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

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

密码学中的可证明安全性

杨 波 著

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

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

网络空间安全重点规划丛书

密码学中的可证明安全性

杨 波 著

清华大学出版社
北京

内 容 简 介

本书全面介绍可证明安全性的发展历史及研究成果。全书共5章，第1章介绍可证明安全性涉及的数学知识和基本工具，第2章介绍语义安全的公钥密码体制的定义，第3章介绍几类常用的语义安全的公钥机密体制，第4章介绍基于身份的密码体制，第5章介绍基于属性的密码体制。

本书取材新颖，结构合理，不仅包括可证明安全性的基础理论和实用算法，同时也涵盖了可证明安全性的密码学的最新研究成果，力求使读者通过本书的学习了解本学科最新的发展方向。

本书适合作为高等院校信息安全、网络空间安全、计算机工程、密码学和信息对抗等相关专业的本科生高年级和研究生教材，也可作为通信工程师和计算机网络工程师的参考读物。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

密码学中的可证明安全性/杨波著. —北京：清华大学出版社，2017
(网络空间安全重点规划丛书)
ISBN 978-7-302-46722-9

Ⅰ. ①密… Ⅱ. ①杨… Ⅲ. ①密码学－研究 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2017)第040288号

责任编辑：张　民　战晓雷
封面设计：常雪影
责任校对：焦丽丽
责任印制：杨　艳

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：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14.25　　**字　　数**：331千字
版　　次：2017年5月第1版　　**印　　次**：2017年5月第1次印刷
印　　数：1～2000
定　　价：39.00元

产品编号：073285-01

网络空间安全重点规划丛书

编审委员会

顾问委员会主任：沈昌祥（中国工程院院士）

特别顾问：姚期智（美国国家科学院院士、美国人文及科学院院士、中国科学院院士、“图灵奖”获得者）

何德全（中国工程院院士）　蔡吉人（中国工程院院士）

方滨兴（中国工程院院士）

主　　任：封化民

副 主 任：韩　臻　李建华　王小云　张焕国　冯登国

委　　员：（按姓氏笔画为序）

马建峰　毛文波　王怀民　王劲松　王丽娜

王育民　王清贤　王新梅　石文昌　刘建伟

刘建亚　许　进　杜瑞颖　谷大武　何大可

来学嘉　李　晖　汪烈军　吴晓平　杨　波

杨　庚　杨义先　张玉清　张红旗　张宏莉

张敏情　陈兴蜀　陈克非　周福才　宫　力

胡爱群　胡道元　侯整风　荆继武　俞能海

高　岭　秦玉海　秦志光　卿斯汉　钱德沛

徐　明　寇卫东　曹珍富　黄刘生　黄继武

谢冬青　裴定一

丛书策划：张　民

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。系列教材的作者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。

该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。

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系列教材中，以进一步满足大家对外版书的需求。“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。

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

试读结束：需要全本请在线购买： www.ertongbook.com

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)。

2015 年 6 月，国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4 号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了“网络空间安全重点规划丛书”的工作，由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”“普通高等教育精品教材”“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，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，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

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

“网络空间安全重点规划丛书”编审委员会

前言

信息安全是一个综合、交叉的学科领域，涉及数学、电子、信息、通信、计算机等诸多学科的长期知识积累和最新发展成果，密码学是信息安全的核心技术，密码技术中的加密方法包括单钥密码体制和公钥密码体制。刻画公钥密码体制的安全性包括两部分：首先是刻画敌手的模型，说明敌手访问系统的方式和计算能力；其次是刻画安全性概念，说明敌手攻破了方案的安全性意味着什么。公钥加密方案语义安全的概念由 Goldwasser 和 Micali 于 1984 年提出，它以一种思维实验的模型刻画了敌手通过密文得不到明文的任何部分信息，即使是 1 比特的信息。这一概念的提出开创了可证明安全性领域的先河，将密码学建立在了计算复杂性理论之上，奠定了现代密码学理论的数学基础，从而将密码学从一门艺术变为一门科学。所以说可证明安全性是密码学和计算复杂性理论的天作之合。

本书全面介绍可证明安全性的发展历史及研究成果，共 5 章。第 1 章介绍可证明安全性用到的一些数学知识和基本工具，包括密码学中一些常用的数论知识和代数知识、计算复杂性、陷门置换、零知识证明、张成方案与秘密分割方案、归约。第 2 章介绍语义安全的公钥密码体制的定义，包括公钥加密方案在选择明文攻击下的不可区分性，公钥加密方案在选择密文攻击下的不可区分性，公钥加密方案在适应性选择密文攻击下的不可区分性。第 3 章介绍几类常用的语义安全的公钥机密体制，包括语义安全的 RSA 加密方案、Paillier 公钥密码系统、Cramer-Shoup 密码系统、RSA-FDH 签名方案、BLS 短签名方案、抗密钥泄露的公钥加密系统。第 4 章介绍基于身份的密码体制，包括基于身份的密码体制定义和安全模型，随机谕言机模型下的基于身份的密码体制，无随机谕言机模型的选定身份安全的 IBE，无随机谕言机模型下的完全安全的 IBE，密文长度固定的分层次 IBE，基于对偶系统加密的完全安全的 IBE 和 HIBE、从选择明文安全到选择密文安全。第 5 章介绍基于属性的密码体制，包括基于属性的密码体制的一般概念，基于模糊身份的加密方案，基于密钥策略的属性加密方案，基于密文策略的属性加密方案，基于对偶系统加密的完全安全的属性加密，非单调访问结构的属性加密方案，函数加密。

本书在编写过程中得到了课题组成员的大力支持和帮助，他们是4位博士后：王涛博士、王鑫博士、来齐齐博士、张丽娜博士，5位博士生：程灏、乜国雷、侯红霞、周彦伟、赵一，5位硕士生：武朵朵、马晓敏、李士强、孟茹、赵艳琪，在此一并表示感谢。另外，本书的编写得到国家自然科学基金项目（批准号：61272436，61572303）的资助，还得到陕西师范大学优秀著作出版基金和陕西师范大学重点学科建设项目的资助，在此表示感谢。

由于作者水平有限，书中不足在所难免，恳请读者批评指正。

作　者

2017年1月

目 录

试读结束：需要全本请在线购买： www.ertongbook.com

第1章 一些基本概念和工具

本章介绍可证明安全的密码学中常用的一些数学知识和基本工具。

1.1 密码学中一些常用的数学知识

1.1.1 群、环、域

群、环、域都是代数系统(也称代数结构)。代数系统是对要研究的现象或过程建立的一种数学模型,模型中包括要处理的数学对象的集合以及集合上的关系或运算,运算可以是一元的也可以是多元的,可以有一个也可以有多个。

设 $*$ 是集合 S 上的运算,若对 $\forall a,b\in S$,有 $a*b\in S$,则称 S 对运算 $*$ 是封闭的。若 $*$ 是一元运算,对 $\forall a\in S$,有 $*a\in S$,则称 S 对运算 $*$ 是封闭的。

若对 $\forall a,b,c\in S$,有 $(a*b)*c=a*(b*c)$,则称 $*$ 满足结合律。

定义 1-1 设$\langle \mathbb{G},*\rangle$是一个代数系统,$*$ 满足

(1) 封闭性。

(2) 结合律。

则称$\langle \mathbb{G},*\rangle$是半群。

定义 1-2 设$\langle \mathbb{G},*\rangle$是一个代数系统,$*$ 满足

(1) 封闭性。

(2) 结合律。

(3) 存在元素 e,对 $\forall a\in\mathbb{G}$,有 $a*e=e*a=a$,e 称为$\langle \mathbb{G},*\rangle$的单位元。

(4) 对 $\forall a\in\mathbb{G}$,存在元素 a^{-1},使得 $a*a^{-1}=a^{-1}*a=e$,称 a^{-1} 为元素 a 的逆元。

则称$\langle \mathbb{G},*\rangle$是群。若其中的运算 $*$ 已明确,有时将$\langle \mathbb{G},*\rangle$简记为$\mathbb{G}$。

如果$\mathbb{G}$是有限集合,则称$\langle \mathbb{G},*\rangle$是有限群,否则是无限群。有限群中,$\mathbb{G}$的元素个数称为群的阶数。

如果群$\langle \mathbb{G},*\rangle$中的运算 $*$ 还满足交换律,即对 $\forall a,b\in\mathbb{G}$,有 $a*b=b*a$,则称$\langle \mathbb{G},*\rangle$为交换群或 Abel 群。

群中运算 $*$ 一般称为乘法,称该群为乘法群。若运算 $*$ 改为 $+$,则称为加法群,此时逆元 a^{-1} 写成 $-a$。

【例 1-1】

(1) $\langle \mathbf{I},+\rangle$是 Abel 群,其中 $\mathbf{I}$ 是整数集合。

(2) $\langle \mathbf{Q},\cdot\rangle$是 Abel 群,其中 $\mathbf{Q}$ 是有理数集合。

(3) 设 A 是任一集合，P 表示 A 上的双射函数集合，$\langle P,\circ\rangle$ 是群，这里 $\circ$ 表示函数的合成，通常这个群不是 Abel 群。

(4) $\langle \mathbb{Z}_n,+_n\rangle$ 是 Abel 群，其中 $\mathbb{Z}_n=\{0,1,\cdots,n-1\}$，$+_n$ 是模加，$a+_nb$ 等于 $(a+b) \bmod n$，$x^{-1}=n-x$。$\langle \mathbb{Z}_n,\times_n\rangle$ 不是群，因为 0 没有逆元，这里 $\times_n$ 是模乘，$a\times_nb$ 等于 $(a\times b) \bmod n$。

定义 1-3 设 $\langle \mathbb{G},*\rangle$ 是一个群，$\mathbf{I}$ 是整数集合。如果存在一个元素 $g\in\mathbb{G}$，对于每一个元素 $a\in\mathbb{G}$，都有一个相应的 $i\in\mathbf{I}$，能把 a 表示成 g^i，则称 $\langle \mathbb{G},*\rangle$ 是循环群，g 称为循环群的生成元，记 $\mathbb{G}=\langle g\rangle=\{g^i\mid i\in\mathbf{I}\}$。称满足方程 $a^m=e$ 的最小正整数 m 为 a 的阶，记为 $|a|$。

密码学中使用的群大多为循环群，循环群的性质在 1.1.10 节和 1.1.11 节专门介绍。

定义 1-4 若代数系统 $\langle \mathbb{R},+,\cdot\rangle$ 的二元运算 $+$ 和 $\cdot$ 满足

(1) $\langle \mathbb{R},+\rangle$ 是 Abel 群。

(2) $\langle \mathbb{R},\cdot\rangle$ 是半群。

(3) 乘法 $\cdot$ 在加法 $+$ 上可分配，即对 $\forall a,b,c\in\mathbb{R}$，有

$$a\cdot(b+c)=a\cdot b+a\cdot c \text{ 和 } (b+c)\cdot a=b\cdot a+c\cdot a$$

则称 $\langle \mathbb{R},+,\cdot\rangle$ 是环。

【例 1-2】

(1) $\langle \mathbf{I},+,\cdot\rangle$ 是环，因为 $\langle \mathbf{I},+\rangle$ 是 Abel 群，$\langle \mathbf{I},\cdot\rangle$ 是半群，乘法 $\cdot$ 在加法 $+$ 上可分配。

(2) $\langle \mathbb{Z}_n,+_n,\times_n\rangle$ 是环，因为 $\langle \mathbb{Z}_n,+_n\rangle$ 是 Abel 群，$\langle \mathbb{Z}_n\times_n\rangle$ 是半群，$\times_n$ 对 $+_n$ 可分配。

(3) $\langle M_n,+,\cdot\rangle$ 是环，这里 M_n 是 $\mathbf{I}$ 上 $n\times n$ 方阵集合，$+$ 是矩阵加法，$\cdot$ 是矩阵乘法。

(4) $\langle R(x),+,\cdot\rangle$ 是环，这里 $R(x)$ 是所有实系数的多项式集合，$+$ 和 $\cdot$ 分别是多项式加法和乘法。

定义 1-5 若代数系统 $\langle \mathbb{F},+,\cdot\rangle$ 的二元运算 $+$ 和 $\cdot$ 满足

(1) $\langle \mathbb{F},+\rangle$ 是 Abel 群。

(2) $\langle \mathbb{F}-\{0\},\cdot\rangle$ 是 Abel 群，其中 0 是 $+$ 的单位元。

(3) 乘法 $\cdot$ 在加法 $+$ 上可分配，即对 $\forall a,b,c\in\mathbb{F}$，有

$$a\cdot(b+c)=a\cdot b+a\cdot c \text{ 和 } (b+c)\cdot a=b\cdot a+c\cdot a$$

则称 $\langle \mathbb{F},+,\cdot\rangle$ 是域。

$\langle \mathbf{Q},+,\cdot\rangle$、$\langle \mathbf{R},+,\cdot\rangle$、$\langle \mathbf{C},+,\cdot\rangle$ 都是域，其中 $\mathbf{Q}$、$\mathbf{R}$、$\mathbf{C}$ 分别是有理数集合、实数集合和复数集合。

有限域是指域中元素个数有限的域，元素个数称为域的阶。若 q 是素数的幂，即 $q=p^r$，其中 p 是素数，r 是自然数，则阶为 q 的域称为 Galois 域，记为 $\mathrm{GF}(q)$ 或 $\mathbb{F}_q$。

已知所有实系数的多项式集合 $R(x)$ 在多项式加法和乘法运算下构成环。类似地，任意域 $\mathbb{F}$ 上的多项式(即系数取自 $\mathbb{F}$)集合 $F(x)$ 在多项式的加法和乘法运算下也构成环。

$F(x)$ 中不可约多项式的概念与整数中的素数概念类似，是指在 $\mathbb{F}$ 上仅能被非 0 常数或自身的常数倍除尽，但不能被其他多项式除尽的多项式。

两个多项式的最高公因式为 1 时，称它们互素。

多项式的系数取自以素数 p 为模的域$\mathbb{F}$时，这样的多项式集合记为 $F_p[x]$。若 $m(x)$是 $F_p[x]$上的 n 次不可约多项式，$F_p[x]$上多项式加法和乘法改为以 $m(x)$为模的加法和乘法，此时的多项式集合记为 $F_p[x]/m(x)$，集合中元素个数为 p^n，$F_p[x]/m(x)$是一个有限域 GF(p^n)。

1.1.2　素数和互素数

1. 因子

设 a、$b(b\neq 0)$是两个整数，如果存在另一整数 m，使得 $a=mb$，则称 b 整除 a，记为 $b\mid a$，且称 b 是 a 的因子。否则称 b 不整除 a，记为 $b\nmid a$。

整除具有以下性质：

(1) $a\mid 1$，那么 $a=\pm 1$。

(2) $a\mid b$且 $b\mid a$，则 $a=\pm b$。

(3) 对任一 $b(b\neq 0)$，$b\mid 0$。

(4) $b\mid g$，$b\mid h$，则对任意整数 m、n，有 $b\mid (mg+nh)$。

这里只给出(4)的证明，其他 3 个性质的证明都很简单。

证明：

(4) 由 $b\mid g$，$b\mid h$知，存在整数 g_1、h_1，使得

$$g = bg_1, \quad h = bh_1$$

所以

$$mg + nh = mbg_1 + nbh_1 = b(mg_1 + nh_1)$$

因此

$$b \mid (mg + nh)$$

2. 素数

称整数 $p(p>1)$是素数，如果 p 的因子只有± 1、$\pm p$。

若 p 不是素数，则称为合数。

任一整数 $a(a>1)$都能唯一地分解为以下形式：

$$a = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$$

其中，$p_1<p_2<\cdots<p_t$ 是素数，$a_i>0(i=1,2,\cdots,t)$。例如：

$$91 = 7\times 13, \quad 11011 = 7\times 11^2\times 13$$

这一性质称为整数分解的唯一性，也可如下陈述：

设 P 是所有素数集合，则任意整数 $a(a>1)$都能唯一地写成以下形式：

$$a = \prod_{p\in P} p^{a_p}$$

其中 $a_p\geqslant 0$。

等号右边的乘积项取所有的素数，然而大多指数项 a_p 为 0。

相应地，任一正整数也可由非 0 指数列表表示。例如，11011 可表示为$\{a_7=1, a_{11}=2, a_{13}=1\}$。

两数相乘等价于对应的指数相加，即，由 $k=mn$ 可得：对每一素数 p，$k_p=m_p+n_p$。

而由 $a|b$ 可得：对每一素数 p，$a_p \leqslant b_p$。这是因为 p^k 只能被 $p^j(j \leqslant k)$ 整除。

3. 互素数

称 c 是两个整数 a、b 的最大公因子，如果

(1) c 是 a 的因子也是 b 的因子，即 c 是 a、b 的公因子。

(2) a 和 b 的任一公因子，也是 c 的因子。

表示为 $c=(a,b)$。

由于要求最大公因子为正，所以 $(a,b)=(a,-b)=(-a,b)=(-a,-b)$。一般 $(a,b)=(|a|,|b|)$。由任一非 0 整数能整除 0，可得 $(a,0)=a$。如果将 a、b 都表示为素数的乘积，则 (a,b) 极易确定。

【例 1-3】

$$300 = 2^2 \times 3^1 \times 5^2$$

$$18 = 2^1 \times 3^2$$

$$(18,300) = 2^1 \times 3^1 \times 5^0 = 6$$

一般由 $c=(a,b)$ 可得：对每一素数 p，$c_p=\min\{a_p,b_p\}$。

如果 $(a,b)=1$，则称 a 和 b 互素。

称 d 是两个整数 a、b 的最小公倍数，如果

(1) d 是 a 的倍数也是 b 的倍数，即 d 是 a、b 的公倍数。

(2) a 和 b 的任一公倍数，也是 d 的倍数。

表示为 $c=[a,b]$。

若 a、b 是两个互素的正整数，则 $[a,b]=ab$。

1.1.3 模运算

设 n 是正整数，a 是整数，如果用 n 除 a，得商为 q，余数为 r，则

$$a = qn + r, \quad 0 \leqslant r < n, \quad q = \left\lfloor \frac{a}{n} \right\rfloor$$

其中 $\lfloor x \rfloor$ 为小于或等于 x 的最大整数。

用 $a \bmod n$ 表示余数 r，则

$$a = \left\lfloor \frac{a}{n} \right\rfloor n + a \bmod n$$

如果 $a \bmod n = b \bmod n$，则称两个整数 a 和 b 模 n 同余，记为 $a \equiv b \bmod n$。称与 a 模 n 同余的数的全体为 a 的同余类，记为 $[a]$，称 a 为这个同余类的表示元素。

注意：如果 $a \equiv 0 \bmod n$，则 $n|a$。

同余有以下性质：

(1) $n|(a-b)$ 与 $a \equiv b \bmod n$ 等价。

(2) $a \bmod n = b \bmod n$，则 $a \equiv b \bmod n$。

(3) $a \equiv b \bmod n$，则 $b \equiv a \bmod n$。

(4) $a \equiv b \bmod n$，$b \equiv c \bmod n$，则 $a \equiv c \bmod n$。

(5) 如果 $a \equiv b \bmod n, d \mid n$，则 $a \equiv b \bmod d$。

(6) 如果 $a \equiv b \bmod n_i (i=1,2,\cdots,k), d=[n_1,n_2,\cdots,n_k]$，则 $a \equiv b \bmod d$。

证明：

(5) 由 $a \equiv b \bmod n$ 及 $d \mid n$，得 $n \mid (a-b), d \mid (a-b)$。

(6) 由 $a \equiv b \bmod n_i$ 得，$n_i \mid (a-b)$，即 $a-b$ 是 $n_1,n_2,\cdots,n_k$ 的公倍数，所以 $d \mid (a-b)$。

从以上性质易知，同余类中的每一元素都可作为这个同余类的表示元素。

求余数运算（简称求余运算）$a \bmod n$ 将整数 a 映射到集合 $\{0,1,\cdots,n-1\}$，称求余运算在这个集合上的算术运算为模运算，模运算有以下性质：

(1) $[(a \bmod n)+(b \bmod n)] \bmod n=(a+b) \bmod n$。

(2) $[(a \bmod n)-(b \bmod n)] \bmod n=(a-b) \bmod n$。

(3) $[(a \bmod n)\times(b \bmod n)] \bmod n=(a\times b) \bmod n$。

证明：

(1) 设 $a \bmod n=r_a$，$(b \bmod n)=r_b$，则存在整数 j、k 使得 $a=jn+r_a$，$b=kn+r_b$。因此

$$\begin{aligned}(a+b) \bmod n &=[(j+k)n+r_a+r_b] \bmod n=(r_a+r_b) \bmod n \\ &=[(a \bmod n)+(b \bmod n)] \bmod n\end{aligned}$$

(2)、(3)的证明类似。

【例 1-4】 设 $\mathbb{Z}_8=\{0,1,\cdots,7\}$，考虑 $\mathbb{Z}_8$ 上的模加法和模乘法，结果如表 1-1 所示。

表 1-1　模 8 运算

+	0	1	2	3	4	5	6	7	×	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	2	3	4	5	6	7	0	1	0	1	2	3	4	5	6	7
2	2	3	4	5	6	7	0	1	2	0	2	4	6	0	2	4	6
3	3	4	5	6	7	0	1	2	3	0	3	6	1	4	7	2	5
4	4	5	6	7	0	1	2	3	4	0	4	0	4	0	4	0	4
5	5	6	7	0	1	2	3	4	5	0	5	2	7	4	1	6	3
6	6	7	0	1	2	3	4	5	6	0	6	4	2	0	6	4	2
7	7	0	1	2	3	4	5	6	7	0	7	6	5	4	3	2	1

从加法结果可见，对每一 x，都有一个 y，使得 $x+y \equiv 0 \bmod 8$。如对 2，有 6，使得 $2+6 \equiv 0 \bmod 8$，称 y 为 x 的负数，也称为加法逆元。

对 x，若有 y，使得 $x\times y \equiv 1 \bmod 8$，如 $3\times 3 \equiv 1 \bmod 8$，则称 y 为 x 的倒数，也称为乘法逆元。本例可见并非每一 x 都有乘法逆元。

一般，定义 $\mathbb{Z}_n$ 为小于 n 的所有非负整数集合，即

$$\mathbb{Z}_n=\{0,1,\cdots,n-1\}$$

称 $\mathbb{Z}_n$ 为模 n 的同余类集合。其上的模运算有以下性质：

(1) 交换律：

$$(w+x) \bmod n=(x+w) \bmod n$$
$$(w\times x) \bmod n=(x\times w) \bmod n$$

试读结束：需要全本请在线购买：　www.ertongbook.com