信息安全

——核心理论与实践

冯登国　卿斯汉　编著

国防工业出版社

信息安全
——核心理论与实践

冯登国　卿斯汉　编著

国防工业出版社
·北 京·

图书在版编目(CIP)数据

信息安全:核心理论与实践/冯登国,卿斯汉编著.
—北京:国防工业出版社,2000.6

ISBN 7-118-02240-3

Ⅰ.信…Ⅱ.①冯…②卿…Ⅲ.电子计算机-安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2000)第 03461 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号)
(邮政编码 100044)
北京怀柔新华印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 10 1/2 233 千字
2000 年 6 月第 1 版 2000 年 6 月北京第 1 次印刷
印数:1—4000 册 定价:18.00 元

前　言

随着全球信息化的飞速发展，我国大量建设的各种信息化系统已经成为国家关键基础设施，其中许多业务要与国际接轨，诸如电信、电子商务、金融网络等。信息安全问题已成为影响国家全局和长远利益的急待解决的重大关键问题。信息安全不但是发挥信息革命带来的高效率、高效益的有力保证，而且是对抗霸权、抵御信息侵略的重要屏障。解决信息安全问题的关键技术之一是密码技术，密码技术主要包括加密技术、认证技术和密钥管理技术。加密的主要目的是防止机密信息的泄露；认证的主要目的是防止信息的篡改、删除、重放和伪造；密钥管理的主要目的是保证加密和认证机制的有效实施。

作者写作本书的主要意图是想让读者了解信息安全核心理论与实践的发展现状，掌握必要的基本理论和技术，能在以后的工作中解决一些实际安全问题。

密码学的研究已有几千年的历史，但直到 1949 年 Shannon 发表了题为“保密通信的信息理论”的论文后它才真正成为一门科学。特别是在 70 年代中期，密码学的发展出现了两件引人注目的事件：一件是 1976 年 Diffie 和 Hellman 发表的题为“密码学的新方向”的论文使密码学更加完善和实用；另一件是美国国家标准局于 1977 年向全世界公布的美国数据加密标准(DES)，人们将这两个事件作为现代密码学诞生的标志。本书关于信息安全核心理论的内容，主要讲述这两个事件以后发展起来的理论和技术，同时阐述以上述核心理论为基础的实践与应用。

全书共分 6 章。第 1 章主要介绍了密码学的基础知识，包括密码学的基本概念、密码学的信息理论基础、密码学的复杂性理论基础、协议的形式化分析技术和本书中所用到的一些最基本的数学知识。第 2 章主要介绍了现有的一些有代表性的加密算法，包括一些有代表性的分组密码、流密码和公钥密码算法。第 3 章主要介绍了现有的一些有代表性的认证协议，包括各种数字签名协议、一些典型的 Hash 算法、一些流行的识别协议。第 4 章主要介绍了一些典型的密钥分配和交换协议、密钥托管技术和秘密共享方案的基本思想。第 5 章主要介绍了一些实用安全系统和技术，包括 X.509、PGP 系统、INTRANET 安全集成系统的实现。第 6 章介绍了一些典型的电子商务协议及其形式化分析技术，包括一些典型的数字货币和电子商务协议。

本书是作者在长期从事科研和教学实践的基础上编写的，主要面向的读者是高年级本科生、计算专业和通信专业的硕士和博士研究生，也可供从事有关专业的教学、科研和工程技术人员参考。

作　者

1999 年 10 月

内 容 简 介

本书系统地介绍了信息安全的核心理论与技术，主要包括密码学的基本概念，一些典型的古典密码体制及其分析，阅读本书所需要的一些数学基础，Shannon 的保密系统的信息理论基础，Simmons 的认证系统的信息理论基础，复杂性理论基础和协议的形式化分析技术；一些典型的加密算法包括分组密码、基于 LFSRs 的流密码和公钥密码算法；一些典型的认证协议，包括各种各样的数字签名协议、Hash 函数、时戳技术、身份识别协议和基于身份的密码方案；一些典型的密钥管理技术，包括密钥分配协议、密钥协定协议、秘密共享和密钥托管技术；一些实用安全系统与技术，包括 X.509、PGP 系统、PEM 系统、SSL 协议、INTRANET 安全集成系统的实现；一些典型的电子商务协议及其形式化分析等。

本书可供从事密码、信息安全、数学、计算机、通信专业的科技人员和高等院校相关专业的师生参考。

目　录

第1章 绪 论

密码学用于保护军事和外交通信可追溯到几千年前。在今天的信息时代，大量的敏感信息如病历、法庭记录、私人财产等常常通过公共通信设施或计算机网络来进行交换，而这些信息的秘密性和真实性是人们迫切需要的。因此，现代密码学的应用已不再局限于军事、政治和外交，其商用价值和社会价值已得到了广泛的重视。

密码学的发展历史可大致划分为三个阶段：从古代到1949年可看作是科学密码学的前夜时期，该时期的密码学专家常常是凭直觉和信念来进行密码设计和分析，而不是靠推理证明。1949年Shannon发表的“保密系统的信息理论”一文为私钥密码系统建立了理论基础，从此密码学成为一门科学。从1949年到1975年这段时期，密码学理论的研究工作进展不大，公开的密码学文献很少，1967年Kahn出版了一本专著《The Codebreakers(破译者)》，该书的意义在于它不仅记述了1967年之前密码学发展的历史，而且使许多不知道密码学的人了解了密码学。70年代初期，IBM发表了Feistel和他的同事在这个学科方面的几篇技术报告。1976年Diffiee和Hellman的《密码编码学新方向》一文导致了密码学上的一场革命。他们首次证明了在发送者和接收者之间无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。

本章主要介绍了密码学的基础知识，包括密码学的基本概念、密码学的信息理论基础、密码学的复杂性理论基础、协议的形式化分析技术和本书中所用到的一些最基本的数学知识。

1.1 密码学的基本概念

密码学是研究密码系统或通信安全的一门科学，它主要包括两个分支，即密码编码学和密码分析学。密码编码学的主要目的是寻求保证消息保密性和可认证性的方法；密码分析学的主要目的是研究加密消息的破译和消息的伪造。

采用密码技术可以隐蔽和保护需要保密的消息，使未授权者不能提取信息也不能窜改信息。被隐蔽的消息称作明文，隐蔽后的消息称作密文。将明文变换成密文的过程称作加密，其逆过程，即由密文恢复出原明文的过程称作解密。对明文进行加密操作的人员称作密码员。密码员对明文进行加密时所采用的一组规则称作加密算法，传送消息的意定对象称作接收者，他对密文进行解密时所采用的一组规则称作解密算法。加密和解密算法的操作通常都是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。

根据密钥的特点，Simmons将密码体制分为对称和非对称密码体制两种。对称密码体制又称单钥或私钥或传统密码体制，非对称密码体制又称双钥或公钥密码体制。在本书中，我们采用私钥和公钥密码体制这两个术语。在私钥密码体制中，加密密钥和解密密

钥是一样的或彼此之间容易相互确定。按加密方式又可将私钥密码体制分为流密码和分组密码两种。在流密码中,将明文消息按字符逐位地加密;在分组密码中,将明文消息分组(每组含有多个字符),逐组地进行加密。在公钥密码体制中,加密密钥和解密密钥不同,从一个难以推出另一个。现有的大多数公钥密码属于分组密码,只有概率加密体制属于流密码。

在消息传输和处理系统中,除了意定的接收者外,还有非授权者,他们通过各种办法如搭线窃听、电磁窃听、声音窃听等来窃取机密信息,称其为截收者。他们虽然不知道系统所用的密钥,但通过分析可能从截获的密文推断出原来的明文甚至密钥,这一过程称作密码分析。从事这一工作的人称作密码分析员或密码分析者。所谓一个密码是可破的,是指如果通过密文能够迅速地确定明文或密钥,或通过明文—密文对能够迅速地确定密钥。通常假定密码分析者或敌手知道所使用的密码系统,这个假设称作 Kerckhoff 假设。当然,如果密码分析者或敌手不知道所使用的密码系统,那么破译密码更难,但是我们不应该把密码系统的安全性建立在敌手不知道所使用的密码系统这个前提之下,因此,在设计一个密码系统时,目的是在 Kerckhoff 假设下达到安全性。

根据密码分析者破译时已具备的前提条件,通常人们将攻击类型分为下述四种:

(1) 唯密文攻击:密码分析者有一个或多个密文。

(2) 已知明文攻击:密码分析者有一些明文以及相应的密文。

(3) 选择明文攻击:密码分析者有机会使用密码机,因此可选择一些明文,并产生密文。

(4) 选择密文攻击:密码分析者有机会使用密码机,因此可选择一些密文,并产生明文。

上述每种攻击的目的是决定所使用的密钥。这四种攻击类型的强度按序递增,唯密文攻击是最弱的一种攻击,选择密文攻击是最强的一种攻击。如果一个密码系统能够抵抗选择密文攻击,那么它当然能够抵抗其余三种攻击。

对一个密码系统采取截获密文进行分析的这类攻击称作被动攻击。密码系统还可能遭受到的另一类攻击是主动攻击,非法入侵者主动向系统窜扰,采用删除、更改、增添、重放、伪造等手段向系统注入假消息。防止这种攻击的一种有效方法是使发送的消息具有可被验证的能力,使接收者或第三者能够识别和确认消息的真伪,实现这类功能的密码系统称作认证系统。消息的认证性和消息的保密性不同,保密性是使截获者在不知密钥条件下不能解读密文的内容,而认证性是使任何不知密钥的人不能构造出一个密报,使意定的接收者解密成一个可理解的消息(合法的消息)。这里谈谈保密系统和认证系统的基本要求。

为了保证信息的机密性,抵抗密码分析,一个安全的保密系统至少应当满足下述基本要求:

(1) 系统即使达不到理论上是不可破的,也应当是实际上不可破的。也就是说,从截获的密文或某些已知明文—密文对,要确定密钥或任意明文在计算上是不可行的。

(2) 系统的保密性不依赖于对加密体制或算法的保密(Kerckhoff 假设),而依赖于对密钥的保密。

(3) 系统既易于实现又便于使用。

为了保证信息的可认证性,抵抗主动攻击,一个安全的认证系统至少应当满足下述基本要求:

(1) 意定的接收者能够检验和证实消息的合法性和真实性。

(2) 消息的发送者对所发的消息不能抵赖。

(3) 除了合法的消息发送者外,其他人不能伪造合法的消息,而且在已知合法密文下,要确定加密密钥或系统地伪造合法密文在计算上是不可行的。

(4) 当通信双方(或多方)发生争执时,可由称作仲裁者的第三方解决争执。

1.2 数学基础

密码学是一门交叉学科,它涉及到许多学科,诸如数学、计算机、通信、物理等。本节主要介绍该书中所用到的一些数学知识。

1.2.1 数论

用 $\mathbf{Z}$ 表示全体整数所构成的集合$\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$。

定义 1.2.1 设 $a,b\in\mathbf{Z},a\neq0$,如果存在 $c\in\mathbf{Z}$,使得 $b=ac$,则称 a 整除 b,并称 a 是 b 的因子,b 是 a 的倍数,记为 $a\mid b$。否则,称 a 不能整除 b,记为 $a\nmid b$。

整除性有下列基本性质:若 $a\neq0,b\neq0$,则

(1) $a\mid a$;

(2) 如果 $a\mid b,b\mid c$,则 $a\mid c$;

(3) 如果 $a\mid c$,则 $ab\mid cb$;

(4) 如果 $a\mid d,a\mid e$,则对所有的 $x,y\in\mathbf{Z}$,有 $a\mid(dx+ey)$;

(5) 如果 $a\mid b,b\mid a$,则 $a=\pm b$。

定理 1.2.1 (带余除法) 设 $a,b\in\mathbf{Z},b\geqslant1$,则存在唯一确定的整数 q 和 r,使得 $a=qb+r,0\leqslant r<b$。q 称为 a 除以 b 所得的商,r 称为 a 除以 b 所得的最小非负剩余。

定义 1.2.2 设 $a,b\in\mathbf{Z},a,b$ 不全为 0,如果 $c\mid a$,且 $c\mid b$,则称 c 为 a 和 b 的公因子。特别地,我们把 a 和 b 的所有公因子中最大的,称为 a 和 b 的最大公因子。

可以证明 a 和 b 的最大公因子必然存在,而且唯一。将这个最大公因子记为 $\gcd(a,b)$。称 a 与 b 互素,如果 $\gcd(a,b)=1$。可以证明,若 $\gcd(a,b)=d$,那么一定存在整数 x 和 y,使得 $xa+yb=d$。约定 $\gcd(0,0)=0$。类似地可以定义任意有限多个整数 $a_1,a_2,\cdots,a_n$ 的最大公因子,记为 $\gcd(a_1,a_2,\cdots,a_n)$,可以证明 $\gcd(a_1,a_2,\cdots,a_n)=\gcd(\gcd(a_1,a_2,\cdots,a_{n-1}),a_n)$。

定义 1.2.3 设 $a,b\in\mathbf{Z},a,b$ 都不为 0,如果 $a\mid D,b\mid D,D\geqslant1$,则称 D 为 a 和 b 的公倍数。我们把 a 和 b 的所有公倍数中最小的正数,称为 a 和 b 的最小公倍数。

a 和 b 的最小公倍数一定存在而且唯一,将它记为 $\mathrm{lcm}(a,b)$。两个非零整数的最小公倍数的概念可以推广到任意多个非零整数的情形。

对两个正整数 a 和 b,可以证明 $ab=\gcd(a,b)\cdot\mathrm{lcm}(a,b)$。

定义 1.2.4 设 $p\in\mathbf{Z},p\geqslant2$,如果 p 的正因子只有 1 和 p,则称 p 为素数,否则,称 p 为合数。

关于素数,有以下一些事实:

(1) 如果 p 是素数,且 $p \mid ab$,则 $p \mid a$ 或 $p \mid b$。

(2) (算术基本定理)每个整数 $n \geqslant 2$,均可以分解成素数幂之积:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

若不计因子的顺序,这个分解式是唯一的。其中 $k \geqslant 1$, $p_i (1 \leqslant i \leqslant k)$是两两不同的素数, $e_i (1 \leqslant i \leqslant k)$是正整数。

(3) 有无穷多个素数。

(4) (素数定理)设 $\pi(x)$表示不大于 x 的素数的数目,则 $\lim\limits_{x \to \infty} \pi(x)/x/\ln(x) = 1$。

素数定理表明,对充分大的 x, $\pi(x)$可用 $x/\ln(x)$来近似表示,这里 $\ln x$ 是自然对数。

设 $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} (e_i \geqslant 0, f_i \geqslant 0, 1 \leqslant i \leqslant k)$,则

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}$$

$$\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}$$

其中, $\min\{e,f\}$表示 e,f 中最小者, $\max\{e,f\}$表示 e,f 中最大者。

例 1.2.1 设 $a = 4864 = 2^8 \times 19$, $b = 3458 = 2 \times 7 \times 13 \times 19$

则 $\gcd(4864,3458) = 2 \times 19$, $\operatorname{lcm}(4864,3458) = 2^8 \times 7 \times 13 \times 19$。

定义 1.2.5 设 $n \geqslant 1$, $\varphi(n)$表示在区间$[1,n]$中与 n 互素的整数的个数。$\varphi(n)$称为 Euler 函数。

Euler 函数 $\varphi(n)$有以下性质:

(1) 如果 p 是素数,则 $\varphi(p) = p - 1$

(2) Euler 函数是一个积性函数,也就是说,如果 $\gcd(m,n) = 1$,则 $\varphi(mn) = \varphi(m) \cdot \varphi(n)$。

(3) 如果 $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ 是 n 的一个典型分解式,则

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

(4) 对于所有的整数 $n \geqslant 5$,有 $\varphi(n) \geqslant n/6\ln(\ln(n))$。

虽然从理论上,可以通过分解整数 a 和 b 来计算它们的最大公因子,但整数分解是一个很困难的问题。实际上,用辗转相除法极易求出两个数的最大公因子,这就是通常所说的 Euclidean 算法,其理论依据是:如果 a,b 是两个正整数, $a > b$,作带余除法,即求 q 与 r 使 $a = qb + r, 0 \leqslant r < b$,则 $\gcd(a,b) = \gcd(b,r)$。

1) 计算两个整数的最大公因子的 Euclidean 算法

输入:两个非负整数 a 和 b, $a \geqslant b$。

输出: a 和 b 的最大公因子。

(1) 当 $b \neq 0$ 时,完成下列步骤:

1.1 置 $q \leftarrow \left[\frac{a}{b}\right]$, $r \leftarrow a - qb$, $a \leftarrow b$, $b \leftarrow r$

(2) 输出 a。

其中, $[x]$表示不超过 x 的最大整数。

该算法的运行时间为 $O((\lg n)^2)$。

Euclidean 算法能被扩展使得不仅可用来计算整数 a 和 b 的最大公因子 d，而且可以找到整数 x 和 y 使得 $ax + by = d$。

2) 扩展的 Euclidean 算法

输入：两个非负整数 a 和 b，$a \geqslant b$。

输出：$d = \gcd(a, b)$和满足等式 $ax + by = d$ 的整数 x 和 y。

(1) 如果 $b = 0$，则置 $d \leftarrow a, x \leftarrow 1, y \leftarrow 0$，并输出$(d, x, y)$。

(2) 置 $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$。

(3) 当 $b > 0$ 时，执行下列步骤：

3.1 $q \leftarrow [a/b], r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$。

3.2 $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, y_2 \leftarrow y_1, x_1 \leftarrow x, y_1 \leftarrow y$。

(4) 置 $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$，并输出$(d, x, y)$。

该算法的时间复杂度为 $O((\lg n)^2)$。

例 1.2.2 设 $a = 4864, b = 3458$。下表是用扩展 Euclidean 算法计算 $\gcd(a, b)$的各步骤：

q	r	x	y	a	b	x_2	x_1	y_2	y_1
				4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

上表表明，$\gcd(4864, 3458) = 38, 4864 \times 32 + 3458 \times (-45) = 38$。

3) 同余式

设 n 是一个正整数。

定义 1.2.6 设 $a, b \in \mathbf{Z}$，如果 $n \mid (b - a)$，则 a 和 b 模 n 同余，记为 $a \equiv b \pmod{n}$。整数 n 称为同余模。

同余式具有下列一些基本性质：

(1) (反身性) $a \equiv a \pmod{n}$。

(2) (对称性) 如果 $a \equiv b \pmod{n}$，那么 $b \equiv a \pmod{n}$。

(3) (传递性)如果 $a \equiv b \pmod{n}$，$b \equiv c \pmod{n}$，那么 $a \equiv c \pmod{n}$。

(4) 如果 $a \equiv a_1 \pmod{n}$，$b \equiv b_1 \pmod{n}$，那么

$$a + b \equiv a_1 + b_1 \pmod{n}, a - b \equiv a_1 - b_1 \pmod{n}, ab \equiv a_1 b_1 \pmod{n}。$$

(5) 如果 $ac \equiv bd \pmod{n}$，$a \equiv b \pmod{n}$，$\gcd(a, n) = 1$，那么 $c \equiv d \pmod{n}$。

(6) 存在 c，使 $ac \equiv 1 \pmod{n}$当且仅当 $\gcd(a, n) = 1$。

由于上述性质(1)～(3)可以将整数分成若干类，使得同类的数都同余，异类的数都不同余，这种类称为同余类或剩余类。如果是模 n，那么共有 n 个同余类，它们是$\{r + qn \mid$

$q\in\mathbf{Z}\}$,$0\leqslant r<n$。同余类$\{r+qn\mid q\in\mathbf{Z}\}$可用其中任一元 a(经常取 $a=r$)代表,记作 $a(\mathrm{mod}n)$。在不言自明时,也简记作 a。用 Z_n 表示模 n 的同余类全体所成的集合,即 $Z_n=\{r(\mathrm{mod}n)\mid 0\leqslant r<n\}$,或简记作 $Z_n=\{r\mid 0\leqslant r<n\}$。根据上述性质(4)模 n 同余类之间可以作加、减与乘这三种运算,即类间的运算可用类的代表元间的同种运算实现。将性质(6)中的 c 称作 $a(\mathrm{mod}n)$的逆,记为 $a^{-1}(\mathrm{mod}n)$。依性质(5)与(6),$a(\mathrm{mod}n)$ 的逆存在的充要条件是 $\gcd(a,n)=1$,而且如果存在逆,那么逆是唯一的。习惯上,将 Z_n 中可逆元全体构成的集合记作 Z_n^*。$a\in Z_n^*$ 的逆可用扩展的 Euclidean 算法求出,这是因为用扩展的 Euclidean 算法可以找到整数 x 和 y 使得 $ax+by=1$,这样 $a^{-1}=x(\mathrm{mod}n)$。

关于 Z_n^*($n\geqslant 2$)有如下的重要定理:

定理 1.2.2(Euler 定理) 对任意的 $a\in Z_n^*$,有 $a^{\varphi(n)}\equiv 1\ \mathrm{mod}n$。特别地,当 n 是一个素数时,$a^{n-1}\equiv 1(\mathrm{mod}\ n)$,这就是著名的 Fermat 定理。

证明 记 $Z_n^*=\{a_1,a_2,\cdots,a_{\varphi(n)}\}$,对任意的 $a\in Z_n^*$,由于存在 a 的逆元 $a^{-1}\in Z_n^*$,所以易证以下集合仍然是 Z_n^*:

$$\{aa_1(\mathrm{mod}n),aa_2(\mathrm{mod}\ n),\cdots,aa_{\varphi(n)}(\mathrm{mod}\ n)\}$$

于是有$\prod_{i=1}^{\varphi(n)}(aa_i)\equiv\prod_{i=1}^{\varphi(n)}a_i(\mathrm{mod}\ n)$,即 $a^{\varphi(n)}\prod_{i=1}^{\varphi(n)}a_i\equiv\prod_{i=1}^{\varphi(n)}a_i(\mathrm{mod}\ n)$,所以 $a^{\varphi(n)}\equiv 1(\mathrm{mod}\ n)$。

定理 1.2.3 设 p 和 q 是两个不同的素数,$n=pq$,$\varphi(n)=(p-1)(q-1)$,对任意的 $x\in Z_n$ 及任意的非负整数 k,有 $x^{k\varphi(n)+1}\equiv x(mod\ n)$。

证明 如果 $p\nmid x$,则由定理 1.2.2 知,$x^{p-1}\equiv 1(\mathrm{mod}p)$,而 $\varphi(p)=(p-1)\mid\varphi(n)$,所以 $x^{k\varphi(n)+1}\equiv x^{k\varphi(n)}\cdot x\equiv x(\mathrm{mod}\ p)$。如果 $p\mid x$,则 $x\equiv 0(\mathrm{mod}\ p)$,显然 $x^{k\varphi(n)+1}\equiv x(\mathrm{mod}\ p)$亦成立。同理可证,恒有 $x^{k\varphi(n)+1}\equiv x\ \mathrm{mod}q$。由上面两式及 $\gcd(p,q)=1$ 知,$x^{k\varphi(n)+1}\equiv x\,\mathrm{mod}\,pq$。

定理 1.2.4(中国剩余定理) 设 $m_i\in\mathbf{Z},(1\leqslant i\leqslant r),\gcd(m_i,m_j)=1,i\neq j$。

$a_i\in\mathbf{Z},1\leqslant i\leqslant r$。那么同余方程组

$$\begin{cases}x\equiv a_1(\mathrm{mod}m_1)\\ x\equiv a_2(\mathrm{mod}m_2)\\ \quad\vdots\\ x\equiv a_r(\mathrm{mod}m_r)\end{cases}$$

必有整数解,其解模 $M=m_1m_2\cdots m_r$ 是唯一的。该解可由下式给出:

$$x=\sum_{i=1}^{r}a_iM_i\gamma_i(\mathrm{mod}n)$$

其中,$M_i=M/m_i$,$\gamma_i=M_i^{-1}\mathrm{mod}m_i$,$1\leqslant i\leqslant r$。

4) 二次剩余

定义 1.2.7 设 $a\in Z_n^*$。如果存在 $x\in Z_n^*$ 使得 $x^2\equiv a\ (\mathrm{mod}\ n)$,那么称 a 是模 n 的二次剩余。否则,我们称 a 是模 n 的二次非剩余。记模 n 的所有二次剩余之集为 Q_n,记模 n 的所有二次非剩余之集为 $\overline{Q}_n$。

关于二次剩余有以下一些基本事实:

(1) 当 $n=p$ 是一个奇素数时,$|Q_p|=|\overline{Q_p}|=(p-1)/2$,这里用 $|S|$ 表示集合 S 中元素的个数。

(2) 当 $n=pq$, p 和 q 是两个不同的奇素数时:

$|Q_n|=|Q_p||Q_q|=(p-1)(q-1)/4$, $|\overline{Q_n}|=3(p-1)(q-1)/4$

(3) (Euler 准则) 设 p 是一个奇素数,则 $x\in Q_p$ 当且仅当 $x^{(p-1)/2}\equiv 1(\bmod p)$。

设 $a\in Q_n$,如果 $x\in Z_n^*$ 使得 $x^2\equiv a(\bmod n)$,那么也称 x 是 a 模 n 的一个平方根。

5) Legendre 和 Jacobi 符号

定义 1.2.8 设 p 是一个奇素数,a 是一个整数。则 Legendre 符号 $\left(\frac{a}{p}\right)$ 定义为

$$\left(\frac{a}{p}\right)=\begin{cases}0, p\mid a\\ 1, a\in Q_p\\ -1, a\in \overline{Q_p}\end{cases}$$

Legendrie 符号有以下的性质:

(1) $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2}(\bmod p)$。特别地,$\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$。因此,如果 $p\equiv 1\ (\bmod 4)$,那么 $-1\in Q_p$;如果 $p\equiv 3\ (\bmod 4)$,那么 $-1\in\overline{Q_p}$。

(2) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$。因此,如果 $a\in Z_p^*$,那么 $\left(\frac{a^2}{p}\right)=1$。

(3) 如果 $a=b(\bmod p)$,那么 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$。

(4) $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$。因此,如果 $p\equiv 1$ 或 $7(\bmod 8)$,那么 $\left(\frac{2}{p}\right)=1$;如果 $p\equiv 3$ 或 $5(\bmod 8)$,那么 $\left(\frac{2}{p}\right)=-1$。

(5) (二次互反律) 设 q 是一个不同于 p 的奇素数,则 $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$。

定义 1.2.9 设 $n\geqslant 3$ 是一个奇数,$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$,其中 $p_i(1\leqslant i\leqslant k)$ 是两两互素的素数。则 Jacobi 符号 $\left(\frac{a}{n}\right)$ 定义为

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_k}\right)^{e_k}$$

特别地,当 n 是奇素数时,Jacobi 符号就是 Legendrie 符号。可见,Jacobi 符号是 Legendre符号的推广。

Jacobi 符号有以下基本性质(以下设 n, m 为奇数):

(1) $\left(\frac{a}{n}\right)=0,1$ 或 -1。再者 $\left(\frac{a}{n}\right)=0$,当且仅当 $\gcd(a,n)\neq 1$。

(2) $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$。特别,如果 $a\in Z_n^*$,那么 $\left(\frac{a^2}{n}\right)=1$。

(3) $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$。

(4) $\left(\frac{1}{n}\right)=1$。

(5) 如果 $a\equiv b(\bmod n)$,那么 $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$。

(6) $\left(\frac{-1}{n}\right)=(-1)^{(n-1)/2}$。

(7) $\left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}$。

(8) (二次互反律)$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$。

例 1.2.3 计算$\left(\frac{7411}{9283}\right)$。

$$\left(\frac{7411}{9283}\right)=(-1)^{\frac{(7411-1)(9283-1)}{4}}\left(\frac{9283}{7411}\right)=-\left(\frac{1872}{7411}\right)=-\left(\frac{2}{7411}\right)^2\left(\frac{3}{7411}\right)^2\left(\frac{13}{7411}\right)=$$

$$-\left(\frac{13}{7411}\right)=(-1)(-1)^{\frac{(13-1)(7411-1)}{4}}\left(\frac{7411}{13}\right)=-\left(\frac{1}{13}\right)=-1$$

1.2.2 代数基础

本节我们简要介绍三种最基本的代数结构:群,环,域。

1.2.2.1 群

定义 1.2.10 设 S 是一个集合,在 S 上的一个二元运算 $*$ 是从 $S\times S$ 到 S 的一个映射。

定义 1.2.11 集合 G 称作群,如果 G 上有满足下列三个条件的二元运算 $*$:

(1) 群运算是可结合的。也就是说,对 G 上任取的元素 a,b,c,有 $a*(b*c)=(a*b)*c$。

(2) G 中有元素 1,使得对所有的 $a\in G$,有 $a*1=1*a=a$。

(3) 对每一个 $a\in G$,有元素 b 使得 $b*a=a*b=1$。

(2)中元素 1 称作群 G 的单位元,(3)中元素 b 称作 a 的逆元。可以证明群 G 中的单位元是唯一的,任一元 a 的逆元 a^{-1} 也是唯一的。对 $i\geqslant 0$,记 $a^i=a*a^{i-1}$, $a^{-i}=(a^{-1})^i$。

一个群 G 是 Abelian 群或交换群或加法群,如果它还满足下列条件:

(4) 对所有的 $a,b\in G$ 有 $a*b=b*a$。

对加法群而言,通常用 0 来表示单位元素,用 $-a$ 表示 a 的逆。

定义 1.2.12 如果 $|G|$ 是有限的,那么称 G 是有限群,$|G|$ 称为它的阶。

例 1.2.4 整数集 $\mathbf{Z}$ 关于普通的加法形成一个加法群。单位是 0,a 的逆是 $-a$。

例 1.2.5 剩余类集 Z_n 关于模 n 加法运算形成一个阶为 n 的加法群。Z_n 关于模 n 的乘法运算不是一个群,因为不是所有的元素都有乘法逆。然而,集 Z_n^* 关于模 n 的乘法运算形成一个阶为 $\varphi(n)$ 的加法群,单位元素为 1。

定义 1.2.13 设 H 是群 G 的一个非空子集,如果 H 本身在群 G 的运算之下构成一个群,我们说 H 是 G 的一个子群。如果 H 是 G 的一个子群且 $H\neq G$,则称 H 是 G 的一个真子群。

定义 1.2.14 设 G 是一个群,如果 G 中有一个元素 a 使得对每一个 $b\in G$ 都存在一个整数 i 使得 $b=a^i$,则称 G 是一个循环群。a 称为 G 的一个生成元。

定义 1.2.15 设 G 是一个群, $a\in G$, a 的阶定义为使得 $a^t=1$ 成立的最小正整数 t (假定这样的正整数存在的话)。如果这样的正整数 t 不存在,那么 a 的阶定义为 ∞。如