ y\in Z)$的整数中的最小正数为d，试证$d\mid(ax+by)$.

5.设$f(x)$为整系数多项式，且存在$k\in Z$，使得$f(0)$，$f(1)$，…，$f(k-1)$都不能被k整除，试证$f(x)$无整数根.

6.若$x\in Z$，试证$2x^2+3$不是整数的平方.

7.若$k\in Z$，$k>1$，试证2^k不可能是不少于两个的连续正整数之

和，但可以是若干个连续的奇数之和.

8.若诸a_i是正奇数，$\sum_{i=1}^{n}\frac{1}{a_i}=1$，试证$n$是奇数.

9.设n，k都是大于2的整数，试证$n(n-1)^{k-1}$可以表成n个连续偶数之和.

10.设α，β为整系数方程$x^2+ax+b=0$的两个根，$S_n=\sum_{r=0}^{n}\alpha^{n-r}\beta^r$，试证对任何正整数$n$，$S_n$都是整数.

§2 整除问题例析*

本节集中讨论整除问题，并通过具体的例题，介绍一些常用的方法.

1.直接运用整除的定义的方法

整除的概念虽然简单，却是解决整除问题的依据.许多命题可直接运用整除的定义得到解决，其特点是通过证明整数q的存在性，或直接找出具体的整数q，使$a=bq$，从而证明了$b\mid a$.

例1 试证任一整数与其各数码之和的差能被9整除，且它与其数码作任意顺序调换后所成整数的差也能被9整除.

证：不妨设整数$m>0$，依十进表示为

$$m=a_1+10a_2+\cdots+10^{n-1}a_n,\quad 0\leqslant a_i\leqslant 9,$$

则

$$m-(a_1+a_2+\cdots a_n)=9(a_2+11a_3+\cdots+\underbrace{11\cdots1}_{n-1\text{个}}a_n).$$

故$9\mid[m-(a_1+a_2+\cdots+a_n)]$.

又设a_1'，$a_2'\cdots$，a_n'是数码a_1，a_2，…，a_n的另一排列，记

※此节可作为自学材料.

$$\sigma=a_1+a_2+\cdots+a_n=a_1'+a_2'+\cdots+a_n',$$

$$m'=a_1'+10a_2'+\cdots+10^{n-1}a_n'.$$

由前面的结论知$m-\sigma=9q$，$m'-\sigma=9q'$，故$m-m'=9(q-q')$，于是$9\mid(m-m')$。

例 2　试证离$n!e^{-1}$最近的整数是$n-1$的倍数。

证：由微分学知识知$e^{-1}=\sum_{k=0}^{\infty}\frac{(-1)^k}{k!}$。记$N=\sum_{k=0}^{n}\frac{(-1)^k}{k!}$，则$|e^{-1}-N|<\frac{1}{(n+1)!}$，故

$$|n!e^{-1}-n!N|<\frac{1}{n+1}.$$

因而$n!N$是离$n!e^{-1}$最近的整数。注意到$\frac{(-1)^{n-1}}{(n-1)!}+\frac{(-1)^n}{n!}=(-1)^{n-1}\frac{n-1}{n!}$，于是

$$\begin{aligned}n!N&=n!\left(1-\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{(-1)^{n-2}}{(n-2)!}\right)+(-1)^{n-1}(n-1)\\&=n(n-1)M+(-1)^{n-1}(n-1),\end{aligned}$$

这里$M\in Z$。于是由整除的定义即知$(n-1)\mid n!N$。

2.分解因式的方法

根据整除的定义，要判断a能否被b整除，只须考虑能否将a分解为b与另一因数的积。在分解时，除了一般的因式分解公式外，还可考虑使用下列公式：

$$(a+b)^n=aM_1+b^n,\ M_1\in Z;\qquad(1)$$

$$a^n-b^n=(a-b)M_2,\ M_2\in Z;\qquad(2)$$

$$a^n+b^n=(a+b)M_3,\ M_3\in Z,\ 2\nmid n。\qquad(3)$$

例 3　试证$1979\mid(1978^{1978}+1980^{1980}-1981)$。

证：由公式（1）可得

$$1978^{1978}=(1979-1)^{1978}=1979M_1+1,$$

$$1980^{1980}=(1979+1)^{1980}=1979M_2+1,$$

这里M_1，$M_2\in Z$。于是

$$1978^{1978}+1980^{1980}-1981=1979(M_1+M_3-1).$$

例 4　设n为正偶数，试证$(2^n-1)\nmid(3^n-1)$。

证：设$n=2k$，由公式（2）知

$$2^n-1=4^k-1=3M,\ M\in Z,$$

故$3\mid(2^n-1)$。若$(2^n-1)\mid(3^n-1)$，则$3\mid(3^n-1)$。但这将导致$3\mid 1$，显然这是不可能。于是$(2^n-1)\nmid(3^n-1)$。

例 5　设$S=\sum_{k=1}^{n}k^{1985}$，试证对于任何自然数n，均有$(n+2)\nmid S$。

证：$2S=1^{1985}+2^{1985}+\cdots+n^{1985}$

$$+n^{1985}+\cdots+2^{1985}+1^{1985}$$

$$=2+\sum_{k=2}^{n}\left[k^{1985}+(n-k+2)^{1985}\right].$$

由公式（3）知$(n+2)\mid\left[k^{1985}+(n-k+2)^{1985}\right]$，$k=2,\cdots,n$。若$(n+2)\mid S$，则由前面等式就可推得$(n+2)\mid 2$。这是不可能的，故$(n+2)\nmid S$。

例 6　设a，b是正整数，n为非负整数，若$a^n\mid b$，试证$a^{n+1}\mid\left[(a+1)^b-1\right]$。

证：对n使用数学归纳法。当$n=0$时，有$(a+1)^b-1=aM$，$M\in Z$，结论成立。

设$n=k$时结论成立，即若$a^k\mid b$，则$a^{k+1}\mid\left[(a+1)^b-1\right]$。现设$a^{k+1}\mid b'$，并记$ab=b'$，则$a^k\mid b$。

$$(a+1)^{b'}-1=(a+1)^{ab}-1=\left[(a+1)^b-1\right]\sum_{s=0}^{a-1}(a+1)^{bs}$$