信息安全系列教材

# 信息安全数学基础

主　编　李继国　余纯武　张福泰　马春光
副主编　宋燕红　陆　阳　张亦辰　沈丽敏　武　朋



WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全系列教材

# 信息安全数学基础

主　编　李继国　余纯武　张福泰　马春光
副主编　宋燕红　陆　阳　张亦辰　沈丽敏　武　朋

WUHAN UNIVERSITY PRESS
武汉大学出版社

**图书在版编目(CIP)数据**

信息安全数学基础/李继国,余纯武,张福泰,马春光主编.—武汉:武汉大学出版社,2006.9
信息安全系列教材
ISBN 7-307-05234-2

Ⅰ.信… Ⅱ.①李… ②余… ③张… ④马… 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116123号

责任编辑:林 莉 责任校对:黄添生 版式设计:支 笛

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)
印刷:湖北新华印务有限责任公司
开本:787×1092 1/16 印张:13.875 字数:352千字
版次:2006年9月第1版 2006年9月第1次印刷
ISBN 7-307-05234-2/TP·219 定价:20.00元

# 信息安全系列教材

## 编 委 会

# 内容提要

本书全面系统地介绍了数论、代数、组合数学等相关基础理论和密码学研究中用到的一些实用算法。包括整除、同余、二次同余式与平方剩余、原根、群、环、有限域、格及其应用、椭圆曲线、组合数学等数学知识以及素性测试、因数分解和离散对数计算等一些实用算法，共13章。书末列出了主要参考文献。本书可作为信息安全、计算机科学与技术、通信工程、数学与应用数学等专业本科生和研究生的教材，也可供从事信息安全、密码学和其他信息技术工作的科研和工程技术人员参考。

# 序　言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

**编委会**

2006 年 9 月 19 日

# 前 言

在计算机技术和网络技术快速发展的信息时代，信息安全受到了社会各界的高度关注。信息安全与国家的军事、外交、政治、经济、金融，甚至普通老百姓的日常生活的关系越来越密切。世界各个国家和地区政府都非常重视自己国家和地区的信息安全问题，在信息安全的基础设施建设、教学以及研究开发方面不断加大人力、物力和财力的投入。近十多年来，我国政府对信息安全的关注与支持也是与日俱增，在国家自然科学基金、863、973 等重要研究和开发计划中，都把信息安全列入了重点资助对象，并相继在一些高等院校中设立了信息安全本科专业。有专家学者指出“未来的信息战争在某种程度上是数学的战争”，可见数学在信息安全中的地位和作用。在信息安全和密码学的学习和研究中，如信息安全模型的建立、密码体制的设计、安全性证明（尤其是可证安全证明）以及对密码体制的形式化分析和密码分析，涉及数论、代数、组合数学等数学知识，而系统介绍信息安全研究和应用所需的相关数学知识的教材较少。本教材——《信息安全数学基础》，正是为适应信息安全本科专业需求编写的系列教材之一。

信息安全数学基础在信息安全中占有非常重要的地位，能够为信息安全的相关理论与技术提供必要的基础知识。因此，信息安全数学基础是信息安全本科专业的主要专业课程之一。

《信息安全数学基础》是针对我国信息安全本科专业学生的基础和实际情况，根据国家的有关指导性意见编写的。教材全面系统地介绍了数论、代数、组合数学等相关基础理论和密码学研究中用到的一些实用算法。在本书编写过程中，作者参考了大量的国内外书籍和论文，由于资料来源的广泛性，书中只列出了主要参考文献，书中引用的很多资料没有一一注明出处，在此我们对这些资料的作者表示由衷的感谢，同时声明原文版权属于原作者。全书共分十三章。第 1 章整除，详细地介绍了整除、素数、最大公因数、最小公倍数的概念、性质及相关定理。第 2 章同余，系统地介绍了同余的概念、性质、相关定理及其在密码学中的应用。第 3 章二次同余式与平方剩余，系统地介绍了二次同余式与平方剩余的概念、性质、相关定理及其在密码学中的应用。第 4 章原根，主要介绍原根的定义、基本性质、存在性问题和一些基本计算方法。第 5 章群，首先给出了与代数系统相关的准备知识，然后介绍了群的定义及相关的性质，并进一步介绍了置换群和循环群的有关理论和方法在计算机密码学中的应用。第 6 章环，重点介绍了环的定义、环的基本性质以及如何利用非负整数环中幂等元素所具有的性质来建立公钥加密算法的实例。第 7 章有限域理论，对信息安全中常用的有限域理论进行了较为深入的讨论。主要介绍有关域的基本理论，包括域的扩张的基本概念、有限域的性质与构造等。第 8 章格及其应用，首先介绍格的预备知识——偏序关系和偏序集，然后给出格的两个等价定义，在此理论基础上，进一步介绍了格在计算机信息系统信息流控制中的应用及几种基于格的安全模型。第 9 章椭圆曲线，主要介绍椭圆曲线的概念、性质和椭圆曲线密码体制。第 10 章组合数学，主要介绍组合数学中最基本的一些内容，包括排列与组合、鸽巢原理、容斥原理、递推关系、生成函数、编码理论等相关知识。第 11 章素性测试，首先对素性测试的基本思想进行了介

绍，然后给出了常用的几个素性测试算法，如 Miller-Rabin 算法和 Lehmann 算法。第 12 章因数分解，介绍常用的因数分解方法。第 13 章离散对数计算，介绍求解离散对数问题的算法。

教材内容全面系统，叙述简洁清楚。为了使学生对所学知识更好地理解，我们在大部分章节给出了相关数学知识在信息安全和密码学中的应用实例或者指出了它们在信息安全和密码学中的什么地方使用，如何使用，怎么使用，以免使学生感到枯燥乏味。我们在各章设置了必要的实验和习题，供读者操作和训练，以加强对所学原理、方法的掌握和应用。

包括实验在内，建议总学时数为 72 学时。授课教师可根据学生情况及教学时间，适当选取课堂讲授内容，特别是对第 10 章至第 13 章的内容，可舍弃或只选讲部分。

本教材由多所高校富有教学和研究经验的教师合作编写。参加编写的主要有：河海大学李继国副教授、武汉大学余纯武副教授、南京师范大学张福泰教授、哈尔滨工程大学马春光副教授、北京电子科技学院宋燕红讲师、河海大学陆阳讲师、河海大学张亦辰讲师、南京师范大学沈丽敏讲师、哈尔滨工程大学武朋讲师，最后的统稿与修改工作由河海大学李继国副教授和南京师范大学张福泰教授完成。河海大学与南京师范大学的研究生王爱芹、章春宇、徐倩、陈礼青、张磊、孙银霞等仔细阅读了全部初稿。提出了不少宝贵的修改意见。在此对所有参与编写和修改的老师和同学表示衷心的感谢。还要感谢武汉大学张焕国教授、武汉大学出版社黄金文老师对编写本教材所给予的帮助和支持，感谢我的导师曹珍富教授多年来的关心、鼓励和支持。另外，特别感谢江苏省公安厅科研项目（编号：200503002）的支持。

尽管我们对全部书稿进行了多次的修改和订正，但由于时间仓促以及知识水平所限，书中的错误和不当之处在所难免，恳请使用的老师和同学把你们所发现的问题、意见和建议及时反馈给我们，可发 E-mail 到 lijiguo@ hhu. edu. cn，ljg1688@ 163. com，zhangfutai@ njnu. edu. cn 或 ffttzhang@ sina. com。任何意见和建议都是对我们的鞭策与支持，谢谢你们。

作　者

2006 年 8 月

# 目 录

# 第1章 整 除

在整数集合中，整除是一种非常重要的二元关系，伴随着整除的性质，有素数、最大公因数、最小公倍数、余数定理和算术基本定理等基本概念和性质，这些概念和性质是研究整数集合中另外一种二元关系——同余关系的基础。

## 1.1 整除的基本性质和余数定理

**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 $q$ 使得等式 $a=bq$ 成立，就称 $b$ 整除 $a$ 或者 $a$ 被 $b$ 整除，记做 $b|a$，并把 $b$ 叫做 $a$ 的因数，把 $a$ 叫做 $b$ 的倍数。否则，就称 $b$ 不能整除 $a$ 或者 $a$ 不能被 $b$ 整除，记做 $b\nmid a$。

由定义可知，0 是任何非零整数的倍数；1 是任何整数的因数；任何非零整数既是其自身的因数，又是其自身的倍数。由定义 1-1 及乘法运算的性质，立即可以得到整除关系具有如下性质：

**性质 1-1** (1) $b|a\Leftrightarrow -b|a\Leftrightarrow b|-a\Leftrightarrow |b|\,|\,|a|$；

(2) $c|b$ 且 $b|a\Rightarrow c|a$；

(3) $c|a$ 且 $c|b\Leftrightarrow$对任意的整数 $x,y$ 有 $c|(ax+by)$；

(4) $b|a$ 且 $a|b\Rightarrow a=\pm b$；

(5) 设 $c\neq 0$，则 $b|a\Leftrightarrow bc|ac$；

(6) 若 $a\neq 0$，则 $b|a\Rightarrow |b|\leqslant |a|$；

(7) 若 $b\neq 0$，且 $\{d_1,d_2,\cdots,d_k\}$ 是 $b$ 的全体因数，则 $\{b/d_1,b/d_2,\cdots,b/d_k\}$ 也是 $b$ 的全体因数。

前面的六个性质由整除的定义很容易得到，对于(7)，如果分别令 $A=\{d_1,d_2,\cdots,d_k\}$，$B=\{b/d_1,b/d_2,\cdots,b/d_k\}$，我们只需证明集合 $A=B$ 即可。

对于任意 $x=d_i\in A,1\leqslant i\leqslant k$，因为 $d_i$ 是 $b$ 的因数，即 $d_i|b$，所以存在整数 $q$ 使得 $b=qd_i$，从而 $q|b$，即 $q$ 也是 $b$ 的因数，所以 $q\in A$，即存在整数 $1\leqslant j\leqslant k$，使得 $q=d_j$，即 $x=d_i=\dfrac{b}{d_j}\in B$，所以有 $A\subseteq B$；反之，任意 $x=\dfrac{b}{d_i}\in B,1\leqslant i\leqslant k$，因为 $x|b$，所以 $x$ 是 $b$ 的因数，而 $A$ 是 $b$ 的全体因数构成的集合，所以 $x\in A$，由 $x$ 的任意性得 $B\subseteq A$，从而有 $A=B$。

这些看起来非常简单的性质是很有用的。

**例 1-1** 证明：若 $3|n,5|n$，那么 $15|n$。

**证** 由整除的定义及 $3|n$ 可知，存在整数 $m$，使得 $n=3m$，所以 $5|3m$。又因为 $5|5m$，所以由性质 1-1(3)得 $5|(2\cdot 3m-5m)=m$，从而由性质 1-1(5)得 $15|3m=n$。

**例 1-2** 设 $a,b$ 是两个非零整数，且存在整数 $s,t$，使得 $sa+tb=1$。证明：

(1)若 $m\mid a,m\mid b$，则有 $m=\pm 1$；

(2)若 $a\mid n,b\mid n$，则有 $ab\mid n$。

**证** (1)由性质 1-1(3)得 $m\mid(sa+tb)=1$，从而由性质 1-1(4)有 $m=\pm 1$。

(2)由 $n=n(sa+tb)=s(na)+t(nb)$ 和 $ab\mid na,ab\mid nb$ 得 $ab\mid(s(na)+t(nb))=n$。

**例 1-3** 设 $a$ 为奇数，$b$ 为偶数，且 $a\mid b$，则 $a\mid\frac{b}{2}$。

**证** 因为 $a$ 为奇数，$b$ 为偶数，所以存在整数 $m,n$，使得 $a=2m-1,b=2n$。因为 $a\mid b=2n$，所以 $a\mid 2mn=(an+n)$，结合 $a\mid an$ 得 $a\mid(an+n-an)=n$，从而 $a\mid\frac{b}{2}$。

**定义 1-2** 设整数 $n\neq 0,\pm 1$，如果除了因数 $\pm 1$ 和 $\pm n$ 外，$n$ 没有其他因数，则称 $n$ 为素数(或质数)，否则称其为合数。

由定义可以看出，0 和 $\pm 1$ 既不是素数，又不是合数；当 $n\neq 0,\pm 1$ 时，由于 $n$ 和 $-n$ 必同时为素数或者合数，所以，以后没有特别说明，素数总是为正。例如，2,3,5,7,11,13,17,19,23,29,31,37,41,43,47 都是素数。这里自然出现的三个问题是：(1)素数如何判定？(2)素数和合数之间具有怎样的关系？(3)素数的个数是有限的还是无限的？如果是有限的，就可以造一张包括一切素数的素数表，使用起来就非常方便了，但是很遗憾，下面将给出否定的回答。首先给出素数的一个判定定理。

**定理 1-1** 设 $n$ 是一个大于 1 的正整数，如果对所有小于或等于$\sqrt{n}$的素数 $p$，都有 $p\nmid n$，则 $n$ 一定是素数。

**证** 用反证法。如果 $n$ 不是素数，则 $n$ 必为合数。令 $T=\{d\geqslant 2\mid d\mid n\}$，因为 $1<n\in T$，所以 $T$ 是有下界的非空集合，从而集合 $T$ 中一定存在最小的正整数，设为 $p$，则 $p$ 一定为素数，否则，$p\geqslant 2$ 是合数，由定义 1-2 知，必有因数 $d'$，使 $2\leqslant d'<p$。显然 $d'\in T$，这和 $p$ 的最小性矛盾。因为 $p\mid n$，所以存在整数 $q$，使得 $n=pq$，则 $q\geqslant 2$，否则 $n=p$，由于 $p$ 是 $n$ 的大于 1 的最小正因数，与 $n$ 为合数矛盾。从而 $q\in T$，由 $p$ 的定义知 $p\leqslant q$，所以 $n=pq\geqslant p^2$，即 $p\leqslant\sqrt{n},p\mid n,p$ 为素数，与题设矛盾。所以 $n$ 一定是素数。

由定理 1-1，对于比较小的整数，我们可以迅速地判断出它是否为素数。

**例 1-4** 求出所有不超过 100 的素数。

**解** 因为$\sqrt{100}=10$，小于或等于 10 的素数有 2,3,5,7，则可以按照如下算法求出所有不超过 100 的素数。

**算法 1-1** (1)输出 2 3 5 7 ，$i=8$；

(2)如果 $2\mid i$，则 $i$ 不是素数，转到(7)；

(3)如果 $3\mid i$，则 $i$ 不是素数，转到(7)；

(4)如果 $5\mid i$，则 $i$ 不是素数，转到(7)；

(5)如果 $7\mid i$，则 $i$ 不是素数，转到(7)；

(6)输出 $i$ 的值；

(7)$i=i+1$；

(8)如果 $i>100$，程序结束；

(9) 否则返回到(2)。

输出的结果为

| | | | |
|---|---|---|---|
| 2 | 3 | 5 | 7 |
| 11 | 13 | 17 | 19 |
| 23 | 29 | | |
| 31 | 37 | | |
| 41 | 43 | 47 | |
| 53 | 59 | | |
| 61 | 67 | | |
| 71 | 73 | 79 | |
| 83 | 89 | | |
| 97 | | | |

从例 1-4 我们可以看出 100 以内素数粗略的分布情况，10 以内的素数有 4 个，10 ~ 20 之间的素数有 4 个，40 ~ 50 和 70 ~ 80 之间的素数都是 3 个，90 ~ 100 之间的素数只有 1 个，是否素数越来越稀疏呢？这需要到后面再回答这个问题。进一步可以由上述例题求出 $n = 10\ 000$ 以内的素数，这种求素数的方法称为爱拉托斯散(Eratosthenes)筛法。

由定理 1-1 可以看出对每个不等于 1 的整数都有一个素因数，下面我们要证明每个整数一定可以表示成素数的乘积。

**定理 1-2** 任一整数 $n > 1$ 都可以表示成素数的乘积，即

$$n = p_1 p_2 \cdots p_r, \quad p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r \tag{1-1}$$

其中 $p_i$ 是素数。

**证** 当 $n = 2$ 时，2 是素数，所以结论成立。

假设对于某个 $n$，当 $2 \leqslant a < n$ 时，结论对所有这种 $a$ 都成立。

当 $a = n$ 时，若 $n$ 是素数，则结论成立；若 $n$ 是合数，则必有

$$n = bc, 2 \leqslant b < n, 2 \leqslant c < n。$$

由假设知 $b, c$ 都可表示为素数的乘积：

$$b = p'_1 p'_2 \cdots p'_k, c = p'_{k+1} p'_{k+2} \cdots p'_r$$

于是，

$$n = p'_1 p'_2 \cdots p'_r$$

适当改变 $p'_i$ 的次序即得(1-1)式。由数学归纳法知对所有大于 1 的整数 $n$ 都成立。

下面我们将回答第三个问题。

**定理 1-3** 素数有无穷多个。

**证** 用反证法。假定素数只有有限个，将它们罗列如下：

$$p_1 = 2, p_2 = 3, \cdots, p_k$$

整数 $n = p_1 \cdot p_2 \cdots p_k + 1$，因为 $n > p_i, i = 1, 2, \cdots, k$，所以 $n$ 一定是合数。根据定理 1-1，$n$ 的大于 1 的最小正因数一定是素数，因此存在某一个 $1 \leqslant j \leqslant k$，使得 $p_j \mid n$，由整除的基本性质(3)得：

$$p_j \mid (n - p_1 p_2 \cdots p_k) = 1$$

这是不可能的。故存在无穷多个素数。

进一步，还有如下结论：

**定理 1-4** 形如 $4k - 1$ 的素数有无穷多个。

**证** 首先证明形如 $4k - 1$ 的正整数 $n$ 的素因数必是 $4k - 1$ 形式的。否则，它的所有素因数都形如 $4k + 1$，由定理 1-2 可知

$$n = p_1 \cdot p_2 \cdots p_r, p_i = 4k_i + 1, i = 1,2,\cdots,r$$

从而得到 $n$ 是形如 $4k+1$ 的正整数，与 $n$ 是 $4k-1$ 形式的正整数矛盾。

其次假设形如 $4k-1$ 素数只有有限个，依次为 $q_1, q_2, \cdots, q_s$。考虑整数

$$n = 4q_1q_2\cdots q_s - 1$$

则 $n$ 是形如 $4k-1$ 的正整数，所以 $n$ 必有相同形式的素因数 $q$，因此存在某一个 $1 \leqslant j \leqslant s$，使得 $q = q_j$，由整除的基本性质(3)有

$$q \mid (4q_1q_2\cdots q_s - n) = 1$$

这是不可能的。故存在无穷多个形如 $4k-1$ 的素数。

上述两个定理都说明了一个问题：素数有无穷多个。若以 $\pi(x)$ 表示不超过实数 $x$ 的素数个数，记 $p_n$ 为第 $n$ 个素数，我们很容易得到 $\pi(x)$ 的一个很弱的下界估计和 $p_n$ 的一个很弱的上界估计。

**定理 1-5** 设全体素数按大小顺序排成的序列是：

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4, p_5, \cdots$$

我们有

$$\pi(x) > \log_2\log_2 x, \quad 2 \leqslant x \tag{1-2}$$

和

$$p_n \leqslant 2^{2^{n-1}}, \quad n = 1,2,\cdots \tag{1-3}$$

**证** 首先我们可以看出，对于 $n > 1$，有

$$p_n \leqslant s = p_1p_2\cdots p_{n-1} + 1 \tag{1-4}$$

否则 $P_{n-1} < s < p_n$，所以 $s$ 为合数，类似于定理 1-3 的证明可以得到某一个素数为 1 这样的矛盾。下面用数学归纳法证明(1-3)式。当 $n = 1$ 时，(1-3)式显然成立。假设对于所有 $n \leqslant k$，(1-3)式成立，当 $n = k+1$ 时，由(1-4)式和归纳假设得

$$p_{k+1} \leqslant 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{k-1}} + 1 = 2^{2^k - 1} + 1 < 2^{2^k}$$

即(1-3)式对 $n = k+1$ 也成立，从而由数学归纳法知(1-3)式成立。

对任意 $x \geqslant 2$，必有惟一的正整数 $n$，使得 $2^{2^{n-1}} \leqslant x < 2^{2^n}$，因而由(1-3)式可得

$$\pi(x) \geqslant \pi(2^{2^{n-1}}) \geqslant \pi(p_n) = n > \log_2\log_2 x$$

由此得到(1-2)式。

进一步运用简单的微积分知识我们可以得到更强一些的 Chebyshev 不等式估计。

**定理 1-6** 设实数 $x \geqslant 2$，我们有

$$\left(\frac{1}{6\ln 2}\right)n\ln n < p_n < \left(\frac{8}{\ln 2}\right)n\ln n, \quad n \geqslant 2$$

$$\left(\frac{\ln 2}{3}\right)\frac{x}{\ln x} < \pi(x) < 6\ln 2\,\frac{x}{\ln x}$$

事实上，还可以得到如下的极限形式

$$\pi(x)\ln x/x \to 1, \qquad x \to +\infty,$$

$$p_n/(n\ln n) \to 1, \qquad n \to \infty。$$

这个结论也被称为素数定理。由素数定理可知，当 $x$ 很大时，$\pi(x) \approx \frac{x}{\ln x}$，表 1-1 说明了此种估计公式在 $x$ 越大时越准确。