重点大学信息安全专业规划系列教材

信息安全数学基础教程
(第2版)

许春香 周俊辉 廖永建 李发根 编著

清华大学出版社

重点大学信息安全专业规划系列教材

信息安全数学基础教程
(第2版)

许春香 周俊辉 廖永建 李发根 编著

清华大学出版社
北京

内 容 简 介

本书系统地介绍信息安全技术所涉及的数学知识，包括整除与同余、群、循环群与群的结构、环、多项式环与有限域、同余式、平方剩余、原根与离散对数、椭圆曲线和格理论。

本书语言精练、概念准确、例题丰富，可以作为信息安全专业、计算机专业、通信工程专业本科生和研究生的教材，也可以作为密码学和信息安全领域的教师、科研人员与工程技术人员的参考书。

图书在版编目(CIP)数据

信息安全数学基础教程/许春香等编著. --2 版. --北京：清华大学出版社，2015
重点大学信息安全专业规划系列教材
ISBN 978-7-302-37599-9

Ⅰ. ①信… Ⅱ. ①许… Ⅲ. ①信息系统－安全技术－应用数学－高等学校－教材 Ⅳ. ①TP309 ②O29

中国版本图书馆 CIP 数据核字(2014)第 186542 号

责任编辑：付弘宇　王冰飞
封面设计：常雪影
责任校对：时翠兰
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：11.25　　**字　　数**：271 千字
版　　次：2008 年 3 月第 1 版　2015 年 4 月第 2 版　　**印　　次**：2015 年 4 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：039747-01

丛书编委会

INTRODUCTION

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中，电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取，甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革,适应社会对信息安全人才的培养需求,教材内容坚持基本理论的扎实和清晰,反映基本理论和原理的综合应用,在其基础上强调工程实践环节,并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要,促进教学发展。教材要适应多样化的教学需要,正确把握教学内容和课程体系的改革方向,在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时,依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

PREFACE

丛书序

随着信息技术与产业的快速发展，信息和信息系统已经成为现代社会中最为重要的基础资源之一。人们在享受信息技术带来的便利的同时，诸如黑客攻击、计算机病毒泛滥等信息安全事件也层出不穷，信息安全的形势是严峻的。党的十八大明确指出要“高度关注海洋、太空、网络空间安全”。加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。而发展我国信息安全技术与产业对于确保我国信息安全具有重要意义。

信息安全作为信息技术领域的朝阳产业，亟需大量的高素质人才。但与此相悖的是，目前我国信息安全技术人才的数量和质量远不能满足社会的实际需求。因此，培养大量的高素质、高技术信息安全专业人才已成为我国本科高等工程教育领域的重要任务。

信息安全是一门集计算机、通信、电子、数学、物理、生物、法律、管理和教育等学科知识为一体的交叉型新学科。探索该学科的培养模式和课程设置是信息安全人才培养的首要问题。为此，电子科技大学计算机科学与工程学院信息安全专业的专家学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了“高等院校本科信息安全专业系列教材”的编写工作。该套系列教材由《信息安全概论》、《计算机系统与网络防御技术》、《PKI 原理与技术》、《网络安全协议》、《信息安全数学基础》、《密码学基础》等构成。全方位、多角度地阐述信息安全技术的原理，反映当代信息安全研究发展的趋势，突出实践在高等工程教育人才培养中的重要性，为该套丛书的最大特点。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，培养

出更多、更优秀的信息安全人才,编写出更多、更好的信息安全教材,为推动我国信息安全事业的发展做出更大的贡献。

张焕国 教授
武汉大学计算机学院
空天信息安全与可信计算教育部重点实验室

FOREWORD

前言

信息安全技术的核心是密码学，信息安全数学基础是学习密码学所必需的数学基础知识，包括近世代数和初等数论。由于信息安全技术在现代社会的快速发展和广泛应用，信息安全数学基础也得到了普遍重视。

信息安全数学基础包含的都是抽象的数学内容，它概念多，结论(定理)多，而且概念一般都没有物理意义，这对初学者来说是一个挑战。我们在编写本书时只选取了最基本、最必需的内容，力图使用简单清晰的语言来描述抽象的内容。我们认为，只要反复研习，再抽象的内容也能变得具体起来，变得容易把握。

近世代数和初等数论本是两门课程，以前只为数学专业开设，一般是先学习初等数论，再学习近世代数。信息安全数学基础将这两门课程融合成一门课程，这就存在它们能不能够融合和怎么融合两个问题。近世代数与初等数论的关联性很强。例如，整除与同余既是数论的开端，也是近世代数的预备知识。因此，这两门课程是能够融合的，而且融合也是它们共同作为信息安全技术数学基础的客观需求。对于信息安全专业的学生来说，分别完整学习近世代数和初等数论这两门课程内容显得过多，耗时耗力，而在一门课程里同时包含近世代数和初等数论中的必要内容，既满足要求，又高效实用。那么如何融合近世代数和初等数论呢？有两种方法，第一种方法是按照传统的思路，先引入数论，再引入近世代数，在了解剩余类、剩余系、原根等概念的基础上再学习近世代数的群、环和域知识；第二种方法是先引入近世代数，再引入数论，先建立群、环和域的框架后，再学习数论，尽量将数论的内容纳入到群、环和域的框架中。这两种选择各有合理之处，数论先于近世代数发展起来，因此第一种方法符合其自然发展过程，数论知识也有助于近世代数的学习；而第二种方法融合性较好，将两部分内容汇合成一个整体。

本书采取第二种方法，即先建立群、环和域的框架后，再引入数论知识。在数论部分，尽量将群、环和域的结论应用到数论之中。

全书共 10 章。第 1 章介绍整除的概念与性质、互素与素数和同余的定义，这一章是初等数论和近世代数的基础。第 2 章讨论群的定义、子群的定

义及其判定方法、同构和同态的基本概念和变换群与置换群性质。第3章介绍一类特殊的群——循环群,并在此基础上介绍剩余类群、子群的陪集和正规子群与商群。第4章首先介绍环的概念与子环的判定条件,然后介绍3种特殊的环——整环、除环和域,最后介绍环的同态与同构、商环和理想。第5章描述多项式环和有限域,这些知识在密码学中具有重要的应用价值。第6章介绍剩余系的概念、同余式的概念、中国剩余定理和素数模同余式。第7章讨论平方剩余的概念以及判定平方剩余的两个重要工具——勒让德符号和雅可比符号,给出求模 p 平方根的方法。第8章讨论指数和原根的概念、原根存在的判定方法和求法及其离散对数的概念。第9章介绍椭圆曲线的基本概念、椭圆曲线的运算和除子,这章知识为学习椭圆曲线密码体制提供了方便。第10章介绍格理论,包括格的定义、正交化、格中的困难问题和高斯约减算法与LLL算法,这章知识对于学习基于格的密码体制是非常有用的。

本书可以作为信息安全专业、计算机专业、通信工程专业本科生和研究生的教材,也可以作为密码学和信息安全领域的教师、科研人员与工程技术人员的参考书。

本书是在作者编写的《信息安全数学基础》(电子科技大学出版社)的基础上进行修订完成的。主要修订的部分为第1章、第7章和第8章。此外,新增加了第9章和第10章的内容。

作者衷心感谢郝玉洁老师及清华大学出版社的编辑,没有他们的大力支持,本书不可能呈现在读者面前。最后衷心感谢电子科技大学计算机学院领导和同事们在本书编写中给予的支持和帮助。

编　者

2014年12月于成都

CONTENTS

目录

CHAPTER 1

第1章 整除与同余

人们对数的认识可以追溯到最初的自然数，随着对自然界认识的不断深入，就有了整数的概念。在初等数论中，读者已经对整数和素数等知识进行了学习。随着学习的深入，有必要重新系统、深入地学习和讨论整数的整除、素数等概念。本章将深入讨论整除、互素和素数的概念，同时还要对同余等概念进行介绍，为后面的学习奠定基础。

1.1 整除

在本节中探讨整数的一些基本概念和性质。设整数 $Z=\{\cdots,-2,-1,0,1,2,\cdots\}$，下面介绍整数的一些性质，首先给出整除的定义。

定义 1-1 设 a、b 是任意两个整数，其中 $b\neq 0$，如果存在一个整数 q，使

$$a = qb \tag{1-1}$$

则称 b 整除 a，或 a 被 b **整除**，记为 $b|a$，此时称 b 是 a 的**因子**，a 是 b 的**倍数**。反之，a 不被 b **整除**，记为 $b\nmid a$。

例 1-1 $3|39,84\nmid 254,256|5376$。

例 1-2 设 a 是整数，且 $a\neq 0$，则 $a|0$。

为了更好地理解整除的性质，这里给出整除的 3 个基本定理。

定理 1-1 设 a、b、c 是整数。

(1) 如果 $b|a$ 且 $a|b$，则 $b=a$ 或 $b=-a$。

(2) 如果 $a|b$ 且 $b|c$，则 $a|c$。

(3) 如果 $c|a$ 且 $c|b$，则 $c|ua+vb$，其中 u、v 是整数。

(4) 如果 $c|a_1$、$\cdots$、$c|a_k$，则对任意整数 u_1、$\cdots$、u_k 有 $c|(u_1a_1+\cdots+u_ka_k)$。

事实上，由于考虑的是所有整数，因此包括了负数，所以性质(1)表明在考虑问题时不要局限于正整数；而性质(2)是整除的传递性；性质(4)是性质(3)的推广。

证明：对于这 4 个基本的整数性质，从定义出发就能得到结论。

(1) 因为 $b|a$，由整除的定义，则存在整数 q_1 使得

$$a = q_1 b$$

又因为 $a|b$,则同理得到,存在整数 q_2 使得

$$b = q_2 a$$

于是

$$a = q_1 b = q_2 q_1 a$$

由于 a 非零,因此有 $q_2 q_1 = 1$。又因为 q_1、q_2 是整数,则

$$q_2 = q_1 = 1 \quad 或 \quad q_2 = q_1 = -1$$

故

$$b = a \quad 或 \quad b = -a$$

(2) 因为 $a|b$,则存在整数 q_1,使得

$$b = q_1 a$$

又因为 $b|c$,则存在整数 q_2,使得

$$c = q_2 b$$

所以有

$$c = q_2 b = q_2 q_1 a = qa,\text{其中 } q = q_2 q_1$$

由整除的定义,有 $a|c$。

(3) 因为 $c|a$ 和 $c|b$,则分别存在整数 q_1 和 q_2,使得

$$a = q_1 c, \quad b = q_2 c$$

所以对任意的整数 u、v,有

$$ua + vb = uq_1 c + vq_2 c = (uq_1 + vq_2)c$$

由整除的定义,有 $c|ua+vb$。

(4) 由于证明与性质(3)类似,这里就不重复了,读者可以自己证明。

除了这4个性质定理,还可以从整除的定义得到以下一些简单而有趣的事实。

(1) 0是任何非零整数的倍数。

(2) ± 1 是任何整数的因子。

(3) 任何非零整数 a 是其自身的倍数。

两个整数除了整除关系外,还有一种关系就是不整除。而当两个整数不能整除时,经常会接触到的方法就是带余除法。

定义 1-2 对于 a、b 两个整数,其中 $b \neq 0$,则 $a = bq + r$,$0 \leqslant r < |b|$。其中 r 称为 a 被 b 除得到的**余数**。显然当 $r = 0$ 时,$b|a$。

注:在带余数除法中,要求余数 r 必须大于等于0且小于 b 的绝对值。如果没有这个条件,对任意的整数 k,等式 $a = b(q-k) + (r+kb)$ 总是成立,那么带余除法的表示就不唯一,即能得到不同的 q 和 r。

例 1-3 (1) $a = -347$,$b = 5$,则

$$-347 = (-70) \times 5 + 3, \quad r = 3$$

(2) $a = 131$,$b = -5$,则

$$131 = (-26) \times (-5) + 1, \quad r = 1$$

(3) $a = 86\,794$,$b = -265$,则

$$86\,794 = (-327) \times (-265) + 139, \quad r = 139$$

定义 1-3

(1) 设 a、b 是两个整数，如果整数 $c|a$ 且 $c|b$，则 c 称为 a、b 的公因子。

(2) 设 $c>0$ 是两个不全为零的整数 a、b 的公因子，如果 a、b 的任何公因子都整除 c，则 c 称为 a、b 的**最大公因子**，记为 $c=(a,b)$，或者 $c=\gcd(a,b)$。

注：在(2)里面要求 a、b 的任何公因子都整除 c，这就说明了 c 的绝对值是公因子里面最大的，又要求 $c>0$，所以 c 一定是 a、b 的公因子里最大的一个，且唯一。

定理 1-2　由最大公因子的定义，能得到如下的结论。

(1) $(a,b)=(-a,b)=(a,-b)=(-a,-b)$。

(2) $(0,a)=|a|$。

由于定理的证明可以用最大公因子的定义简单推导，在此就不证明了。

例 1-4　2、5、7 是 140、−210 的公因子，同样的，−2、−5、−7 是 140、−210 的公因子。140、210 的最大公因子(140，−210)=70。

在此能注意到 140 和 −210 的任何公因子也是 −70 的因子，但它们的最大公因子是 70，这就是为什么在定义中要求两个数的最大公因子 $c>0$ 这个条件。

已知两个整数 a、b，求它们的最大公因子，最直观也是最简单的方法就是通过分解它们再找公因子和最大公因子。

例 1-5　设整数 $a=-2^3\times5^2\times7^3$，$b=2^5\times5\times7$，则最大公因子 $(a,b)=(-a,b)=2^3\times5\times7=280$。

但是当整数和其因子很大时，则没有好的方法来对整数进行分解(分解一个非常大的整数被认为是很困难的问题)，因此需要比较高效的方法——**欧几里得除法**(又称**辗转相除法**)。由定义 1-3 和定理 1-2 可以知道，整数的正负性是不影响它们的因子和公因子的，也就不影响两个整数的最大公因子。因此在使用欧几里得除法时只考虑计算两个正整数的最大公因子。

设 a、b 是两个正整数，记 $r_0=a$，$r_1=b$，于是有：

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 \leqslant r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && 0 \leqslant r_3 < r_2 \\
&\vdots \\
r_{l-2} &= q_{l-1} r_{l-1} + r_l, && 0 \leqslant r_l < r_{l-1} \\
r_{l-1} &= q_l r_l \\
r_l &= (a,b)
\end{aligned}
$$

欧几里得除法是非常高效的算法，下面证明欧几里得除法的正确性。

定理 1-3　设 a、b 是正整数，使用欧几里得除法计算得到 r_l，则 r_l 是 a、b 的最大公因子。

证明：

(1) 首先证明 r_l 是 a、b 的公因子。

从等式 $r_{l-1}=q_l r_l$ 中得到 $r_l|r_{l-1}$，即 r_l 整除 r_l 和 r_{l-1}，是 r_l 和 r_{l-1} 的公因子；

从等式 $r_{l-2}=q_{l-1}r_{l-1}+r_l$ 中得到 $r_l|r_{l-2}$，即 r_l 整除 r_{l-1} 和 r_{l-2}，是 r_{l-1} 和 r_{l-2} 的公因子；

$\vdots$

因此，r_l 整除 r_1、r_0，所以 r_l 是 a、b 的公因子。

(2) 其次证明 r_l 是 a、b 的最大公因子，即证明 a、b 的任意公因子都是 r_l 的因子。

如果 d 是 a、b 的任意公因子,根据定理 1-1 的第 3 个性质,从等式 $r_0=q_1r_1+r_2$ 中得到 $d|r_2$,即 d 整除 r_1 和 r_2;同理,d 整除 r_3、…、r_{l-2}、r_{l-1}、r_l。

由(1)、(2),根据最大公因子的定义,得到 $r_l=(a,b)$。

例 1-6 (1) $a=888,b=312$,求(a,b)。

(2) $a=-3824,b=1837$,求(a,b)。

解:(1)

$$\begin{aligned}888&=2\times312+264\\312&=1\times264+48\\264&=5\times48+24\\48&=2\times24\end{aligned}$$

故(888,312)=24。

(2)

$$\begin{aligned}(-3824,1837)&=(3824,1837)\\3824&=2\times1837+150\\1837&=12\times150+37\\150&=4\times37+2\\37&=18\times2+1\\2&=2\times1\end{aligned}$$

得(3824,1837)=1,故(−3824,1837)=1。

欧几里得除法作为密码学中的基础算法,其计算机实现非常简单,下面进行介绍。

```
输入: a,b
输出: a 和 b 的最大公因子(a,b)
    (1) x←a; y←b;
    (2) while(y≠0)do
        (i) r = x mod y;
        (ii) x←y;
        (iii) y←r;
    (3) return x = (a,b).
```

表 1-1 给出了利用计算机实现来求 $a=888$ 和 $b=312$ 的最大公因子的具体过程,最后返回 $x=24=(a,b)$。

表 1-1 求(888,312)的具体过程

循环	x	y	r
初始值	888	312	
1	312	264	264
2	264	48	48
3	48	24	24
4	24	0	0

欧几里得除法可以求两个整数的最大公因子,同时为了后面的性质,这里给出下面的一个重要定理,该定理表明两个整数的最大公因子可以用这两个整数的线性组合表示出来。

定理 1-4 设 a、b 是两个不全为零的整数,则存在两个整数 u、v,使得