普通高等教育“十一五”国家级规划教材

重点大学信息安全专业规划系列教材

信息安全数学基础
(第2版)

陈恭亮 主编

清华大学出版社

普通高等教育“十一五”国家级规划教材

重点大学信息安全专业规划系列教材

信息安全数学基础
(第2版)

陈恭亮 主编

清华大学出版社
北京

内 容 简 介

本书用统一的数学语言和符号系统地介绍了网络与信息安全所涉及的数学理论和方法，特别是与三大难解数学问题相关的数论、代数和椭圆曲线理论等，并对一些重要算法作了详尽的推理和阐述。此外，还介绍了网络与信息安全研究和应用中所产生的新的数学成果。

本书可作为网络与信息安全专业、通信安全、计算机安全和保密专业等的本科生和研究生的教学用书，也可以作为网络与信息安全的专业人员和从业人员的参考用书。

图书在版编目(CIP)数据

信息安全数学基础/陈恭亮主编. -- 2 版. --北京：清华大学出版社，2014
重点大学信息安全专业规划系列教材
ISBN 978-7-302-37035-2

Ⅰ. ①信… Ⅱ. ①陈… Ⅲ. ①信息系统-安全技术-应用数学 Ⅳ. ①TP309 ②O29

中国版本图书馆 CIP 数据核字(2014)第 143102 号

责任编辑：魏江江　薛　阳
封面设计：常雪影
责任校对：梁　毅
责任印制：沈　露

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
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：26.75　　**字　　数**：668 千字
版　　次：2004 年 6 月第 1 版　2014 年 10 月第 2 版　　**印　　次**：2014 年 10 月第1 次印刷
印　　数：28501～30500
定　　价：45.00 元

产品编号：041210-01

引　言

信息安全学科是一门新兴的学科, 它涉及通信学、计算机科学、信息学和数学等多个学科, 其中公钥密码学所基于的三个难解数学问题是:

(1) 大因数分解问题;

(2) 离散对数问题;

(3) 椭圆曲线离散对数问题.

这些问题涉及数论、代数和椭圆曲线论等, 但应用于信息安全的数学理论和知识只是这些数学理论中的一小部分, 而有关数论、代数和椭圆曲线论等方面的书籍多半是针对数学专业的学生的. 此外, 在信息安全研究和应用中所产生的一些新的数学成果也没有在数论、代数和椭圆曲线论等教科书中体现.

作者自 2000 年以来, 在武汉大学数学系和计算机学院信息系以及上海交通大学信息安全工程学院给本科生和研究生相继开设了“数论与密码”、“椭圆曲线论”和“信息安全数学基础”等课程, 深知学生在学习与信息安全相关的数学知识, 特别是关于数论、代数和椭圆曲线论等数学知识的过程中所遇到的困难. 因此, 希望将这些应用于信息安全的数学理论作一次较系统的介绍, 以方便信息安全专业、数学系、计算机学院、通信工程系等学生以及信息安全方面的工作者学习.

本书在编写过程中得到了上海交通大学信息安全工程学院及武汉大学数学系和计算机学院信息系许多教师以及本科生和研究生的支持和帮助, 在此向他们表示衷心的感谢. 此外, 特别感谢姚家燕、周超勇和沈丽敏的许多具体帮助. 另外, 特别感谢国家自然科学基金青年基金 (项目编号: 19501032) 和国家教委优秀青年教师基金的支持.

陈恭亮

2004 年 2 月

第 2 版引言

本书自 2004 年 6 月出版后，在上海交通大学、武汉大学、西安电子科技大学、北京电子技术学院、杭州电子科技大学等几十所高校使用. 许多教师和学生提出了很多宝贵建议. 作者根据这些建议，面向传统教学和远程教学、视频课程教学、MOOC 课程教学和“翻转式”课堂教学等，以及信息安全专业学生、网络和信息安全从业人员对网络和信息安全的数学理论和方法的需求，结合网络与信息安全技术的最新进展，以及“信息安全数学基础”课程教学经验的积累，特别是“发现、学习、寻求、解决、提升”的教学理念，对本书作了一些修订.

(1) 基础性: 对网络和信息安全所涉及的数学理论和方法及重要算法给出了详细的推理和说明.

(2) 系统性: 用统一的数学语言和符号来将三大数学难题、网络和信息安全所涉及的散落在数论、代数、椭圆曲线三方面的数学知识形成系统的知识体系.

(3) 前沿性: 密切跟踪国际上的信息安全和密码算法标准，并给出详细阐述.

(4) 重构性: 对定理及例题作了更有序的编号, 使得一些知识可以构成独立的知识体系, 以满足网络和信息安全专业人员和非专业人员对相关知识的学习和掌握.

(5) 专业性: 对一些数学符号和语言作了更系统的表述, 以满足网络和信息安全专业人员和非专业人员对相关知识的进一步学习和掌握.

(6) 工程性: 对一些重要定理及应用作了更详细的阐述, 以满足网络和信息安全专业人员和非专业人员对相关工程实现和创新应用的需求.

发现: 就是要发现信息化推进中不断提出的网络和信息安全问题 (如国际密码标准 P1363，密码技术、RSA、Diffie-Hellman 密钥协商、ECC、AES、物联网安全、轻量级密码技术、身份认证鉴别、认证加密和身份管理等) 以及国内外相关信息通信技术的新进展.

学习: 就是要学习该课程所涉及的基本数学理论和方法, 如学习与三大难解数学问题 (大整数分解问题、离散对数问题、椭圆曲线离散对数问题) 相关的整数理论、同余理论、代数理论、椭圆曲线理论等.

寻求: 就是要寻求关于网络和信息安全问题的应用技术, 如广义欧几里得除法、中国剩余定理、欧拉定理、大素数生成、有限域的构造、Galois 域等.

解决: 就是要运用基本理论和方法，以及应用技术解决信息安全的工程问题, 如公钥加密/解密、密钥协商等.

提升: 就是要在发现、学习、寻求、解决的过程中提升科学素养，进而发现更深层的信息安全问题并提高学习和创新能力.

陈恭亮

2014 年 2 月于巴黎

目　录

第 1 章　整数的可除性

信息通信技术的广泛应用需要信息的数字化. 在保证信息的安全性和有效性 (如公钥密码系统即 RSA) 时往往要用到整数的算术性质, 所以本章将讨论整数的算术性质、基本理论和方法, 特别是整除、因数、素数、最大公因数、最小公倍数以及欧几里得除法和广义欧几里得除法, 最后给出算术基本定理和素数定理.

1.1　整除的概念、欧几里得除法

1.1.1　整除的概念

本节考虑关于整数的一些基本概念和性质: 整除和欧几里得除法.

首先考虑具有一般意义的整除定义, 它只涉及乘法运算.

定义 1.1.1　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

$$a = q \cdot b \tag{1.1}$$

成立, 就称 b **整除** a 或者 a 被 b 整除, 记作 $b \mid a$, 并把 b 叫做 a 的 **因数**, 把 a 叫做 b 的 **倍数**. 人们常将 q 写成 a/b 或 $\dfrac{a}{b}$. 否则, 就称 b 不能整除 a, 或者 a 不能被 b 整除, 记作 $b \nmid a$.

因为整数乘法运算的可交换性, 又有 $a = b \cdot q$, 所以 q 也是 a 的因数. 此外, 在不会混淆的情况下, 乘法 $a \cdot b$ 常简记为 ab.

注

(1) 当 b 遍历整数 a 的所有因数时, $-b$ 也遍历整数 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时, $\dfrac{a}{b}$ 也遍历整数 a 的所有因数.

例 1.1.1　$30 = 15 \cdot 2 = 10 \cdot 3 = 6 \cdot 5$.

将 2, 3, 5 分别整除 30 或 30 被 2, 3, 5 分别整除, 记作 $2 \mid 30$, $3 \mid 30$, $5 \mid 30$. 这时, 2, 3, 5 都是 30 的因数, 30 是 2, 3, 5 的倍数. 同时, 也有 $15 \mid 30$, $10 \mid 30$, $6 \mid 30$.

30 的所有因数是 $\{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$,

或是 $\{\mp 1, \mp 2, \mp 3, \mp 5, \mp 6, \mp 10, \mp 15, \mp 30\}$,

或是 $\left\{ \pm 30 = \dfrac{30}{\pm 1}, \pm 15 = \dfrac{30}{\pm 2}, \pm 10 = \dfrac{30}{\pm 3}, \pm 6 = \dfrac{30}{\pm 5}, \pm 5 = \dfrac{30}{\pm 6}, \pm 3 = \dfrac{30}{\pm 10}, \right.$

$\left. \pm 2 = \dfrac{30}{\pm 15}, \pm 1 = \dfrac{30}{\pm 30} \right\}$.

列表就是:

d	± 1	± 2	± 3	± 5	± 6	± 10	± 15	± 30
$-d$	∓ 1	∓ 2	∓ 3	∓ 5	∓ 6	∓ 10	∓ 15	∓ 30
$\dfrac{n}{d}$	± 30	± 15	± 10	± 6	± 5	± 3	± 2	± 1

又例如: $7 \mid 84$, $-7 \mid 84$, $5 \mid 20$, $19 \mid 171$, $3 \nmid 8$, $5 \nmid 12$, $13 \mid 0$, $11 \mid 11$.

根据定义有:

- 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 a 是其自身的倍数, 也是其自身的因数.

例 1.1.2 设 a, b 为整数. 若 $b \mid a$, 则 $b \mid (-a)$, $(-b) \mid a$, $(-b) \mid (-a)$.

证 设 $b \mid a$, 则存在整数 q 使得 $a = q \cdot b$. 因而,

$$(-a) = (-q) \cdot b, \quad a = (-q) \cdot (-b), \quad (-a) = q \cdot (-b).$$

因为 $-q$, q 都是整数, 所以根据整除的定义有

$$b \mid (-a), \quad (-b) \mid a, \quad (-b) \mid (-a).$$

证毕.

整除具有传递性, 即

定理 1.1.1 设 a, $b \neq 0$, $c \neq 0$ 是三个整数. 若 $b \mid a$, $c \mid b$, 则 $c \mid a$.

证 设 $b \mid a$, $c \mid b$, 根据整除的定义, 分别存在整数 q_1, q_2 使得

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

因此, 有

$$a = q_1 \cdot b = q_1 \cdot (q_2 \cdot c) = q \cdot c.$$

因为 $q = q_1 \cdot q_2$ 是整数, 所以根据整除的定义, 有 $c \mid a$. 证毕.

例 1.1.3 因为 $7 \mid 42$, $42 \mid 84$, 所以 $7 \mid 84$.

在加法、减法运算中, 整除的性质是保持的.

定理 1.1.2 设 a, b, $c \neq 0$ 是三个整数. 若 $c \mid a$, $c \mid b$, 则 $c \mid a \pm b$.

证 设 $c \mid a$, $c \mid b$, 那么存在两个整数 q_1, q_2 分别使得

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

因此,

$$a \pm b = q_1 \cdot c \pm q_2 \cdot c = (q_1 \pm q_2) \cdot c.$$

因为 $q_1 \pm q_2$ 是整数, 所以 $a \pm b$ 被 c 整除. 证毕.

例 1.1.4 因为 $7 \mid 14$, $7 \mid 84$, 所以

$$7 \mid (84 + 14) = 98, \quad 7 \mid (84 - 14) = 70.$$

进一步, 在整数 a, b 的线性组合中, 整除的性质是保持的.

定理 1.1.3 设 a, b, $c \neq 0$ 是三个整数. 若 $c \mid a$, $c \mid b$, 则对任意整数 s、t, 有 $c \mid (s \cdot a + t \cdot b)$.

证 设 $c \mid a$, $c \mid b$, 那么存在两个整数 q_1, q_2 分别使得

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

因此,

$$s \cdot a + t \cdot b = s \cdot (q_1 \cdot c) + t \cdot (q_2 \cdot c) = (s \cdot q_1 + t \cdot q_2) \cdot c.$$

因为 $s \cdot q_1 + t \cdot q_2$ 是整数, 所以 $s \cdot a + t \cdot b$ 被 c 整除. 证毕.

例 1.1.5 因为 $7 \mid 14$, $7 \mid 21$, 所以

$$7 \mid (3 \cdot 21 - 4 \cdot 14) = 7, \quad 7 \mid (3 \cdot 21 + 4 \cdot 14) = 119.$$

例 1.1.6 设 a, b, $c \neq 0$ 是三个整数, $c \mid a$, $c \mid b$. 如果存在整数 s, t, 使得 $s \cdot a + t \cdot b = 1$, 则 $c = \pm 1$.

证 设 $c \mid a$, $c \mid b$, 因为存在整数 s, t, 使得 $s \cdot a + t \cdot b = 1$, 根据定理 1.1.3, 有

$$c \mid s \cdot a + t \cdot b = 1.$$

因此, $c = \pm 1$. 证毕.

定理 1.1.3 可推广为多个整数的线性组合.

定理 1.1.4 设整数 $c \neq 0$. 若整数 $a_1, \cdots, a_n$ 都是整数 c 的倍数, 则对任意 n 个整数 $s_1, \cdots, s_n$, 整数

$$s_1 a_1 + \cdots + s_n a_n$$

是 c 的倍数.

证 设 $c \mid a_i$, $1 \leqslant i \leqslant n$, 那么存在 n 个整数 q_i, $1 \leqslant i \leqslant n$ 使得

$$a_i = q_i \cdot c, \quad 1 \leqslant i \leqslant n.$$

因此,

$$s_1 a_1 + \cdots + s_n a_n = s_1 (q_1 \cdot c) + \cdots + s_n (q_n \cdot c) = (s_1 q_1 + \cdots + s_n q_n) \cdot c$$

因为 $s_1 q_1 + \cdots + s_n q_n$ 是整数, 所以 $s_1 a_1 + \cdots + s_n a_n$ 能被 c 整除. 证毕.

例 1.1.7 因为 $7 \mid 14$, $7 \mid 21$, $7 \mid 35$, 所以

$$7 \mid (5 \cdot 21 + 4 \cdot 14 - 3 \cdot 35) = 56.$$

定理 1.1.5 设 a, b 都是非零整数. 若 $a \mid b$, $b \mid a$, 则 $a = \pm b$.

证 设 $a \mid b$, $b \mid a$, 那么存在两个整数 q_1, q_2 分别使得

$$a = q_1 \cdot b, \quad b = q_2 \cdot a.$$

从而,

$$a = q_1 \cdot b = q_1 \cdot (q_2 \cdot a) = (q_1 \cdot q_2)\, a \quad \text{或} \quad (q_1 \cdot q_2 - 1)\, a = 0.$$

因为 $a \neq 0$, 根据整数乘法的性质, 有 $q_1 \cdot q_2 = 1$. 但 q_1, q_2 都是整数, 所以 $q_1 = q_2 = \pm 1$. 进而, $a = \pm b$. 证毕.

前面考虑了整除和因数, 现在考虑对于乘法的最小整数, 也就是不能继续分解的整数 (± 1 除外), 即下面的素数.

定义 1.1.2 设整数 $n \neq 0$, ± 1. 如果除了显然因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么, n 就叫做 **素数** (或**质数**或**不可约数**), 否则, n 叫做 **合数**.

当整数 $n \neq 0$, ± 1 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, 素数总是指正整数, 通常写成 p.

例 1.1.8 整数 2, 3, 5, 7 都是素数; 而整数 4, 6, 10, 15, 21 都是合数.

下面要证明每个合数必有素因子.

定理 1.1.6 设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数, 则 p 一定是素数, 且 $p \leqslant \sqrt{n}$.

证 反证法. 如果 p 不是素数, 则存在整数 q, $1 < q < p$, 使得 $q \mid p$. 但 $p \mid n$, 根据整除的传递性 (定理 1.1.1), 有 $q \mid n$. 这与 p 是 n 的最小正因数矛盾. 所以, p 是素数.

因为 n 是合数, 所以存在整数 n_1 使得

$$n = n_1 \cdot p, \quad 1 < p \leqslant n_1 < n.$$

因此, $p^2 \leqslant n$. 故 $p \leqslant \sqrt{n}$. 证毕.

注 定理 1.1.6 表明, 素数为乘法的最小单元, 并且整数可以表示成素数的乘积 (定理 1.6.1).

1.1.2 Eratoshenes 筛法

根据定理 1.1.6, 合数 n 的最小因数 p 为素数, 且 $p \leqslant \sqrt{n}$. 由此, 可立即得到一个判断整数是否为素数的法则 (只用到整数的乘法运算).

定理 1.1.7 设 n 是正整数. 如果对所有的素数 $p \leqslant \sqrt{n}$, 都有 $p \nmid n$, 则 n 一定是素数.

应用定理 1.1.7, 可得到一个寻找素数的确定性方法, 通常叫做 **平凡除法** 或 **厄拉托塞师 (Eratosthenes) 筛法**.

下面给出具体的描述.

对任意给定的正整数 N , 要求出所有不超过 N 的素数. 列出 N 个整数, 从中删除不大于 $\sqrt{N}$ 的所有素数 p_1, p_2, $\cdots$, p_k 的倍数 (除素数 p_1, p_2 $\cdots$, p_k 外). 具体地是依次删除,

$$\begin{aligned}
&p_1 \text{ 的倍数}: \quad 2 \cdot p_1, \quad 3 \cdot p_1, \quad \cdots, \quad \left[\frac{N}{p_1}\right] \cdot p_1;\\
&p_2 \text{ 的倍数}: \quad 2 \cdot p_2, \quad 3 \cdot p_2, \quad \cdots, \quad \left[\frac{N}{p_2}\right] \cdot p_2;\\
&\qquad\qquad \vdots\\
&p_k \text{ 的倍数}: \quad 2 \cdot p_k, \quad 3 \cdot p_k, \quad \cdots, \quad \left[\frac{N}{p_k}\right] \cdot p_k.
\end{aligned}$$

余下的整数 (不包括 1) 就是所要求的不超过 N 的素数 (符号 [ ] 的解释见定义 1.1.4).

例 1.1.9 求出所有不超过 $N = 100$ 的素数.

解 因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 所以依次删除 2, 3, 5, 7 的倍数,

$$\begin{array}{lllll}
2 \cdot 2, & 3 \cdot 2, & 4 \cdot 2, & \cdots, & 49 \cdot 2, \quad 50 \cdot 2\\
2 \cdot 3, & 3 \cdot 3, & 4 \cdot 3, & \cdots, & 32 \cdot 3, \quad 33 \cdot 3\\
2 \cdot 5, & 3 \cdot 5, & 4 \cdot 5, & \cdots, & 19 \cdot 5, \quad 20 \cdot 5\\
2 \cdot 7, & 3 \cdot 7, & 4 \cdot 7, & \cdots, & 13 \cdot 7, \quad 14 \cdot 7.
\end{array}$$

余下的整数 (不包括 1) 就是所要求的不超过 $N = 100$ 的素数.

将上述解答列表如下:

对于素数 $p_1 = 2$,

1	2	3	$\not 4$	5	$\not 6$	7	$\not 8$	9	$\not 10$
11	$\not 12$	13	$\not 14$	15	$\not 16$	17	$\not 18$	19	$\not 20$
21	$\not 22$	23	$\not 24$	25	$\not 26$	27	$\not 28$	29	$\not 30$
31	$\not 32$	33	$\not 34$	35	$\not 36$	37	$\not 38$	39	$\not 40$
41	$\not 42$	43	$\not 44$	45	$\not 46$	47	$\not 48$	49	$\not 50$
51	$\not 52$	53	$\not 54$	55	$\not 56$	57	$\not 58$	59	$\not 60$
61	$\not 62$	63	$\not 64$	65	$\not 66$	67	$\not 68$	69	$\not 70$
71	$\not 72$	73	$\not 74$	75	$\not 76$	77	$\not 78$	79	$\not 80$
81	$\not 82$	83	$\not 84$	85	$\not 86$	87	$\not 88$	89	$\not 90$
91	$\not 92$	93	$\not 94$	95	$\not 96$	97	$\not 98$	99	$\not 100$

对于素数 $p_2 = 3$,

1	2	3		5		7		$\not 9$	
11		13		$\not 15$		17		19	
$\not 21$		23		25		$\not 27$		29	
31		$\not 33$		35		37		$\not 39$	
41		43		$\not 45$		47		49	
$\not 51$		53		55		$\not 57$		59	
61		$\not 63$		65		67		$\not 69$	
71		73		$\not 75$		77		79	
$\not 81$		83		85		$\not 87$		89	
91		$\not 93$		95		97		$\not 99$	

对于素数 $p_3 = 5$,

1	2	3		5		7			
11		13				17		19	
		23		$\not 25$				29	
31				$\not 35$		37			
41		43				47		49	
		53		$\not 55$				59	
61				$\not 65$		67			
71		73				77		79	
		83		$\not 85$				89	
91				$\not 95$		97			

对于素数 $p_4 = 7$,

1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		$\not 49$	
		53						59	
61						67			
71		73				$\not 77$		79	
		83						89	
$\not 91$						97			

余下的整数 (不包括 1) 就是所要求的不超过 $N = 100$ 的素数.

$\not 1$	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			

即 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.