普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

信息安全数学基础
——算法、应用与实践

任 伟 编著

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

信息安全数学基础
——算法、应用与实践

任 伟 编著

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书包括初等数论、抽象代数、椭圆曲线论等方面的内容。本书选材合理、难度适中、层次分明、内容系统。书中以大量例题深入浅出地阐述信息安全数学基础各分支的基本概念、基本理论与基本方法，注重将抽象的理论与算法和实践相结合，并强调理论在信息安全特别是密码学中的具体应用实例。本书语言通俗易懂，容易自学。

本书可作为高等院校信息安全、计算机科学与技术、密码学、通信工程、信息对抗、电子工程等领域的研究生和本科生相关课程的教科书，也可作为这些领域的教学、科研和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：算法、应用与实践/任伟编著. —北京：清华大学出版社，2016
高等院校信息安全专业系列教材
ISBN 978-7-302-41637-1

Ⅰ. ①信… Ⅱ. ①任… Ⅲ. ①信息安全—应用数学—高等学校—教材 Ⅳ. ①TP309 ②029

中国版本图书馆 CIP 数据核字(2015)第 228404 号

责任编辑：张　民　李　晔
封面设计：何凤霞
责任校对：梁　毅
责任印制：宋　林

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 装 者：三河市中晟雅豪印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：8.75　　**字　数**：214 千字
版　　次：2016 年 1 月第 1 版　　**印　次**：2016 年 1 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：046936-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

随着中央网络安全与信息化领导小组的成立，信息安全进入公众的视野，它不仅关系到国防军事等重大战略问题以及国计民生等新兴战略产业的发展，而且与每个人的日常生活息息相关。目前，我国信息安全所面临的形势十分严峻，信息安全学科的发展已经刻不容缓，信息安全学科升级为国家一级学科也已经提上议事日程。

信息安全数学是信息安全学科的理论基础，其内容涉及面较广，例如数论与有限域等在信息安全的重要基础课如密码学中有大量的应用。信息安全数学基础是信息安全专业一门重要的基础必修课程。此外，信息安全数学在计算机科学、信息与通信工程、网络工程、电子对抗等学科中也都有着重要的应用。

目前信息安全数学方面的书籍有些难以读懂，这在一定程度上阻碍了信息安全学科以及信息安全知识的普及。对抽象的数学知识介绍较多，虽然一定程度上可以锻炼学生的抽象思维能力，但容易造成学生对所学内容的畏难情绪。另外，单纯的理论知识介绍会导致学生不清楚这些理论如何应用，从而对所学内容不能留下较深刻的印象。一些来自计算机科学、通信工程、网络工程等专业的学生虽然对信息安全方向感兴趣，但是因为信息安全数学知识的抽象和难以普及导致无法将本专业与信息安全方向结合起来。

本书重点强调信息安全数学基础在信息安全中的应用，并通过实践（算法与编程）环节强化对理论的理解。减少了一些在信息安全中应用较少的非重点数学理论，注重从计算机科学（算法）角度介绍而不是从纯数学角度介绍。强调抽象知识的算法解释和形象化，便于读者自学和易于教学。

本书在写作过程中特别遵循了以下思路。

（1）体例新颖活泼、语言通俗易懂、精心安排示例。注意到目前市场上“大话×××”、“×××趣谈”、“图解×××”等图书深受读者喜爱，本书在保证论述的严谨性前提下，语言尽量形象生动、文风尽量活泼，以激发学习者的兴趣。根据作者对“信息安全数学基础”这一课程多年的教学实践经验，给出一些较为独特的比喻，虽然有些比较浅显，但主要目的是让读者特别是初学者快速理解，印象深刻，阅读轻松。

（2）内容编排独特、循序渐进、由浅入深。注重内容之间的联系和讲解先后次序。内容选取尽量考虑到重要性和必要性。注重给出一些浅显易懂的类比，便于读者建立所学知识与前后内容之间的联系。

(3) 以应用为导向，理论联系实际。不单纯讲解数学基础，而是从应用需要的角度出发，着重讲解基础知识点和关键点，突出实用性和可操作性。注重对算法和实践能力的培养，书中重点介绍计算数论(算法数论)中的算法，鼓励读者自主实现这些算法来提高实践能力。

(4) 注重启发性和对创新能力的培养。通过在正文中设立“思考”环节，以提高启发性并激发读者思考。在内容组织中潜移默化地强调数学素养的培养，根据数学内容的需要，采用合情归纳法、演绎法、公理集合论方法等多种论述方法。

全书共分 12 章：第 1 章整除；第 2 章同余；第 3 章同余式；第 4 章二次同余式和平方剩余；第 5 章原根与指数；第 6 章群；第 7 章环与域；第 8 章素性检测；第 9 章椭圆曲线群；第 10 章大整数分解算法；第 11 章离散对数算法；第 12 章其他高级应用。其中，第 9～12 章为高级部分，高级部分与部分打星号的章节可选学。全书授课学时为 40～64 学时。

本书面向的主要对象包括从事信息和网络安全研究的科研人员，学习信息安全相关课程的高等院校信息安全类、计算机科学类、信息与计算科学类专业本科生，以及从事信息安全技术研发、应用和管理的工程技术人员。

本书受到了国家自然科学基金面上项目(No. 61170217)，以及湖北省教育厅高等学校教学研究项目(No. 2015A06)的支持，在此表示感谢。感谢研究生叶敏、刘宇靓、林佳华、曹强、曾玲玲的辅助性工作。

愿本书的写作能为我国信息安全数学的教学和普及起到一点抛砖引玉的作用。由于作者水平和学识有限，不足之处在所难免，在此衷心恳请广大读者、同行批评指正。联系方式是 weirencs@cug. edu. cn。

作　者

目 录

基 础 篇

高 级 篇

基　础　篇

第1章 整 除

在整数集合中，整除是一种重要的二元关系，相关概念和性质包括素数、公因数、欧几里得除法(辗转相除法，Euclid 除法)、算术基本定理等。这些概念和性质又是整数集合中另一种重要的二元关系——同余关系的基础。本章先介绍整除，第 2 章介绍同余。

本章的重点是 Euclid 除法和 Euclid 算法，难点是扩展的 Euclid 算法。

1.1 整除的概念

通常，用 Z 表示整数集合，整数即为 $0,\pm1,\pm2,\cdots$。

自然数是非负整数，用 N 来表示。

定义 1.1(整除) 设 a,b 是任意两个整数，其中 $b\neq0$。如果存在一个整数 q，使得等式

$$a = qb$$

成立，则称 b 整除 a 或者 a 被 b 整除，记作 $b|a$。b 叫做 a 的因数，a 叫做 b 的倍数。q 写成 a/b 或者 $\frac{a}{b}$。否则，称 b 不能整除 a，或者 a 不能被 b 整除，记作 $b\nmid a$。

注意，这里整除的定义通过乘法运算给出的(而不是通过除法运算定义的)；通过整数 q 的存在性表述整除性。另外，符号 $b|a$ 本身就包含了 $b\neq0$。

例 1.1 请写出 20 的所有因数。

解答：$\pm1,\pm2,\pm4,\pm5,\pm10,\pm20$。

根据定义，有：

0 是任何非零整数的倍数，即 $a|0$，这里 $a\neq0,a\in Z$；

1 是任何整数的因数，即 $1|a,a\in Z$；

任何非零整数 a 是自己的倍数，也是自己的因数，即 $a|a$，这里 $a\neq0,a\in Z$。

整除有如下性质：

例 1.2 设 a,b 为整数。若 $b|a$，则 $b|(-a),(-b)|a,(-b)|(-a),|b||a|$。

证明：由 $b|a$，于是存在整数 q，使得 $a=qb$。

要证明所需结论，即需要证明存在整数 Q，使得等式 $(-a)=Qb,a=Q(-b),(-a)=Q(-b),|a|=Q|b|$ 成立。

由条件 $a=qb$ 通过简单的推理可以发现，当 Q 分别为 $-q,-q,q,|q|$ 时，上述等式满足。于是可知，相应的整数 Q 存在。 ■

由这个例子可知，可将重点放在正整数的整除上来。

上述证明的思路在于：从已知条件和证明目标同时入手，变换转换，中间相遇。具体而言，由整除的概念得到相应等式，由相应等式推出整数 Q 的存在性，由整数 Q 的存在性推出整除性。

由这一思路，可以证明整除的如下性质(请读者自行给出证明并给出实例)：

定理 1.1(传递性) 设 $a\neq 0, b\neq 0, c$ 是三个整数。若 $a|b, b|c$，则 $a|c$。

定理 1.2 设 $a, b, c\neq 0$ 是三个整数。若 $c|a, c|b$，则 $c|a\pm b$。

定理 1.3 设 $a, b, c\neq 0$ 是三个整数。若 $c|a, c|b$，则对任意整数 s, t，有

$$c|sa\pm tb$$

(提示：Q 分别为 $q_1q_2, q_1\pm q_2, sq_1\pm tq_2$)

例 1.3 设 $a, b, c\neq 0$ 是三个整数，对于 $c|a, c|b$，如果存在整数 s, t，使得 $sa+tb=1$，则 $c=\pm 1$。

证明：因为 $c|a, c|b$，存在整数 s, t，使得 $sa+tb=1$，于是由定理 1.3，有 $c|sa+tb=1$，于是，$c=\pm 1$。 ■

由整除和因数的概念，可以根据因数情况对整数进行分类。

定义 1.2 设整数 $n\neq 0, \pm 1$，如果除了平凡因数 $\pm 1, \pm n$ 外，n 没有其他因数，那么 n 叫做**素数**(或**质数**、**不可约数**)，否则 n 叫做**合数**。

当整数 $n\neq 0, \pm 1$ 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。

思考 1.1：请写出 30 以内的素数。

(答案：2,3,5,7,11,13,17,19,23,29)

下面证明每个合数必有素因数。

定理 1.4 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 $p\leqslant\sqrt{n}$。

证明：反证法。若 p 不是素数，则存在整数 $q, 1<q<p$，使得 $q|p$，由条件知 $p|n$，于是根据定理 1.1，有 $q|n$，这与 p 是 n 的大于 1 的最小正因数矛盾。所以 p 是素数。

若 $p>\sqrt{n}$ 成立，则 n 的另一个因数 $n/p<n/\sqrt{n}=\sqrt{n}$，于是，n/p 是一个比 p 小的因数，这与 p 是 n 的大于 1 的最小正因数矛盾。证毕。 ■

非正式地说，上述定理说明了两点：素因数可以视为合数的“组成成分”。且这一“组成成分”中必然有一个小于等于 $\sqrt{n}$。

定理 1.4 给出了寻找素数的有效方法。为了求出不超过给定正整数 $x(x>1)$ 的所有素数，只要把从 2 到 x 的所有合数都删去即可。因为不超过 x 的合数 n 必有一个素因子 $p\leqslant\sqrt{n}\leqslant\sqrt{x}$，所以只要先求出 $\sqrt{x}$ 以内的全部素数 $\{p_i, 1\leqslant i\leqslant k\}$(其中，$k$ 为 $\sqrt{x}$ 以内的素数个数)，然后把不超过 x 的 p_i 的倍数(p_i 本身除外)全部删去，剩下的就正好是不超过 x 的全部素数。这种寻找素数的方法称为 Eratosthenes 筛法。

例 1.4 求出不超过 64 的所有素数。

解答：先求出不超过 $\sqrt{64}=8$ 的所有素数，依次为 2,3,5,7，然后从 2～64 的所有整

数依次删去除了 2、3、5、7 以外的 2 的倍数、3 的倍数、5 的倍数、7 的倍数，剩下的即为所求。具体过程如下所示：

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	
~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~			
~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~			
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	㊾	~~50~~	51			
~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~		

可见，没有删去的数是：2、3、5、7、11、13、17、19、23、29、31、37、41、43、47、51、53、59、61。这些即为不超过 64 的所有素数。

依据上述方法可以编写一个算法，输出不超过输入值的所有素数。

一个很自然会想到的问题就是：素数是否可以穷举？下面的证明说明素数的数量有无穷多个。

定理 1.5　素数有无穷多个。

证明：反证法。假设有有限个素数，则不妨设它们为 $p_1, p_2, \cdots, p_n$。考虑大于 1 的整数

$$N = p_1 p_2 \cdots p_n + 1$$

容易看到：$p_1, p_2, \cdots, p_n$ 都不能整除 N，于是 N 没有素因数，由定理 1.4 知，N 不是合数，于是 N 为素数。这与有限个素数矛盾。 ■

公元前 3 世纪古希腊大数学家欧几里得(Euclid)在 *The Elements*(中文译名为《几何原本》)一书中给出了该证明方法，成了一种经典的“构造矛盾”的反证法。①

可以看到，本节论述的过程遵循了数学公理化方法，该方法从基本概念和公理出发，通过证明逐步扩充定理和性质。

1.2　Euclid 算法

前面讨论的是整除的情况，如果不能整除时会如何呢？

定理 1.6(Euclid 除法，也称为带余除法)　设 a, b 是两个整数，其中 $b>0$，则存在唯一的整数 q, r 使得

$$a = qb + r, \quad 0 \leqslant r < b \tag{1.1}$$

证明：先证明存在性。考虑一个整数序列

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

它们将实数轴分成长度为 b 的一系列区间，而 a 必定落在其中的一个区间上。因此存在一个整数 q，使得

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

① 该命题为《几何原本》第 9 卷第 20 个命题，编号为 IX. 20，原命题是：预先给定几个质数，那么有比它们更多的质数。该证明被《来自天书的证明》一书收录为数学史上的经典证明。(类似的方法包括 Cantor 的对角线反证法，Turing 的停机问题的不可判定性，以及 Godel 的不完备性定理。)欧几里得的《几何原本》是西方数学公理化方法的起源和数学逻辑演绎推导的代表。《九章算术》为代表的中国数学则是以归纳计算和构造为主要方法。

令 $r=a-qb$，则有

$$a = qb+r, 0\leqslant r<b$$

再证明唯一性。如果分别有 q_1, r_1 和 q_2, r_2 满足(1.1)式，则

$$a = q_1 b+ r_1, \quad 0\leqslant r_1<b$$

$$a = q_2 b+ r_2, \quad 0\leqslant r_2<b$$

两式相减，有

$$(q_1-q_2)b=-(r_1-r_2)$$

当 $q_1\neq q_2$ 时，左边的绝对值$\geqslant b$，而右边的绝对值$<b$，这是不可能的。于是，$q_1=q_2$，$r_1=r_2$。证毕。 ■

定义 1.3 (1.1)式中的 q 叫做 a 被 b 除所得的不完全商，r 叫做 a 被 b 除所得的余数。

Euclid 除法可以理解成用一个长度为 b 的“尺子”去度量长度 a，度量最后剩下的一段 r 不会大于“尺子”的长度 b。

Euclid 除法的用途是可以将两个数之间整除关系的判定问题转化为计算问题。判断 a 是否能被非零整数 b 整除的充要条件是 a 被 b 除所得的余数 $r=0$。

通常，$0\leqslant r<b$，这时 r 叫做最小非负余数；但在有些时候通过“平移”(即调整不完全商的大小，一般是加 1)，可以将 r 调整为 $|r|\leqslant b/2$，这时 r 叫做绝对值最小余数，它在后面介绍的 Euclid 算法中(见例 1.8)能起到算法加速的作用。

思考 1.2 令 $b=7$，则最小非负余数为多少？绝对值最小余数为多少？

解答：$r=0,1,2,3,4,5,6$ 为最小非负余数；

$r=-3,-2,-1,0,1,2,3$ 为绝对值最小余数。

定义 1.4(公因子) 设 $a_1,\cdots,a_n$ 是 $n(n\geqslant 2)$ 个整数。若整数 d 是它们中每一个数的因数，那么 d 就叫做 $a_1,\cdots,a_n$ 的一个公约数(也叫公因数)。

d 是 $a_1,\cdots,a_n$ 的一个公因数的数学表达式为：

$$d|a_1,\cdots,d|a_n$$

如果整数 $a_1,\cdots,a_n$ 不全为零，那么 $a_1,\cdots,a_n$ 的所有公约数中最大的一个公约数叫做最大公约数(Greatest Common Divisor)，记作 $\gcd(a_1,\cdots,a_n)$ 或 $(a_1,\cdots,a_n)$。

特别地，当 $(a_1,\cdots,a_n)=1$，称 $(a_1,\cdots,a_n)$ 互素或互质。

最大公约数的等价定义为：

$d>0$ 是 $a_1,\cdots,a_n$ 的最大公约数的数学表达式可以表述为：

(1) $d|a_1,\cdots,d|a_n$。

(2) 若 $e|a_1,\cdots,e|a_n$，则 $e|d$。

条件(1)说明 d 是公约数；条件(2)说明 d 在公约数中最大。

下面的定理给出了最大公约数的另一个等价定义：

定理 1.7 a,b 是不全为零的整数，a,b 的最大公约数 $d=(a,b)$ 是集合

$$\{sa+tb \mid s, t\in Z\}$$

中的最小正整数。

证明：令集合 $\{sa+tb|s,t\in Z\}$ 中最小的正整数为 m。下面证明 $m=d$，方法是先证明