

21世纪

高等学校电子信息类规划教材

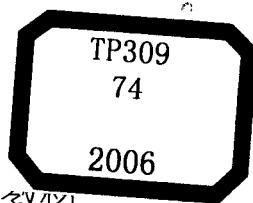
信息安全数学基础

■ 谢 敏 编著



西安电子科技大学出版社

<http://www.xduph.com>



★ 21 世纪高等学校电子信息类规划教材

信息安全数学基础

谢 敏 编著

西安电子科技大学出版社

2006

内 容 简 介

本书系统地介绍了信息安全专业所需的数论和抽象代数的基础知识,给出了一些相关的应用实例。本书结构紧凑、例题翔实、习题丰富并且配有解答,可作为高等院校信息安全、密码、通信、信息工程、计算机专业及相关专业的本科生、研究生教材,也可供从事信息安全、密码及相关工作的专业人员参考使用。

图书在版编目(CIP)数据

信息安全数学基础/谢敏编著. —西安:西安电子科技大学出版社, 2006. 11

21 世纪高等学校电子信息类规划教材

ISBN 7-5606-1746-8

I. 信… II. 谢… III. 信息系统-安全技术-应用数学-高等学校-教材 IV. TP309

中国版本图书馆 CIP 数据核字(2006)第 116528 号

策 划 臧延新

责任编辑 郑 东 臧延新

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

http: //www. xduph. com

E-mail: xdupfxb@pub. xaonline. com

经 销 新华书店

印刷单位 陕西华沐印刷科技有限责任公司

版 次 2006 年 11 月第 1 版 2006 年 11 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 14.25

字 数 338 千字

印 数 1~4000 册

定 价 18.00 元

ISBN 7-5606-1746-8/TP·0437

XDUP 2038001-1

*** 如有印装问题可调换 ***

本社图书封面为激光防伪覆膜,谨防盗版。

前 言

到目前为止,信息安全领域所涉及的数学知识主要是数论、代数以及概率。其中,数论和代数是工科数学教育中所匮乏的。作者试图通过系统地阐述初等数论、抽象代数的基本内容来弥补这种数学准备上的不足——这种不足通常被视为知识上的,其实更大程度上是修养上的。

希望读者在使用本书的过程中能够真切地关注知识体系是如何建立起来的。事实上,初等数论是展示公理化方法的好素材,抽象代数更是如此。在书中许多地方,作者给出了不同的建立途径,其中限于篇幅而没有展开的部分则给出了必要的提示。作者非常乐于看到自己的努力能够转变为读者视界的改观。

需要提醒读者的是,习题不是本书的附庸,而是全书的有机组成部分。在本书中,自然有着针对基本训练而设计的习题,更有相当数量的习题是正文的补充和延伸,它们的价值不言而喻。考虑到习题的重要性以及习题相对于初学者的难度,本书编入了习题解答,可供读者在教学或自学中参考使用。

书中未加说明的符号都是规范和常用的。为了体现定理在体系中的骨干地位,在本书中推论采用了和定理相同或相近的记号。倘若使用本书进行教学,则以 60 学时为宜。

在本书的撰写过程中,作者受到了国家自然科学基金青年基金(项目编号:60503010)的资助;同时,本书作为西安电子科技大学的教材立项项目,其出版得到了西安电子科技大学出版社的大力支持。

作者衷心感谢自己的家人和朋友,正是他们给予了作者无以回报的关爱;衷心地感谢王育民教授的扶掖;感谢通信工程学院及信息工程系领导的支持,感谢计算机网络与信息安全教育部重点实验室领导的支持;特别感谢李晖教授——由于他的倡议,作者的讲义才得以蜕变为教材。

谢 敏

2006 年 8 月于西安电子科技大学

欢迎选购西安电子科技大学出版社教材类图书

~~~~~国家级、部级重点教材~~~~~

计算机系统结构(第四版)(统编)	25.00
离散数学(第三版)(统编)(乔维声)	16.00
雷达对抗原理(统编)	15.00
雷达原理(第三版)	23.00
通信网的安全——理论与技术	42.00
模拟电子线路基础(傅丰林)	16.00
移动通信(第三版)(统编)(郭梯云)	26.00
智能控制理论和方法	18.00

~~~全国信息技术水平考试指定教材~~~

计算机网络信息安全理论与实践教程	32.00
网页设计与网站开发基础教程	54.00
中小校园网络管理基础教程	19.00
中小校园网络管理实验教程	25.00

~~~~~计算机提高普及类~~~~~

计算机应用基础(第三版)(丁爱萍)	19.00
计算机组装与维护(高职)(杜飞明)	22.00
计算机组装与维护实用教程(第二版)(高职)	29.00
计算机应用基础(Windows 2000 &Office 2002)(教育部高职)	23.00
《计算机应用基础》实践技能训练 与案例分析(教育部高职)	11.00
计算机综合能力实训教程(高职)	10.00
办公自动化技术及应用教程	22.00
办公自动化设备的使用和维护 (第二版)(高职)	18.00
网络办公自动化技术及应用(高职)	21.00

~~~~~计算机网络类~~~~~

Internet基础与使用(第二版)(高职)	13.00
计算机网络安全(高职)	15.00
计算机网络管理	20.00
网络安全技术(高职)	17.00
网络安全与保密	24.00
网络信息安全技术	17.00

网络信息安全	11.00
网站建设与维护(崔良海)	18.00
网站建设与维护(廖常武)	19.00
Internet技术及其应用教程	15.00
Windows网络程序设计	26.00
嵌入式系统原理与开发	21.00
通信网理论与技术	25.00
计算机图形图像与网页制作(高职)	19.00
互联网实用技术与网页制作(高职)	14.00
局域网组建、管理与维护(高职)	20.00
综合布线技术(高职)	18.00
计算机网络技术导论	16.00
计算机网络(第二版)(袁家政)	26.00
计算机网络技术(刘敏涵)	20.00
计算机网络(第二版)(蔡皖东)	18.00
计算机网络(第二版)(雷振甲)	21.00
计算机网络工程	20.00
计算机网络实验教程	14.00
计算机组网实验教程	23.00
计算机网络学习辅导及习题详解	23.00
网络工程设计与实践	29.00
网络应用程序设计	21.00
现代网络技术	24.00
网络计算	19.00

~~~~~计算机技术类~~~~~

计算机系统结构(陈智勇)	22.00
计算机系统设计——概念与技术(洪龙)	18.00
计算机组成原理 与系统结构实验教程(杨小龙)	12.00
计算机系统安全	22.00
实用计算机类毕业设计指导	18.00
计算机原理课程设计	10.00
电子政务理论与实务	20.00
电子商务概论(李晓燕)	17.00
电子商务概论(宋沛军)	20.00

电子商务基础与应用(第四版)(含盘)	34.00	~~~~~操作系统类~~~~~	
电子商务基础与实务(第二版)(高职)	16.00	计算机操作系统(第二版)(颜彬)(高职)	17.00
数据结构(C)(第二版)(杨秀金)	20.00	计算机操作系统(修订版)(汤)	24.00
《数据结构》算法实现及解析		《计算机操作系统》学习指导与题解	16.00
——配合严蔚敏的《数据结构》(C语言版)		计算机操作系统(王津)	16.00
(含光盘)(第二版)	35.00	计算机操作系统(孙雅如)	15.00
数据结构——使用C++语言(第二版)	23.00	计算机操作系统(方敏)	28.00
数据结构(高职)(周岳山)	15.00	计算机操作实训教程(张晓云)(高职)	18.00
计算方法与实习(高职)	11.00	操作系统教程——Linux实例分析(孟)	21.00
算法设计与分析	15.00	Linux操作系统实用教程(高职)	20.00
编译原理教程(第二版)	18.00	Linux实训指导教程(高职)	13.00
《编译原理教程(第二版)》		~~~~~图形处理类~~~~~	
习题解析与上机指导	18.00	多媒体技术及应用(王坤)	21.00
离散数学(蔡英)	21.00	多媒体软件设计技术(第二版)	20.00
《离散数学》学习指导书	16.00	多媒体技术与应用(第二版)(傅献祯)	16.00
离散数学(马光思)	22.00	多媒体技术教程(杨安琪)	20.00
离散数学——精讲·精解·精练	24.00	计算机图形学(张义宽)	20.00
软件工程(第二版)	22.00	计算机图形学(丁爱玲)	14.00
软件工程与数据库概论	14.00	计算机图形学(研究生系列)(璩柏青)	26.00
信息系统分析与设计(卫红春)	19.00	计算机图形学——图形的计算与显示原理	22.00
信息系统分析与设计(高职)(卫红春)	18.00	数字图像处理	20.00
信息系统分析与设计(第二版)(陈圣国)	14.00	3DS MAX 6.0实用教程(高职)	23.00
人工智能技术导论(第二版)	18.00	~~~~~微机与控制类~~~~~	
~~~~~计算机辅助技术类~~~~~		微型计算机原理与应用(第二版)(本科)	33.00
电子工程制图(含习题集)(高职)	25.00	《微型原理及应用》(第二版)学习指导	18.00
工程制图(含习题集)(高职)	22.00	微型计算机原理(第四版)	29.00
机械制图与计算机绘图(含习题集)(高职)	24.00	《微型计算机原理》(第四版)学习指导书	14.00
计算机绘图(第二版)	25.00	《微型计算机原理》学习与实验指导	18.00
DSP应用技术(高职)	25.00	微型计算机原理及接口技术(新世纪)	25.00
现代DSP技术	22.00	80X86微机原理与接口技术	26.00
电子电路CAD程序及其应用(高职)	16.00	单片机原理及接口技术(喻宗泉)	15.00
电子线路CAD实用教程(第二版)	22.00	单片机应用实训教程(高职)	22.00
电子工艺与电子CAD(高职)	14.00	单片机原理与应用技术	19.00
电子电路EDA技术	15.00	新编单片机原理与应用(第二版)	22.00
EDA技术及应用(第二版)	24.00	可编程序控制器原理及应用(第二版)	22.00
EDA技术综合应用实例与分析	22.00	计算机控制技术(高职)(温希东)	12.00
EDA技术与数字系统设计(高职)	14.00	计算机外部设备(第二版)	17.00
数字电路EDA设计(高职)	19.00		

微机外围设备的使用与维护(高职)	19.00	模拟电子技术(第二版)(江晓安)	18.00
微机结构组成与外部设备(第二版)(高职)	17.00	《模拟电子技术》学习指导与题解	12.00
~~~~~数据库及计算机语言类~~~~~			
数据库原理(第二版)(郭盈发)	16.00	模拟电子技术实验(高职)	9.00
数据库原理(高荣芳)	18.00	模拟电子技术实训(高职)	9.00
Visual FoxPro 6.0数据库原理与应用(高职)	21.00	《模拟电子技术(修订版)》	
基于VFP和SQL的数据库技术及应用	16.00	目标测试及习题全解	11.00
SQL Server 2000应用基础与实训教程(高职)	19.00	《电路分析(修订版)》	
Oracle数据库SQL和PL/SQL实例教程(高职)	17.00	学习指导及习题全解(高职)	19.00
数据库技术及应用(高职)	14.00	电子产品工艺实训(高职)	15.00
网络数据库技术及应用(高职)	20.00	电子工艺实训教程	19.00
C++程序设计语言	20.00	电工技能实训基础(高职)	14.00
《C++程序设计语言》经典题解与实验指导	13.00	电工中级技能实训(高职)	15.00
新编C语言程序设计教程(第二版)	22.00	流行PLC实用程序及设计	32.00
《新编C语言程序设计教程(第二版)》		多媒体通信技术(王汝言)	23.00
习题解答与实验指导	15.00	现代通信系统	24.00
C++Builder 6.0 程序设计(高职)	19.00	现代通信系统导论(高职)	18.00
Visual Basic 程序设计(第二版)	20.00	通信电路(沈伟慈)	18.00
Visual Basic.NET 程序设计教程(高职)	18.00	通信电源(高职)	14.00
汇编语言程序设计(第二版)(韩海)	18.00	通信系统(修订版)(王秉钧)	22.00
汇编语言程序设计(李强)	23.00	现代通信网概论	25.00
汇编语言程序设计(李革新)	19.00	现代通信理论与技术导论	25.00
微型计算机汇编语言程序设计(龚)	23.00	现代通信技术与网络应用	23.00
面向对象程序设计与VC++实践	22.00	现代通信新技术	20.00
面向对象程序设计与C++语言(第二版)	18.00	数字移动通信技术	15.00
面向对象程序设计教程	19.00	通信工程专业英语	12.00
面向对象程序设计——JAVA(第二版)	32.00	微波技术与天线	17.00
跨平台程序设计语言——JAVA	24.00	微波技术及应用	20.00
JAVA语言程序设计教程	18.00	电磁波——传输·辐射·传播	26.00
JAVA程序设计(高职)	18.00	锁相技术	14.80
~~~~~电子技术类~~~~~			
测试与计量技术基础	19.00	计算机通信网(沈金龙)	24.00
测试技术基础	15.00	计算机通信网(修订版)(刘后铭)	18.00
现代测控技术	20.00	计算机数据通信教程(张燕)	15.00
传感器原理及工程应用(第二版)	20.00	纠错码——原理与方法(王新梅)	35.00
模拟电子技术(第二版)(教育部高职)	17.00	编码理论	19.00
模拟电子电路基础(王卫东)	23.00	现代交换技术	20.00
		程控交换技术实用教程(李正吉)(高职)	11.00
		程控数字交换原理学习指导与习题解析	12.00
		数字视觉视频技术(研究生)	26.00

数据融合理论与应用（第二版）	20.00	机械加工技术（高职）（魏康民）	24.00
自动控制原理（赵四化）	16.00	计算机辅助机械设计（秦汝明）	19.00
自动控制原理（薛安克）	19.00	数控机床原理与编程（高职）（陈富安）	20.00
《自动控制原理》学习指导与题解（方斌）	22.00	数控加工与编程（高职）	19.00
自动控制原理及其应用（高职）	15.00	数控加工工艺（高职）（赵长旭）	22.00
智能化仪器原理及应用（曹建平）	16.00	数控编程与操作（高职）（秦启书）	16.00
楼宇自动化（高职）	14.00	数控技术及应用（高职）（马一民）	17.00
电梯原理及逻辑排故（高职）	22.00	数控机床故障分析与维修（高职）（潘海丽）	19.00
~~~~~家用电器与机电类~~~~~			
电视原理与系统（赵坚勇）	16.00	数控机床电气控制（高职）（姚勇刚）	21.00
电视原理与电视机检修（高职）	16.00	机电一体化技术（高职）	17.00
数字电视技术	20.00	机床电器 PLC（高职）（李伟）	14.00
电器原理与技术（裴昌幸）	24.00	机床电气与 PLC（高职）	16.00
调音技术（高职）	16.00	电机及拖动基础（高职）（孟宪芳）	17.00
音响技术	13.00	电机拖动与控制（高职）（刘保录）	25.00
现代音响与调音技术	19.00	电机与电气控制（高职）（冉文）	23.00
电气控制与 PLC 原理及应用（常文平）	17.00	电切削加工技术（高职）（詹华西）	13.00
工程力学（皮智谋）（高职）	12.00	金属切削与机床（高职）（聂建武）	22.00
工程力学（史艺农）（高职）	23.00	模具制造技术（高职）（刘航）	22.00
工程材料与热加工技术（高职）（程晓宇）	20.00	液压与气动技术（朱梅）	19.00
机械工程基础（李茹）（高职）	26.00	特种加工技术（周旭光）	10.00
机械设计基础（赵冬梅）（高职）	21.00	汽车电工电子技术（高职）（袁建华）	20.00
机械设计基础（张京辉）（高职）	24.00	工业机器人技术（高职）（郭洪红）	16.00
机械设计基础（郭红星）（高职）	20.00	互换性与技术测量（高职）（杨好学）	16.00
机械基础（周家泽）	17.00	车工基本技能训练（高职）（武建荣）	6.00
机械 CAD/CAM 技术（方新）	20.00	钳工基本技能训练（高职）（彭彦）	5.00
机械制图（刘家平）（高职）	32.00	焊接基本技能训练（高职）（王红英）	6.00
机械制造工艺装备（高职）（吴秀佳）	19.00	建筑管道工基本技能训练（高职）（陈斐明）	8.00
机械制造技术（高职）（邵堃）	24.00	铣工基本技能训练（高职）（韩振武）	4.00
		高等教育管理导论（研究生）	36.00

欢迎来函索取本社最新书目和教材介绍，欢迎投稿！

从邮局或银行汇款邮购者，汇款单上务必写清收书人姓名、地址、邮编、电话。款到后我社将挂号发书，加收5元包装邮寄费（一次购书30元以上者可免收邮费）。

通信地址：西安市太白南路2号 西安电子科技大学出版社发行部 邮 编：710071

电 话：（029）88201467

传 真：（029）88213675

主 页：<http://www.xduph.com>

E-mail：xdupfb@pub.xaonline.com

目 录

第一篇 数论基础

第 1 章 整除	3
1.1 整数的除法	3
1.2 算术基本定理	11
1.3 素数	16
1.4 Euclid 算法	19
第 2 章 同余	23
2.1 同余的基本概念与性质	23
2.2 Euler 定理和 Fermat 小定理及其应用	33
2.3 孙子定理	42
2.4 同余方程的一般理论	46
第 3 章 二次剩余	57
3.1 Legendre 符号(1): Euler 判别法	57
3.2 Legendre 符号(2): 二次互反律	62
3.3 Jacobi 符号	69
3.4 二次同余方程	77
第 4 章 原根和指数	84
4.1 原根	84
4.2 指数	93

第二篇 代数基础

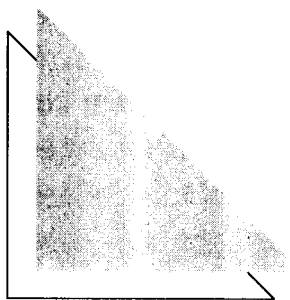
第 5 章 群	99
5.1 群的基本概念	99
5.2 循环群	106
5.3 陪集和 Lagrange 定理	110
5.4 正规子群和商群	113
第 6 章 环和域	117
6.1 环和域的基本概念	117

6.2 理想和商环	122
6.3 多项式环	127
第 7 章 有限域	136
7.1 域的有限扩张	136
7.2 有限域(Galois 域)的性质	142
7.3 有限域的表示	146
7.4 有限域上的多项式	151
习题解答	156
参考文献	222

第一篇 数论基础

初等数论是一门十分重要的数学基础课。它是古老的却至今仍充满活力并蓬勃发展的数学分支，在信息安全、数字信号处理、通信工程、计算机科学等重要科技领域有着广泛的应用。初等数论是数学工作者以及许多从事实际应用工作的工程技术人员必备的数学知识。

本书的第一篇介绍了信息安全所用到的初等数论知识，主要有数的整除性质、同余理论、二次剩余、原根以及指数等内容。



第1章 整 除

初等数论的研究对象主要是整数集合 $\mathbf{Z}$ 和正整数集合 $\mathbf{N}^+$ 。整除理论和同余理论是初等数论的两大支柱,其中整除理论是初等数论的基础,是对涉及除法运算的整数的算术内容作抽象的、系统的总结,它的主要结果是唯一分解定理(也称算术基本定理)和最大公约数理论;同余理论是初等数论的堂奥,它包含了初等数论所特有的思想和手法。

1.1 整数的除法

正整数是人们从生活和生产实践中最早抽象出来的数的概念。针对正整数,人们还定义了加法和乘法这两种二元运算(运用代数的眼光来看,正整数集对于加法、乘法运算是封闭的)。把零纳入数集是人类认识的一次进步。加法逆运算(即减法运算)促使人们引入了负数,数集因而扩展为整数集;乘法逆运算(即除法运算)促使人们引入了小数,数集进而扩展为有理数集($\mathbf{Q}$)。在古希腊时期人们就认识到开方会导致无理数的出现,而直到十九世纪后期人们才基本弄清楚了实数的结构,在此之前引入的复数集($\mathbf{C}$)也就获得了圆满的结局——人们实现了数集中开方的封闭性。简要回顾人们对数的认识历程,会促使我们更加关注数集中运算的特性。

我们知道在整数集 $\mathbf{Z}$ 中可以进行加法“+”和乘法“ $\cdot$ ”运算,这两种运算具备下述特性:

加法“+”运算满足:

- (1) 交换律:对任意 $a, b \in \mathbf{Z}$, 有 $a+b=b+a$;
- (2) 结合律:对任意 $a, b, c \in \mathbf{Z}$, 有 $(a+b)+c=a+(b+c)$;
- (3) 存在零元“0”,对任意 $a \in \mathbf{Z}$, 有 $a+0=a$ (或 $0+a=a$);
- (4) 对任意 $a \in \mathbf{Z}$, 存在负元“ $-a$ ”,使得 $a+(-a)=0$ (或 $(-a)+a=0$)。

依据(1)~(4),借助并非十分简单的推理,我们知道加法运算还满足:

- (5) 零元是唯一的;
- (6) 负元是唯一的;
- (7) 消去律:若 $a, b, c \in \mathbf{Z}$ 且 $a+b=a+c$, 则 $b=c$ 。

乘法“ $\cdot$ ”运算满足:

- (1) 交换律:对任意 $a, b \in \mathbf{Z}$, 有 $a \cdot b=b \cdot a$;

(2) 结合律: 对任意 $a, b, c \in \mathbf{Z}$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(3) 存在单位元“1”, 对任意 $a \in \mathbf{Z}$, 有 $a \cdot 1 = a$ (或 $1 \cdot a = a$);

(4) 非零元可消去: 若 $a, b, c \in \mathbf{Z}$, $a \neq 0$, $a \cdot b = a \cdot c$, 则 $b = c$.

依据(1)~(3)我们知道乘法运算还满足:

(5) 单位元 1 唯一。

乘法“ $\cdot$ ”运算对于加法“ $+$ ”运算还满足分配律:

左分配律: 对任意 $a, b, c \in \mathbf{Z}$, 有 $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;

右分配律: 对任意 $a, b, c \in \mathbf{Z}$, 有 $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ 。

为了方便, 我们常将 $a \cdot b$ 简记为 ab 。

整数集对于除法运算来说不是封闭的, 即设 $a, b \in \mathbf{Z}$, $b \neq 0$, 则 $\frac{a}{b}$ 不一定是整数, 也就是说不一定存在整数 c , 使得 $a = bc$ 。由此就产生出初等数论中第一个基本概念——整除。

定义 1.1.1 (整除) 设 $a, b \in \mathbf{Z}$, $b \neq 0$, 如果存在整数 c , 使得 $a = bc$, 则称 b 整除 a (或称 a 能被 b 整除), 记为 $b | a$ 。这时称 b 是 a 的一个因数 (也称约数、因子), 而 a 为 b 的倍数。

如果不存在整数 c , 使得 $a = bc$, 则称 b 不整除 a , 记为 $b \nmid a$ 。

例 1 $1 | 8, -3 | 9, 6 \nmid 8$ 。

易见: (1) 对于每一整数 n , 都有 $\pm 1 | n$;

(2) 对于每一非零整数 n , 都有 $n | 0, \pm n | \pm n$ 。

由整除的定义及乘法“ $\cdot$ ”运算的性质, 我们可以推出整除有如下性质:

定理 1.1.1

(1) $a | b \Leftrightarrow -a | b \Leftrightarrow a | -b \Leftrightarrow -a | -b \Leftrightarrow |a| \parallel |b|$;

(2) $b \neq 0$ 且 $a | b \Rightarrow |a| \leq |b|$;

(3) $a | b$ 且 $b | c \Rightarrow a | c$;

(4) $a | b$ 且 $b | a \Rightarrow b = \pm a$;

(5) $a | b$ 且 $a | c \Leftrightarrow$ 对任意 $t, s \in \mathbf{Z}$ 有 $a | tb + sc$;

(6) 设 $m \neq 0$, $a | b \Leftrightarrow ma | mb$ 。

证明 (1) $a | b \Leftrightarrow$ 存在整数 c , 使得 $b = ac$

$\Leftrightarrow$ 存在整数 $-c$, 使得 $b = (-a)(-c)$

$\Leftrightarrow$ 存在整数 $-c$, 使得 $-b = a(-c)$

$\Leftrightarrow$ 存在整数 c , 使得 $-b = (-a)c$

$\Rightarrow$ 存在整数 $|c|$, 使得 $|b| = |a| |c|$

$|a| \parallel |b| \Rightarrow$ 存在整数 c_1 , 使得 $|b| = |a| c_1$

$\Rightarrow$ 存在整数 c_1 , 使得 $b = ac_1$ 或 $b = a(-c_1)$

$\Rightarrow a | b$

(2) 由(1)知, $|b| = |a| |c|$, 因为 $b \neq 0$, 所以 $c \neq 0$, 从而整数 $|c| \geq 1$, 由此得 $|a| \leq |b|$.

(3) $a|b$ 且 $b|c \Rightarrow$ 存在整数 q_1, q_2 使得 $b = aq_1$ 且 $c = bq_2$

$$\Rightarrow c = (aq_1)q_2 = a(q_1q_2)$$

$$\Rightarrow a|c$$

(4) $a|b$ 且 $b|a \Rightarrow$ 存在整数 q_1, q_2 使得 $b = aq_1$ 且 $a = bq_2$

$$\Rightarrow a = aq_1q_2$$

$$\Rightarrow q_1q_2 = 1$$

$$\Rightarrow q_1 = \pm 1, q_2 = \pm 1 \Rightarrow b = \pm a$$

(5) $(\Rightarrow)$ 由题设可知, 存在整数 q_1, q_2 使得 $b = aq_1$ 且 $c = aq_2$, 所以

$$tb + sc = t(aq_1) + s(aq_2) = a(tq_1 + sq_2)$$

故有 $a|bt + cs$.

$(\Leftarrow)$ 由题设知, 对任意 $t, s \in \mathbf{Z}$ 有 $a|bt + cs$, 若取 $t = 1, s = 0$, 则有 $a|b$; 若取 $t = 0, s = 1$, 则有 $a|c$.

(6) 由非零元可消去知, 当 $m \neq 0$ 时, $b = aq \Leftrightarrow mb = m(aq)$, 从而 $a|b \Leftrightarrow ma|mb$.

定理 1.1.1 的内容比较简单, 但从中我们可以得到一些很有用的结论, 例如: (2) 说明非零整数的因子只有有限多个; (3) 说明整除具有传递性; (5) 则将整除和线性组合联系起来. 利用这些基本性质, 我们可更进一步探讨整数之间的整除关系.

例 2 设 n 为整数, 求证: 若 $3|n$ 且 $4|n$, 则 $12|n$.

证明 由 $3|n$ 知存在整数 m , 使得 $n = 3m$, 由题设知 $4|3m$, 由此及 $4|4m$, 利用定理 1.1.1(5), 有 $4|4m - 3m$, 所以 $m = 4k, k \in \mathbf{Z}$, 从而 $n = 12k$, 即 $12|n$.

例 3 设 m 为奇数, $n \in \mathbf{Z}$, 求证: 若 $m|2n$, 则 $m|n$.

证明 可设 $m = 2k + 1, k \in \mathbf{Z}$. 因为 $m|(2n)$, 所以 $m|2kn$, 注意到 $m|mn$, 再由定理 1.1.1(5)知, $m|mn - 2kn$, 所以 $m|n$.

定义 1.1.2 设 $x \in \mathbf{R}$, 我们以 $[x]$ 表示不超过 x 的最大整数, 称作实数 x 的整数部分; 而 $x - [x]$ 称作实数 x 的小数部分, 记为 $\{x\}$.

例 4 $[\pi] = 3, \{3.14\} = 0.14; [-\pi] = -4, \{-3.14\} = 0.86$.

由定义 1.1.2 易知 $x = [x] + \{x\}, 0 \leq \{x\} < 1$.

容易证明:

(1) $x \in \mathbf{Z} \Leftrightarrow x = [x] \Leftrightarrow \{x\} = 0$;

(2) 若 $n \in \mathbf{Z}$, 则 $\forall x \in \mathbf{R}$ 有 $[x + n] = [x] + n$.

关于取整符号“ $[]$ ”更进一步的讨论可参阅习题 1.1 中的第 6 题至第 13 题.

我们知道, 以非零整数为除数做除法时有两种情形: 能够整除或除不尽. 这两种情形都可以归结为一种形式——带余除法. 自然地, 它是初等数论中一个根本性的重要工具.

定理 1.1.2(带余除法) 设 a, b 是两个给定的整数, $b > 0$, 则存在唯一的一对整数 q 和 r , 使得 $a = qb + r, 0 \leq r < b$.

证明 (存在性)先证满足条件的 q 和 r 是存在的。令 $q = \left[\frac{a}{b} \right]$, $r = a - qb$, 则 q 和 r 均为整数, 由

$$\frac{r}{b} = \frac{a}{b} - q = \left\{ \frac{a}{b} \right\} \text{ 以及 } 0 \leq \left\{ \frac{a}{b} \right\} < 1$$

知 $0 \leq \frac{r}{b} < 1$, 即 $0 \leq r < b$ 。

(唯一性)再证 q 和 r 是唯一确定的。如果存在 $q_1, q_2 \in \mathbf{Z}$, $r_1, r_2 \in \mathbf{Z}$, $0 \leq r_1, r_2 < b$, 使得

$$a = q_1 b + r_1 = q_2 b + r_2$$

于是

$$|r_1 - r_2| < b, \text{ 且 } r_1 - r_2 = b(q_1 - q_2)$$

若 $q_1 - q_2 \neq 0$, 则有

$$|r_1 - r_2| = b |q_1 - q_2| \geq b$$

这与 $|r_1 - r_2| < b$ 相矛盾, 从而有 $q_1 = q_2$, $r_1 = r_2$ 。

注意定理 1.1.2 中要求除数 $b > 0$, 但是很容易推广为 $b \neq 0$, 因为当除数 $b < 0$ 时, 我们总可以将其转化为除数大于零的情况, 事实上此时 $\frac{a}{b} = \frac{-a}{-b}$, 而 $-b > 0$ 。

从定理 1.1.2 中我们还可以得出:

推论 1.1.2 设 $a = qb + r$, 其中 $a, b, q, r \in \mathbf{Z}$, $0 \leq r < b$, 则 $b|a \Leftrightarrow r = 0$ 。

下面我们引入最大公约数这一重要的概念。

定义 1.1.3 设 a, b 是两个不全为零的整数, a 和 b 的最大公约数是指满足下述条件的整数 d :

- (1) d 为 a 和 b 的公约数, 即 $d|a$ 且 $d|b$;
- (2) d 为 a 和 b 的所有公约数中最大的, 即对于整数 c , 如果 $c|a$ 且 $c|b$, 则 $c \leq d$ 。

记为 (a, b) , 有时也记为 $\gcd(a, b)$ ($\gcd$ 即 the greatest common divisor)。

由定义知 $(a, b) = \max\{d; d|a \text{ 且 } d|b\}$ 。

一个非零整数只有有限多个约数, 所以若 a 和 b 是不全为零的整数, 那么它们的公约数也只有有限多个, 从而它们的最大公约数必然存在且是唯一的。

将最大公约数的定义进行推广, 我们可用 $(a_1, a_2, \dots, a_n)$ 表示不全为零的有限个整数 $a_1, a_2, \dots, a_n$ 的最大公约数:

$$(a_1, a_2, \dots, a_n) = \max\{d; \forall 1 \leq i \leq n, i \in \mathbf{N}, d|a_i\}$$

定义 1.1.4 当 $(a, b) = 1$ 时, 我们称 a 和 b 互素(既约), 即 a 和 b 只有公约数 ± 1 。

定义 1.1.5 设 a, b 是两个均不为零的整数, a 和 b 的最小公倍数是指满足下述条件的整数 m :

- (1) m 为正整数, 且 m 为 a 和 b 的公倍数, 即 $m > 0$, 且 $a|m, b|m$;

(2) m 为 a 和 b 的所有正公倍数中最小者, 即对于整数 c , 如果 $c > 0$, 且 $a | c, b | c$, 则 $m \leq c$ 。

记为 $[a, b]$, 有时也记为 $\text{lcm}(a, b)$ (lcm 即 the least common multiple)。

由定义知 $[a, b] = \min\{m: a | m \text{ 且 } b | m, m > 0\}$ 。

将最小公倍数的定义进行推广, 我们可用 $[a_1, a_2, \dots, a_n]$ 表示均不为零的有限个整数 $a_1, a_2, \dots, a_n$ 的最小公倍数:

$$[a_1, a_2, \dots, a_n] = \min\{m: \forall 1 \leq i \leq n, i \in \mathbf{N}, a_i | m, m > 0\}$$

下面给出了一些关于最大公约数、最小公倍数的性质。

定理 1.1.3

$$(1) (a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b),$$

$$[a, b] = [b, a] = [-a, b] = [a, -b] = [-a, -b];$$

$$(2) \text{ 若 } a | b, \text{ 则 } (a, b) = |a|, [a, b] = |b|;$$

$$(3) \text{ 对任意整数 } x, \text{ 有 } (a, b) = (a, b+ax);$$

$$(4) \text{ 对任意整数 } d | a, \text{ 有 } [a, b] = [a, b, d]。$$

证明 (1)、(2)由定义易知, 证明略。

(3) 设 $g = (a, b)$, $h = (a, b+ax)$ 。由于 $g | a, g | b$, 从而 $g | b+ax$, 即 g 是 a 和 $b+ax$ 的公约数, 于是 $g \leq h$; 另一方面, 由于 $h | a, h | b+ax$, 从而 $h | (b+ax) - ax$, 即 $h | b$, 进而知 h 是 a 和 b 的公约数, 于是 $h \leq g$ 。因此我们有 $h = g$ 。

(4) 由(2)及最小公倍数的定义易知, 证明略。

下面的定理给我们指出这样一个事实: 公倍数一定是最小公倍数的倍数, 公约数一定是最大公约数的约数。

定理 1.1.4

$$(1) a | c, b | c \Leftrightarrow [a, b] | c;$$

$$(2) d | a, d | b \Leftrightarrow d | (a, b)。$$

证明 (1) ($\Leftarrow$) 显然。

($\Rightarrow$) 设 $L = [a, b]$ 。由定理 1.1.2 (带余除法) 知, 存在整数 q, r 使

$$c = qL + r, 0 \leq r < L$$

由 $a | c, b | c$ 知 $a | r$ 且 $b | r$, 所以 r 是 a 和 b 的公倍数。又由最小公倍数的定义及 $0 \leq r < L$ 知 $r = 0$, 即 $L | c$ 。

(2) ($\Leftarrow$) 显然。

($\Rightarrow$) 设 $d_1, d_2, \dots, d_n$ 为 a 和 b 的全体公约数, $L = [d_1, d_2, \dots, d_n]$ 。由(1)稍加推广可知 $L | a, L | b$, 又因为 $d_i | L, i = 1, 2, \dots, n$, 故 $|d_i| \leq L$ 。由最大公约数的定义知 L 为 (a, b) 。所以若 $d | a, d | b$, 则 $d | (a, b)$ 。

由最大公约数和最小公倍数的定义以及定理 1.1.4 可得以下推论。

推论 1.1.4 $(a, b, c) = ((a, b), c), [a, b, c] = [[a, b], c]$ 。