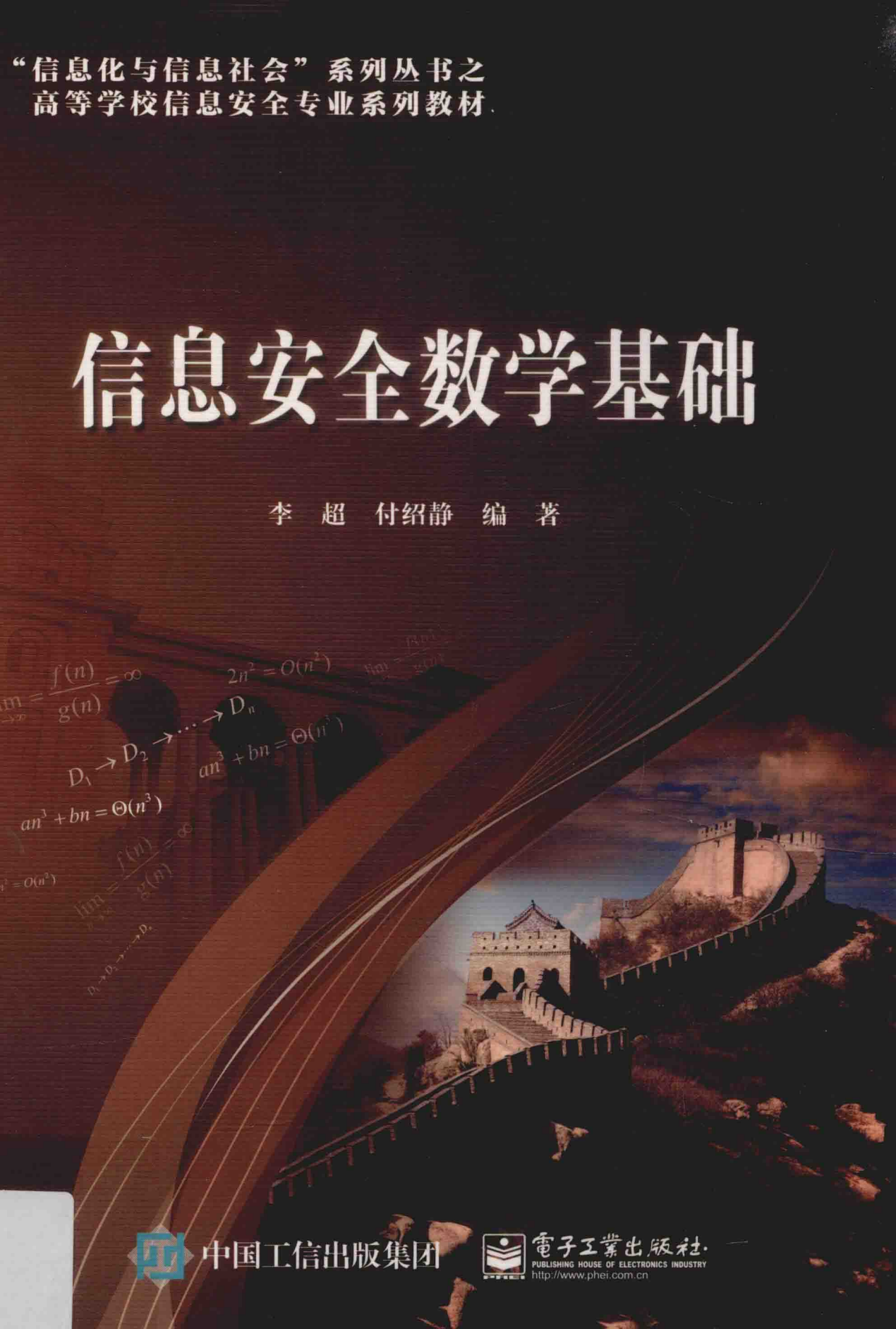
“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全数学基础

李 超 付绍静 编 著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全数学基础

李　超　付绍静　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书系统地介绍了数论、代数、组合、信息论和计算复杂性等数学理论与方法，突出数论、代数、组合、信息论和计算复杂性的一体化融合，前后内容相互呼应，相互支撑。在知识结构的应用性方面，突出教材内容在信息安全领域中的应用。数论部分给出了代换密码、RSA 算法、Diffie-Hellman 协议的数学原理刻画；代数部分给出了 AES 算法、EIGmal 算法、Schnorr 算法和 DSS 算法的数学原理刻画；组合部分给出了 Hash 函数和 Bent 函数的设计与分析方面所涉及的组合知识；信息论部分给出了完善保密性的信息论刻画；计算复杂性部分给出了基于计算安全的密码方案分析原理的刻画。本书可作为信息安全领域相关专业本科生和研究生的教材，也可供从事信息安全和其他信息技术工作的科研和工程技术人员参考。

图书在版编目(CIP)数据

信息安全数学基础 / 李超，付绍静编著. —北京：电子工业出版社，2015.11
(信息化与信息社会系列丛书)
高等学校信息安全专业系列教材
ISBN 978-7-121-27505-0

Ⅰ. ①信… Ⅱ. ①李… ②付… Ⅲ. ①信息安全－应用数学－高等学校－教材 Ⅳ. ①TP309②O29

中国版本图书馆 CIP 数据核字(2015)第 263670 号

策划编辑：章海涛　刘宪兰
责任编辑：章海涛　　特约编辑：刘宪兰　李　虹
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：14.75　字数：314 千字
版　　次：2015 年 11 月第 1 版
印　　次：2015 年 11 月第 1 次印刷
定　　价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

编委会名单 EDITORIAL COMMITTEE LIST

“信息化与信息社会”系列丛书编委会名单

编 委 会 主 任 曲维枝

编委会副主任 周宏仁　张尧学　徐　愈

编 委 会 委 员 何德全　邬贺铨　高新民　高世辑　张复良　刘希俭
刘小英　李国杰　秦　海　赵泽良　杜　链　朱森第
方欣欣　陈国青　李一军　李　琪　冯登国

编委会秘书处 廖　瑾　刘宪兰　刘　博　等

高等学校信息安全专业系列教材编委会名单

专业编委会顾问 （以汉字拼音为序）
蔡吉人　方滨兴　何德全　刘小英　宁家骏　曲成义
沈昌祥　邬贺铨　熊澄宇　赵泽良

专业编委会主任 冯登国

专业编委会委员 （以汉字拼音为序）
陈克非　封化民　韩　臻　胡爱群　黄继武　黄刘生
李　超　李建华　刘建伟　陆哲明　马建峰　秦玉海
秦志光　石文昌　王怀民　王清贤　王小云　向　宏
谢冬青　杨义先　俞能海　曾庆凯　张宏莉　张焕国
郑　东

作者简介

李超 博士，国防科技大学教授、理学院应用数学专业和计算机学院密码学专业的博士生导师，担任中国密码学会理事、湖南省数学会常务理事、湖南省计算数学与应用软件学会理事。在《IEEE Transactions on Information Theory》和《Science in China》等国内外学术刊物上合作发表（录用）论文 60 余篇，在 CRYPT、FSE 和 SAC 等国际会议上合作发表论文 20 余篇，其中被 SCI 检索 40 余篇、被 EI 检索 50 余篇，获得 2010 年澳洲密码年会最佳论文奖、2010 年中国密码年会最佳论文奖和 2014 年中国密码年会最佳论文奖。在 Springer 出版社、高等教育出版社和科学出版社等出版社合作出版会议录 2 部、专著 2 部、教材 6 部。主持国家自然科学基金和国家密码发展基金等 10 余项科研任务，获军队科技进步一等奖 1 项，部委级科技进步二等奖 1 项、三等奖 2 项，国家教育部霍英东优秀青年教师奖 1 项，军队院校育才奖金奖和银奖各 1 项。

付绍静 博士，国防科技大学计算机学院副教授，日本 IEICE 学会会员，中国计算机学会会员，中国密码学会会员。在《Designs, Codes and Cryptography》《Information Science》和《中国科学》等国内外学术期刊和学术会议上发表论文 30 余篇，其中作为第一作者发表 SCI 收录论文 12 篇，主持国家自然科学基金和信息安全国家重点实验室开放课题等 8 项科研任务。作为技术骨干参与了国家自然科学基金、国家 863 项目、973 项目等多项科研任务。担任《IEEE Transactions on Information Theory》《Information Science》《Information Processing Letters》和《IEICE Transactions on Fundamentals》等国际期刊的审稿人，是 ICISC 2012（韩国）、WISA2012（韩国）、ICISC 2013（韩国）等 10 多个著名国际会议的程序委员会委员。申请国家发明专利 2 项。获军队院校育才奖银奖 1 项。

总　序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，中国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会按照党中央、国务院领导同志的要求，就中国信息化发展中的前瞻性、全局性和战略性的问题进行了调查研究，提出了政策建议和咨询意见。信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力。大量培养符合中国信息化发展需要的人才是国家信息化发展的一个紧迫需求，也是中国推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006 年 5 月，中国公布《2006—2020 年国家信息化发展战略》，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会致力于通过讲座、论坛、出版等各种方式推动信息化知识的宣传、教育和培训工作。2007 年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的，是力图结合中国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实中国信息化实践中的成功案例，进一步完善中国信息化教学的框架体系，提高中国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强中国信息化人才队伍的建设具有重要意义。

考虑到当时国家信息化人才培养的需求，各个专业和不同教育层次（博士生、硕士生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社

会”系列丛书编委会采取了集中全国优秀学者和教师，分期分批出版高质量的信息化教育丛书的方式，结合高校专业课程设置情况，在“十一五”期间，先后组织出版了“信息管理与信息系统”、“电子商务”、“信息安全”三套本科专业高等学校系列教材，受到高校相关专业学科以及相关专业师生的热烈欢迎，并得到业内专家和教师的一致好评和高度评价。

但是，随着时间的推移和信息技术的快速发展，上述专业的教育面临着持续更新、不断完善的迫切要求，日新月异的技术发展及应用变迁也不断对新时期的建设和人才培养提出新要求。为此，“信息管理与信息系统”、“电子商务”、“信息安全”三个专业教育需以综合的视角和发展的眼光不断对自身进行调整和丰富，已出版的教材内容也需及时进行更新和调整，以满足需求。

这次，高等学校“信息管理与信息系统”、“电子商务”、“信息安全”三套系列教材的修订是在涵盖第 1 版主题内容的基础上进行的更新和调整。我们希望在内容构成上，既要保持原第 1 版教材基础的经典内容，又要介绍主流的知识、方法和工具，以及最新的发展趋势，同时增加部分案例、实例或新的课程教材，使每一本教材都有明确的定位，分别体现“信息管理与信息系统”、“电子商务”、“信息安全”三个专业领域的特征，并在结合中国信息化发展实际特点的同时，选择性地吸收国际上相关教材的成熟内容。

对于这次三套系列教材（以下简称系列教材）的修订，我们仍提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争修订教材达到我们一贯秉承的精品要求，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；最后，要求各专业编委会对教材大纲、内容等进行严格的审核。

我们衷心期望，系列教材的修订能对中国信息化相应专业领域的教育发展和教学水

平的提高有所裨益，对推动中国信息化的人才培养有所贡献。同时，我们也借系列教材修订出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、教师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，有待继续尝试和不断总结经验，也难免会出现这样那样的缺点和问题。我们衷心希望使用该系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

2013 年 11 月 1 日

序　言

“十一五”期间，由国家信息化专家咨询委员会牵头，教育部信息安全专业类教学指导委员会有关领导、学者组织，众多信息安全专业著名专家和教师参与开发，并由电子工业出版社出版的“高等学校信息安全专业系列教材”，由于在体系设计上较全面地覆盖了新时期信息安全专业教育的各个知识层面，包括宏观视角上对信息化大环境下信息安全相关知识的综合介绍，对信息安全应用发展前沿的深入剖析，以及对信息安全系统建设各项核心任务的系统讲解和对一些重要信息安全应用形式的讨论，在“高等学校信息安全专业系列教材”面世后，受到高校该专业学科及相关专业师生的热烈欢迎，得到业内专家和教师的好评和高度评价，被誉为该学科专业教材中的精品系列教材。

但是，随着信息技术的快速发展，信息安全专业教育面临着持续更新、不断完善的迫切要求，其日新月异的技术发展及应用变迁也不断对新时期信息安全建设和人才培养提出新的要求。为此，信息安全专业教育需以综合的视角和发展的眼光不断对教学内容进行调整和丰富，已出版的教材内容也需及时进行更新、修改和补充，以满足需求。

这次修订，除对“高等学校信息安全专业系列教材”第 1 版各册教材的主题内容进行了相应更新和调整外，同时对系列教材的总体架构进行了调整并增加了 3 个分册，即《信息安全数学基础》、《信息安全实验教程》和《信息隐藏概论》。

调整后的教材在体系架构和内容构成上既保持了基础的经典内容，又介绍了主流的知识、方法和工具，以及最新发展趋势，同时增加了部分案例或实例。使得系列中的每一本教材都有明确的定位，充分体现了国家“信息安全”的领域特征，在结合中国信息安全实际特点的同时，还注重借鉴国际上相关教材中适于作为信息安全本科教育知识的成熟内容。

我们希望这套修订教材能够成为新形势下高等学校信息安全专业的精品教材，成为高等学校信息安全专业学生循序渐进了解和掌握专业知识不可或缺的教科书和知识读本，成为国家信息安全新环境下从业人员及管理者学习信息安全知识的有益参考书。

高等学校信息安全专业系列教材编委会

2013 年 10 月于北京

前　言

随着信息技术的不断发展，信息安全的内涵也在不断地延伸。从最初的信息保密性发展到信息的保密性、完整性、可用性和不可否认性，进而发展到网络攻防、安全控制、安全测评和安全管理等多方面的理论与技术。

近半个世纪以来，信息安全有了很大的发展，数学研究对信息安全的发展起了巨大的推动作用。20 世纪 70 年代公开密钥密码体制的提出，是信息安全领域的一场革命。目前采用的两种主要的公开密钥密码体制（RSA 密码体制和椭圆曲线密码体制）均源于数论（大整数分解理论和椭圆曲线算术理论）。21 世纪初美国公布的高级加密标准（AES 算法）是当前信息安全领域的研究热点，该算法的设计采用了有限域上基本代数运算。近年来，人们对于数字签名、身份认证、密钥共享和多方安全计算等问题，均采用了数论工具（指数和估计）和组合工具（组合设计和 Matroid 理论）。与此同时，信息领域为数学提出了大量的数学问题，也促进了数学的发展，增强了数学研究的活力。

本书主要介绍从事信息安全研究所需要的基本数学知识，包括数论、代数、组合、信息论和计算复杂性等数学理论与方法。与其他同类型的教材相比，本书更加关注知识结构的合理性，更加关注知识结构的系统性，更加关注知识结构的应用性。在知识结构的合理性方面，按照由浅入深、由易入难的理念组织教材内容，编写过程中力求做到叙述自然流畅，文字生动活泼，例题充实新颖；在知识结构的系统性方面，突出数论、代数、组合、信息论和计算复杂性的一体化融合，前后内容相互呼应，相互支撑。在知识结构的应用性方面，突出教材内容在信息安全领域中的应用。数论部分给出了代换密码、RSA 算法、Diffie－Hellman 协议的数学原理刻画；代数部分给出了 AES 算法、EIGmal 算法、Schnorr 算法和 DSS 算法的数学原理刻画；组合部分给出了 Hash 函数和 Bent 函数的设计与分析方面所涉及的组合知识；信息论部分给出了完善保密性的信息论刻画；计算复杂性部分给出了基于计算安全的密码方案分析原理的刻画。

本书是作者长期从事信息安全教学和科研基础上完成的。其研究工作先后得到国家自然科学基金项目（61070215、61103191 和 61103192）、国家 863 项目（2011AA7114065

和2012AA7114065)、国家973项目（2013CB338002和613203032012）的资助。书中前三章由李超编写，后两章由付绍静编写，全书由李超负责统稿。本教材内容已经在国防科学技术大学计算机学院信息安全本科专业进行了多次教学实践。

由于作者水平所限，书中难免会有不妥和错误之处，恳请读者批评指正。

作者

2014年6月于长沙

目　录

第1章

数论基础

数论研究整数环中整数最基本性质，整除理论、同余理论和不定方程求解构成数论的基本内容。随着信息技术的飞速发展，数论所涉及的知识在信息领域特别是信息安全领域具有广泛的应用，公钥密码标准 RSA 算法是基于大整数分解困难性而设计的，通信系统中广泛使用的 Diffie-Hellmen 协议与整数的同余和原根密切相关。掌握数论的基本知识，对于从事信息安全理论与应用研究具有重要作用。

1.1 整数的整除

全体整数的集合通常用 $\mathbb{Z}$ 来表示，即

$$\mathbb{Z}=\{0,\pm1,\pm2,\pm3,\cdots\}$$

在整数集合 $\mathbb{Z}$ 中，两个整数可以进行加、减、乘三种运算，并且运算后的结果仍为整数。但两个整数进行除法运算后所得的结果未必为整数，比如 4 除以 2 所得结果为 2，它是一个整数，而 4 除以 3 所得结果为 $\frac{4}{3}$，它不是整数。

定义 1.1 设 a,b 是任意两个整数，$b\neq0$，如果存在整数 c，使得 $a=bc$，则称 b 整除 a，记做 $b\mid a$，否则称 b 不整除 a，记做 $b\nmid a$。

如果有 $b\mid a$，称 b 为 a 的因数，a 为 b 的倍数。显然 ±1 是任何整数的因数，所有的非零整数均为 0 的因数。由整除的定义，易知如下性质成立：

(1) 如果 $c\mid b$，$b\mid a$，则 $c\mid a$；

(2) 如果 $c\mid b$，$c\mid a$，则对任意 $m,n\in\mathbb{Z}$，均有 $c\mid(ma+nb)$；

(3) 如果 $b\mid a$，且 $a\neq0$，则 $|b|\leqslant|a|$；

(4) 如果 $a\mid b$，$b\mid a$，则 $|a|=|b|$，即 $a=\pm b$。

例 1.1 证明：对任意正整数 n，均有 $6\mid n(n+1)(2n+1)$。

证明 当 $n=1$ 时，$n(n+1)(2n+1)=1\times2\times3=6$，它是 6 的倍数，结论成立。

假设当 $n=k$ 时，结论成立，即

$$6\mid k(k+1)(2k+1)$$

则当 $n=k+1$ 时，有

$$n(n+1)(2n+1)=(k+1)(k+2)(2k+3)=k(k+1)(2k+1)+6(k+1)^2$$

由归纳假设，$6\mid k(k+1)(2k+1)$，并且 $6\mid 6(k+1)^2$，从而根据整除的性质(3)，得到

$$6\mid(k+1)(k+2)(2k+3)$$

由归纳法原理，$6\mid n(n+1)(2n+1)$ 对任意正整数 n 成立。 □

例 1.2 如果 $m,n,r,q\in\mathbb{Z}$，并且 $(m-p)\mid(mn+pq)$，证明 $(m-p)\mid(mq+np)$。

证明 由于

$$mq+np=mq-pq+pq+mn-mn+np=q(m-p)+(mn+pq)-n(m-p)$$

上式右边三项都是 $m-p$ 的倍数，从而有

$$(m-p) \mid (mq+np)$$ □

定理 1.1(带余除法)　设 $a,b \in \mathbb{Z}$，$b \neq 0$，则存在唯一的 q，$r \in \mathbb{Z}$，使得 $a = bq + r$，这里 $0 \leqslant r < |b|$。

证明　不妨设 $b > 0$。当 $b < 0$ 时，类似可证。

考虑如下整数序列

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

则对任意 $a \in \mathbb{Z}$，必存在 $q \in \mathbb{Z}$，使得

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

令 $r = a - qb$，则 $0 \leqslant r < b$，并且 $a = r + qb$，存在性得以证明。

下面讨论 q 和 r 的唯一性。

如果 $a = q_1 b + r_1 = q_2 b + r_2$，这里 $0 \leqslant r_1$，$r_2 < b$，则

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

若 $q_1 \neq q_2$，则 $|r_2 - r_1| \geqslant b$，这与 $0 \leqslant r_1$，$r_2 < b$ 矛盾！故 $q_1 = q_2$，从而 $r_1 = r_2$，唯一性得以证明。 □

定义 1.2　设 $a,b \in \mathbb{Z}$，$b \neq 0$，如果 $a = bq + r$，这里 $0 \leqslant r < |b|$，则称 q 为 b 除 a 所得商，r 为 b 除 a 所得的余数。

利用带余除法容易判定两个整数的整除关系，即定理 1.2。

定理 1.2　设 $a,b \in \mathbb{Z}$，$b \neq 0$，则 $b \mid a$ 当且仅当 b 除 a 所得余数为 0。

例 1.3　从 176～545 的所有整数中，13 的倍数有多少个？

解　对实数 x 而言，记 $[x]$ 为小于或等于 x 的最大整数。由带余除法，从 1～176 的所有整数中，13 的倍数有 $\left[\frac{176}{13}\right] = 13$ 个，从 1～545 的所有整数中，13 的倍数有 $\left[\frac{545}{13}\right] = 41$ 个，从而从 176～545 的所有整数中，13 的倍数有 41－13＝28 个。 □

定义 1.3　设 $d, a_1, a_2, \cdots, a_n \in \mathbb{Z}$，并且 $a_1, a_2, \cdots, a_n$ 不全为 0，如果对每个 a_i，均有 $d \mid a_i$，则称 d 为 $a_1, a_2, \cdots, a_n$ 的一个公因数。整数 $a_1, a_2, \cdots, a_n$ 的所有公因数中最大的正因数称为 $a_1, a_2, \cdots, a_n$ 的最大公因数，记为 $(a_1, a_2, \cdots, a_n)$。

对于任意一组不全为零的整数 $a_1, a_2, \cdots, a_n$，由于不为零整数的因数只有有限个。从而 $a_1, a_2, \cdots, a_n$ 的公因数也只有有限个，故其最大公因数一定存在。如何计算最大公因数 $(a_1, a_2, \cdots, a_n)$，这是整除理论中一个基本问题。下面介绍求最大公因数的辗转相除法。

定理 1.3 设 $a,b,c \in \mathbb{Z}$，并且 $b \neq 0$，如果

$$a = bq + c$$

则 $(a,b) = (b,c)$。

证明 设 $(a,b) = d_1$，$(b,c) = d_2$。由于 $(a,b) = d_1$，则 $d_1 \mid a$，$d_1 \mid b$，又 $c = a - bq$，故 $d_1 \mid c$，从而 d_1 为 b 和 c 的一个公因子，于是 $d_1 \leqslant d_2$。同理可证 $d_2 \leqslant d_1$，故 $(a,b) = (b,c)$。 □

由定理 1.3，可以求两个不全为 0 的整数的最大公因数。

设 $a,b \in \mathbb{Z}$，并且 a,b 不全为 0，不妨设 $b \neq 0$。由带余除法，必存在正整数 n，满足

$$\begin{aligned}
a &= bq_1 + r_1 && 0 \leqslant r_1 < |b| \\
b &= r_1 q_2 + r_2 && 0 \leqslant r_2 < |r_1| \\
&\vdots \quad \vdots \quad \vdots && \vdots \quad \vdots \quad \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 \leqslant r_n < |r_{n-1}| \\
r_{n-1} &= r_n q_{n+1} + r_{n+1} && r_{n+1} = 0
\end{aligned}$$

由定理 1.3，得到

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_n,r_{n+1}) = r_n$$

上面求两个整数的最大公因数的方法称为辗转相除法，由辗转相除法的推导过程反推回去，便有如下定理 1.4。

定理 1.4 设 $a,b \in \mathbb{Z}$，a,b 不全为 0，则存在 $m,n \in \mathbb{Z}$，使得

$$(a,b) = ma + nb$$

一般而言，定理 1.4 中 m,n 不一定唯一，比如

$$2 = (4,6) = (-1) \times 4 + 1 \times 6 = 5 \times 4 + (-3) \times 6$$

由定理 1.4 可以看出，a 和 b 的任意公因数都是 a 和 b 的最大公因数的因数。反过来，a 和 b 的最大公因数的因数也一定是 a 和 b 的公因数。这说明两个不全为零的整数的公因数与它们最大公因数的因数一致。

例 1.4 计算 $(2295,4471)$，并求整数 x,y，使得 $(2295,4471) = 2295x + 4471y$。

解

$$4471 = 2295 \times 1 + 2176$$

$$2295 = 2176 \times 1 + 119$$

$$2176 = 119 \times 18 + 34$$

$$119 = 34 \times 3 + 17$$