高等院校密码信息安全类专业系列教材

中国密码学会教育工作委员会推荐教材

信息安全的数学基础

罗守山 陈萍 罗群 辛阳 编著

XINXI ANQUAN DE SHUXUE JICHU

国防工业出版社
National Defense Industry Press

高等院校密码信息安全类专业系列教材
中国密码学会教育工作委员会推荐教材

信息安全的数学基础

罗守山　陈萍　罗群　辛阳　编著

国防工业出版社
·北京·

总　序

信息系统所面临的各种安全威胁日益突出，信息安全问题已成为涉及国家政治、军事、经济和文教等诸多领域的战略安全问题。我国政府对网络与信息安全问题高度重视，国办印发的文件《关于网络信任体系建设的若干意见》明确指出了要特别重视网络安全的6方面内容；中办、国办印发的《国家2006年至2020年长期科学发展规划》中也突出了对各种网络安全问题的关注，将建设国家信息安全保障体系列为我国信息化发展的战略重点；国家“十一五”计划中也包含了提升国家信息安全保障服务能力的战略要求。西方发达国家纷纷制订了本国的网络与信息安全战略。比如，美国奥巴马政府正在采取措施加强美国网络战的备战能力，其中一项措施是创建网络战司令部，这表明美国的网络与信息安全战略已经由克林顿时代的“全面防御”、布什时代的“攻防结合”，转到奥巴马时代的“攻击为主，网络威慑”。

当前，制约我国网络与信息安全事业发展的瓶颈之一就是人才极度匮乏，为此，教育部从2001年起，陆续批准了包括北京邮电大学在内的近百所各类高校开设信息安全本科专业。但是，毕竟与其他经典的本科专业相比，信息安全本科专业的建设问题还面临许多挑战，需要全国同行共同努力，早日探索出一条办好信息安全专业的捷径。可喜的是，现在国内若干高校的教授团队都纷纷行动起来，各尽所能在信息安全本科专业建设方面取得了不少业绩。比如，灵创团队（http://www.cleader.net）就是众多热心于信息安全本科专业建设的创新团队，该团队中的“信息安全教学团队”被教育部和财政部批准为“2009年度国家级教学团队”；其完成的成果“信息安全专业规范研究与专业体系建设”获得了国家级教学成果奖二等奖；其带头人也被评为“国家级教学名师”并受到了胡锦涛等党和国家领导人的接见。希望国内能够有更多的类似教学团队投身于信息安全本科专业建设。

由于教材建设是信息安全专业建设的重点和难点之一，中国密码学会教育工作委员会自成立以来就一直致力于推进密码学与信息安全方面的教学和教材建设，比如，与国防工业出版社联合主办了“密码学与信息安全教学研讨会”等一系列研讨活动，并成立“普通高等教育本科密码信息安全类系列教材”编审委员会来组织策划相关系列教材。编审委员会在充分研究信息安全本科专业规范的基础上，经过细致研究，多次反复讨论，规划了与信息安全本科专业规范相配套的本系列教材。

本系列教材参照荣获国家级教学成果奖的信息安全最新专业规范，确定教材题目，组织教材书稿内容。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。由于本系列教材涉及的内容比较多，在教材内容选择时，一

方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象；同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能；编审委员会多次召开会议，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”。

为便于高校教师选用本套教材，我们将为高校教师提供完善的教学服务，免费为选用本套教材的教师提供所有教材的电子教案和部分教材的习题答案。同时我们还提供信息安全专业本科教学实验室建设方案与实验教学指导咨询和信息安全专业本科生实习、实训与技能认证咨询。

本系列教材尽管通过反复讨论修改，但限于作者水平和其他客观条件限制，难免存在不足和值得商榷之处，敬请批评指正。

教授　博士生导师　国家级教学名师
灾备技术国家工程实验室主任
网络与信息攻防教育部重点实验室主任
北京邮电大学信息安全中心主任

2009 年 9 月 30 日星期三

高等院校密码信息安全类专业系列教材
编委会名单

顾　问　王　越　（中国科学院院士、中国工程院院士）
方滨兴　（中国工程院院士）
白中英　（北京邮电大学教授、博士生导师）

主　任　杨义先　北京邮电大学

编　委　（按姓氏笔画排序）
马文平　西安电子科技大学
马民虎　西安交通大学
马春光　哈尔滨工程大学
王永滨　中国传媒大学
王景中　北方工业大学
牛少彰　北京邮电大学
孙国梓　南京邮电大学
任　伟　中国地质大学(武汉)
苏盛辉　北京工业大学
吴晓平　海军工程大学
张　伟　南京邮电大学
林柏钢　福州大学
罗守山　北京邮电大学
罗森林　北京理工大学
郑智捷　云南大学
赵俊阁　海军工程大学
秦志光　电子科技大学
贾春福　南开大学
徐茂智　北京大学
蒋文保　北京信息科技大学
游　林　杭州电子科技大学
慕德俊　西北工业大学

此为试读，需要完整PDF请访问：www.ertongbook.com

高等院校密码信息安全类专业系列教材
编委会名单

顾　问　王　越　（中国科学院院士、中国工程院院士）
方滨兴　（中国工程院院士）
白中英　（北京邮电大学教授、博士生导师）

主　任　杨义先　北京邮电大学

编　委　（按姓氏笔画排序）
马文平　西安电子科技大学
马民虎　西安交通大学
马春光　哈尔滨工程大学
王永滨　中国传媒大学
王景中　北方工业大学
牛少彰　北京邮电大学
孙国梓　南京邮电大学
任　伟　中国地质大学(武汉)
苏盛辉　北京工业大学
吴晓平　海军工程大学
张　伟　南京邮电大学
林柏钢　福州大学
罗守山　北京邮电大学
罗森林　北京理工大学
郑智捷　云南大学
赵俊阁　海军工程大学
秦志光　电子科技大学
贾春福　南开大学
徐茂智　北京大学
蒋文保　北京信息科技大学
游　林　杭州电子科技大学
慕德俊　西北工业大学

目　录

第1章　整数和多项式的表示与运算

数论是研究整数性质的一个数学分支，它在密码学与网络安全领域中有着很多重要的应用。本章将学习关于整数和多项式的一些基本知识，如素数与带余除法、最大公因子与辗转相除法、模运算与同余、欧拉定理、多项式的带余除法与辗转相除法。同时还将介绍一些密码学的基本知识，并学习一些基于模运算的古典密码算法。

1.1　素数与带余除法

1.1.1　素数

整除是数论中的基本概念，这里主要介绍与整除相关的一些基本概念及其性质，如整除、因子、公因子、分解因子等，这里将给出这些概念的严格的数学定义。通过掌握这些概念的数学定义及性质，可以解决许多初等数论里与整除相关的问题。这些知识不仅是数论的基础，在密码学中也有很广泛的应用。

大家知道，整数除了加法和乘法之外还可以作减法运算，但是一般不能作除法，由此引出初等数论中的第一个基本概念：数的整除性。

定义　设 a 和 b 是整数，$b\neq 0$，如果存在整数 c 使得 $a=bc$，则称 b 整除 a，表示成 $b\mid a$，并称 b 是 a 的因子，而 a 为 b 的倍数；如果不存在上述的整数 c，则称 b 不整除 a，表示成 $b\nmid a$。

由整除的定义可以导出整除的如下基本性质。

(1) $b\mid b$。

(2) 如果 $b\mid a, a\mid c$，则 $b\mid c$。

(3) 如果 $b\mid a, b\mid c$，则对任意整数 x, y，有 $b\mid(ax+cy)$。

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

(5) 设 $m\neq 0$，那么，$b\mid a\Leftrightarrow mb\mid ma$。

(6) 设 $b\neq 0$，那么，$a\mid b\Rightarrow|a|\leqslant|b|$。

性质(2)的证明：由于 $b\mid a$，根据整除的定义可知，存在 x 使 $a=xb$，同样，存在 y 使 $c=ya$，从而，$c=ya=yxb=(yx)b$，即 $b\mid c$。

其他性质可以采用类似的方法证明。

显然，± 1、$\pm b$ 是 b 的因子，称其为 b 的显然因子；b 的其他因子称为 b 的真因子。

定义　设 p 为大于 1 的整数，如果 p 没有真因子，即 p 的正因子只有 1 和 p 自身，则称 p 为素数，否则称为合数。

定理　素数有无穷多个。

证明：用反证法。假设只有有限个素数，设为 q_1、q_2、…、q_k，考虑数 $a=q_1q_2\cdots q_k+1$，由

于每一个 q_i 均不为 a 的因子，由素数的定义可知，a 为素数，这与假设矛盾，故原定理得证。

将素数从小到大排列，假设 p_n 表示第 n 个素数，$\pi(x)$ 表示不超过 $x(x>0)$ 的素数个数。虽然无法知道 p_n 的确切位置，但是可以得到 p_n 的一个弱上界估计，而对于 $\pi(x)$，也有一个弱下界估计。

定理 将全体素数按从小到大的顺序排列，则第 n 个素数 p_n 与 $\pi(x)$ 分别有以下性质。

(1) $p_n \leqslant 2^{2^{n-1}}, n=1,2,\cdots$。

(2) $\pi(x) \geqslant \log_2(\log_2 x), x \geqslant 2$。

证明：结论(1) 采用归纳法来证明。

当 $n=1$ 时，结论显然成立。假设对于 $n \leqslant k$ 时，结论成立。

当 $n=k+1$ 时，由上述定理知 $p_{k+1} \leqslant p_1 p_2 \cdots p_k + 1$。

因此，$p_{k+1} \leqslant 2^{2^0}2^{2^1}\cdots 2^{2^{k-1}} + 1 = 2^{2^0+2^1+\cdots+2^{k-1}} + 1 = 2^{2^k-1} + 1 < 2^{2^k}$，故结论(1)得证。

结论(2)的证明：$\forall x \geqslant 2$，必存在唯一的整数 n，使 $2^{2^{n-1}} \leqslant x < 2^{2^n}$，由结论(1)知，$\pi(x) \geqslant \pi(2^{2^{n-1}}) \geqslant \pi(p_n) = n > \log_2(\log_2 x)$，结论(2)得证。

素数有以下性质。

(1) 素数有无穷多个。

(2) 设 p 是素数，a、b、$\cdots$、c 是整数，如果 p 整除乘积 $ab\cdots c$，则 a、b、$\cdots$、c 中至少有一个能被 p 整除。

(3)(素数定理)设 $\pi(x)$ 表示不大于 x 的素数的数目，则 $\lim\limits_{x\to\infty}\dfrac{\pi(x)}{x/\ln x}=1$。素数定理表明，对充分大的 x，$\pi(x)$ 可用 $x/\ln x$ 来近似表示。

(4)(算术基本定理)每个大于等于 2 的整数 n，均可分解成素数幂之积：$n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$。若不计因子的顺序，这个分解式是唯一的，其中 $p_i(1 \leqslant i \leqslant k)$ 是不同的素数，$e_i(1 \leqslant i \leqslant k)$ 是正整数。

(5) 如果 a 是一个大于 1 的整数，如果所有 $\leqslant \sqrt{a}$ 的素数都除不尽 a，则 a 是素数。(该性质提供了一种判定素数的方法，是最简单的“筛法”)

可以通过表 1-1 对上述性质(3)做一个直观的理解。

表 1-1 素数定理的直观解释

x	$\pi(x)$	$\left(\frac{x}{\ln x}\right)$的整数部分	$\frac{\pi(x)}{x/\ln x}$
1000	168	145	1.159
10000	1229	1086	1.132
100000	9592	8686	1.104
1000000	78498	72382	1.084
10000000	664579	620241	1.071
100000000	5761455	5428681	1.061
1000000000	50847478	48254942	1.054

此为试读，需要完整PDF请访问：www.ertongbook.com

性质(3),可以用另一种方式叙述:设 $\pi(x)=|\{p|p$ 是素数,且 $p\leqslant x\}|$,则对于足够大的数 x,有 $\pi(x)\approx\frac{x}{\ln x}$。

由以上论述可以得到下面的结论:在正整数 x 范围内的数中,素数出现的概率大约为 $\frac{1}{\ln x}$。

人们还发现,素数的分布是不规则的。随着正整数的增大,素数也越来越稀疏,即:$\lim\limits_{x\to\infty}\frac{\pi(x)}{x}=0$。

在密码学中还会遇到一个与素数有关的问题:素数的检测问题,即素性测试。素性测试指的是判断一个大整数是否为素数。目前的素性测试算法都是概率性的算法,而非确定性的。一种较好的常用素性测试算法是 Miller-Rabin 概率算法,该算法产生的结果几乎肯定是素数。该算法可以这样简单地理解:返回的否定结论一定是正确的,返回的肯定结论的出错概率很低,因此执行多次若均返回肯定结论,则出错的概率会大大降低。

1.1.2 带余除法

初等数论还有一个基本的结论——带余除法定理。

定理 设 a 和 b 是整数,$b>0$,则存在整数 q、r,使下式成立。$a=bq+r$,其中 $0\leqslant r<b$,且整数 q、r 由上述条件唯一决定。

式中:整数 q 称为 a 被 b 除的商;数 r 叫做 a 被 b 除得的余数。以上方法称为带余除法,或欧几里德除法。

证明:先证明唯一性。假设存在另外一对整数 q_1、r_1,满足 $a=bq_1+r_1$,其中 $0\leqslant r_1<b$。将以上两式相减,得 $b(q-q_1)=r_1-r$。

两边取绝对值,$b|q-q_1|=|r_1-r|$。

因为,$0\leqslant r_1,r<b$,则 $0\leqslant|r_1-r|<b$,即 $b|q-q_1|<b$。则有 $q=q_1$,从而 $r=r_1$。

再证存在性。考虑整数序列$\cdots$、$-3b$、$-2b$、$-b$、0、b、$2b$、$3b$、$\cdots$。此时,整数 a 一定位于其中某两个相邻的整数之间,即存在一个整数 q,使 $qb\leqslant a<(q+1)b$,令 $r=a-qb$,则有 $a=bq+r$,其中 $0\leqslant r<b$。

例 证明 x^3 被 9 除之后所得的余数只能是 0、1、8,这里 x 为任意的整数。

证明:由带余除法的知识,只需讨论 x 为 0~8 的数即可。

$0^3=0\times9+0;1^3=0\times9+1;2^3=0\times9+8;$

$3^3=3\times9+0;4^3=7\times9+1;5^3=13\times9+8;$

$6^3=24\times9+0;7^3=38\times9+1;8^3=56\times9+8$。故题目的论述得证。

定理 设给定的正整数 $a\geqslant2$,那么任一正整数 n 必可唯一表示为

$n=r_ka^k+r_{k-1}a^{k-1}+\cdots+r_1a+r_0$。其中整数 $k\geqslant0;0\leqslant r_j\leqslant a-1,(0\leqslant j\leqslant k);r_k\neq0$。这就是正整数的 a 进位表示。

证明:对正整数 n 必有唯一的 $k\geqslant0$,使 $a^k\leqslant n<a^{k+1}$,由带余除法知,必有唯一的 q_0、r_0,满足 $n=q_0a+r_0$,这里,$0\leqslant r_0<a$。

以下对 k 采用数学归纳法。

若 $k=0$,则必有 $q_0=0,1\leqslant r_0<a$,所以结论成立。

假设,当 $k=m\geqslant 0$ 时结论成立。

那么,当 $k=m+1$ 时,上式中的 q_0 满足 $a^m\leqslant q_0<a^{m+1}$。

由假设知:$q_0=s_m a^m+s_{m-1}a^{m-1}+\cdots+s_1 a+s_0$。

式中:$0\leqslant s_j\leqslant a-1,(0\leqslant j\leqslant m-1);1\leqslant s_m\leqslant a-1$。

因而有:$n=s_m a^{m+1}+s_{m-1}a^m+\cdots+s_0 a+r_0$。

即结论对 $m+1$ 也成立,以上定理得证。

本节学习了素数与整数的相关知识,学习了一些与素数个数有关的结论,包括:素数的数量是无限的;素数数量的估计。还学习了带余除法,通过带余除法可以将任意一个正整数用 a 进位来表示。这些知识在密码学中的一些加密算法中都有一定的应用。

1.2 最大公因子与辗转相除法

辗转相除法在数论中有着重要的地位,利用辗转相除法不仅可以求出有限个整数之间的最大公因子,而且可以求出最大公因子用这些整数表示的线性系数。该方法还可以直接用于求解一次不定方程,欧几里德算法在密码学中也有多种应用,并可用于破译或分析某些密码算法。

定义 设 $a,b,\cdots,c$ 是有限个不全为零的整数,同时满足下面两个条件(唯一的)的整数 d 称为它们的最大共因子(或最大公约数),记作$(a,b,\cdots,c)$或 $\mathrm{GCD}(a,b,\cdots,c)$。

(1) d 是 $a,b,\cdots,c$ 的公共约数,即 $d\mid a,d\mid b,\cdots,d\mid c$。

(2) d 是 $a,b,\cdots,c$ 的所有公约数中最大的,即如果整数 d_1 也是 $a,b,\cdots,c$ 的公约数,则 $d_1\leqslant d$。

任意整数 $a,b,\cdots,c$ 必然有公约数(如 ± 1),如果它们不全为零,则易知它们的公约数只有有限多个,所以它们的最大公约数必然存在并且是唯一的。此外,最大公约数一定是正整数。

由于 0 可以被任意整数整除,所以,任一正整数 a 与 0 的最大共因子就是 a 本身。

如果$(a,b,\cdots,c)=1$,则称 $a,b,\cdots,c$ 是互素的。如果 $a,b,\cdots,c$ 中的任意两个都是互素的,则称两两互素。

定理 设 a,b,c 为 3 个正整数,且 $a=bq+c$,其中 q 为整数,则$(a,b)=(b,c)$。

证明:由公约数的定义可知,$(a,b)\mid a,(a,b)\mid b$,又有 $c=a-bq$,因此$(a,b)\mid c$,可以得到$(a,b)\mid(b,c)$;同理可得$(b,c)\mid(a,b)$,因此$(a,b)\mid(b,c)$。

最大公约数有如下性质。

(1) 对于任意整数 x,有:$(a_1,a_2)=(a_1,a_2+a_1x)$。

(2) 设 $m>0$,则 $m(b_1,b_2,\cdots,b_k)=(mb_1,mb_2,\cdots,mb_k)$。

(3) 若$\left(\dfrac{a_1}{(a_1,a_2)},\dfrac{a_2}{(a_1,a_2)}\right)=1$,一般情况下,有$\left(\dfrac{a_1}{(a_1,\cdots,a_k)},\dfrac{a_2}{(a_1,\cdots,a_k)},\cdots,\dfrac{a_k}{(a_1,\cdots,a_k)}\right)=1$。

(4) 设 $a,b,\cdots,c$ 是不全为零的整数,则存在整数 $x,y,\cdots,z$,使

$ax+by+\cdots+cz=(a,b,\cdots,c)$。特别地,如果 $a,b,\cdots,c$ 互素,则存在整数 $x,y,\cdots,z$,使得 $ax+by+\cdots+cz=1$。

(5) 设 $(a,m)=(b,m)=1$,则 $(ab,m)=1$。

(6) 如果 $c\mid ab$,且 $(c,b)=1$,则 $c\mid a$。

例 设 a,b,c 为3个正整数,证明:$\left(\frac{a}{(a,c)},\frac{b}{(b,a)},\frac{c}{(c,b)}\right)=1$。

证明:由最大公因子的定义,有 $\frac{a}{(a,c)}\left|\frac{a}{(a,b,c)},\frac{b}{(b,a)}\right|\frac{b}{(a,b,c)},\frac{c}{(c,b)}\left|\frac{c}{(a,b,c)}\right.$。

故 $\left(\frac{a}{(a,c)},\frac{b}{(b,a)},\frac{c}{(c,b)}\right)\left|\left(\frac{a}{(a,b,c)},\frac{b}{(a,b,c)},\frac{c}{(a,b,c)}\right)\right.$。

又 $\left(\frac{a}{(a,b,c)},\frac{b}{(a,b,c)},\frac{c}{(a,b,c)}\right)=1$,则 $\left(\frac{a}{(a,c)},\frac{b}{(b,a)},\frac{c}{(c,b)}\right)=1$。

对于正整数 a,b,利用上述定理及带余除法,可以求出 a,b 的最大公约数 (a,b),该方法称为辗转相除法,具体步骤如下。

令 $r_0=b,r_1=a,a\leqslant b$,

用 r_1 除 r_0:$r_0=r_1q_1+r_2,0\leqslant r_2<r_1$。

用 r_2 除 r_1:$r_1=r_2q_2+r_3,0\leqslant r_3<r_2$。

……

用 r_{m-1} 除 r_{m-2}:$r_{m-2}=r_{m-1}q_{m-1}+r_m,0\leqslant r_m<r_{m-1}$。

用 r_m 除 r_{m-1}:$r_{m-1}=r_mq_m$。

注意到:$r_0\geqslant r_1>\cdots>r_{m-1}>\cdots\geqslant 0$。

经过有限步上述的带余除法后余数必为零。另一方面,由上述定理知

$$(a,b)=(r_0,r_1)=(r_1,r_2)=\cdots=(r_{m-1},r_m)=(r_m,0)=r_m$$

欧几里德辗转相除法不仅可以求出 (a,b),还可以求出不定方程 $sa+tb=(a,b)$ 的一组整数解,在该表达式中,s、t 是变量,具体做法如下。

由算法的倒数第二行,得到 $(a,b)=r_m=r_{m-2}-r_{m-1}q_{m-1}$,这就将 (a,b) 表示成 r_{m-2},r_{m-1} 的整系数线性组合。再用算法中前面的一行 $r_{m-1}=r_{m-3}-r_{m-2}q_{m-2}+r_m$,代入上式,消去 r_{m-1},得出 $(a,b)=(1+q_{m-1}q_{m-2})r_{m-2}-q_{m-1}r_{m-3}$,即 (a,b) 为 r_{m-2},r_{m-3} 的线性组合,如此进行,最终可得 $(a,b)=sa+tb$。

例 求42823及6409的最大公因子,并将它表示成42823和6409的整系数线性组合形式。

解:采用辗转相除法。$42823=6\times6409+4369,6409=1\times4369+2040,4369=2\times2040+289,2040=7\times289+17,289=17\times17$。

于是有:$(42823,6409)=(6409,4369)=(4369,2040)=(2040,289)=(289,17)=17$。

将上述各式由后向前逐次代入:$17=2040-7\times289$,

$17=2040-7\times(4369-2\times2040)=-7\times4369+3\times2040$,

$17=-7\times4369+3\times(6409-4369)=3\times6409-10\times4369$,

$17=3\times6409-10\times(42823-6\times6409)=-10\times42823+63\times6409$。

这就求出了线性组合形式:$(42823,6409) = -10 \times 42823 + 63 \times 6409$。

例 若$(a,b)=1$,则任一整数n必可表为$n=ax+by$,此时,x、y是整数。

证明:因为$(a,b)=1$,由上述定理知:存在x_0、y_0,使得$ax_0+by_0=1$。故可取:$x=nx_0$,$y=ny_0$。

本节学习了最大公因子的概念与辗转相除法。利用辗转相除法可以计算出任意两个正整数的最大公约数。在计算效率上,辗转相除法具有较高的效率。因此,该方法在密码学中有着应用。比如,在公钥加密算法 RSA 中可以采用辗转相除法来高效地计算私钥。

1.3 模运算与同余

在密码算法中通常会用到模运算,模运算可以将数字的加法、乘法的结果限制在一定的范围内。利用模运算,可以规定两个整数之间的同余关系。欧拉定理是公钥加密算法 RSA 设计的理论基础。本节将学习模运算、同余、欧拉定理等知识。

1.3.1 模运算

模运算的含义是:取得两个整数相除后结果的余数,记作 mod。例如,7mod3 = 1,因为 7 除以 3 商 2 余 1,余数 1 即执行模运算后的结果。

一般地,给定一个正整数p,任意一个整数n,由带余除法知,一定存在等式:$n=kp+r$,其中k、r是整数,且$0 \leqslant r < p$,称k为n除以p的商,r为n除以p的余数。

对于正整数p和整数a、b,定义如下运算为模运算:$a \mod p$表示a除以p的余数。

同样可以定义与模运算相关的一些运算。

模p加法:$(a+b) \bmod p$,其结果是$a+b$的和除以p的余数,也就是说,若$(a+b)=kp+r$,则$(a+b) \bmod p = r$。

模p减法:$(a-b) \bmod p$,其结果是$a-b$除以p的余数。

模p乘法:$(a \times b) \bmod p$,其结果是$a \times b$除以p的余数。

下面,仅以$p=8$为例,给出模 8 加法、模 8 乘法运算表,如表 1-2 和表 1-3 所列。

表 1-2 模 8 加法

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

表 1-3 模 8 乘法

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

由模运算的定义知,模运算满足以下性质。

$(a+b)\bmod p=[(a\bmod p)+(b\bmod p)]\bmod p$

$(a-b)\bmod p=[(a\bmod p)-(b\bmod p)]\bmod p$

$(a\times b)\bmod p=[(a\bmod p)\times(b\bmod p)]\bmod p$

模 p 运算和普通的四则运算有如下类似的运算律。

(1) 结合律:$((a+b)\bmod p+c)\bmod p=(a+(b+c)\bmod p)\bmod p$

$((a\times b)\bmod p\times c)\bmod p=(a\times(b\times c)\bmod p)\bmod p$

(2) 交换律:$(a+b)\bmod p=(b+a)\bmod p$;$(a\times b)\bmod p=(b\times a)\bmod p$

(3) 分配律:$((a+b)\bmod p\times c)\bmod p=((a\times c)\bmod p+(b\times c)\bmod p)\bmod p$

仅以结合律为例做证明:$((a+b)\bmod p+c)\bmod p=(a+(b+c)\bmod p)\bmod p$。

先考虑等式的左边。

假设:$a=k1\times p+r1$;$b=k2\times p+r2$;$c=k3\times p+r3$。

则:$a+b=(k1+k2)p+r1+r2$。

如果 $r1+r2\geqslant p$,则:$(a+b)\bmod p=(r1+r2)-p$;否则,$(a+b)\bmod p=r1+r2$。

再和 c 进行模 p 和运算,结果为 $r1+r2+r3$ 的和除以 p 的余数。

对等式右边进行类似分析,可以得到同样的结果,结合律得证。

1.3.2 同余

同余指的是两个整数之间可能满足的一种关系。如果两个数 a、b 满足 $a \bmod p=b \bmod p$,则称它们同余(或模 p 相等),记作:$a\equiv b \bmod p$。

同余也可以这样叙述,令 3 整数 a,b 及 p,当且仅当 a 与 b 的差为 p 的整数倍时,称 a 在模 p 时与 b 同余,即 $a-b=kp$,其中 k 为任一整数。若 a 与 b 在模 p 中同余,记作:$a\equiv b\bmod p$。

可知:若 a 与 b 在模 p 中同余,则 p 必整除 a 与 b 的差,即 p 整除 $a-b$,用符号可写成 $p|(a-b)$。

需要注意的是,对于同余和模 p 乘法来说,有一个和普通整数中的四则运算不同的规则。在普通整数的四则运算中有这样一个结论:如果 c 是一个非 0 整数,则由 $ac=bc$ 可以得出 $a=b$,即乘法满足消去律。

但是,在模 p 运算中,这种关系不存在,例如,

$(3\times3)\bmod 9=0,(6\times3)\bmod 9=0$。

但是,$3 \bmod 9=3,6 \bmod 9=6$。

即对于同余和模 p 乘法而言,消去律不一定成立。但是,如果增加一些约束条件,消去律也可以成立。

定理(消去律) 如果 $\mathrm{GCD}(c,p)=1$,则 $ac\equiv bc \bmod p$ 可以推出 $a\equiv b \bmod p$。

证明:因为 $ac\equiv bc \bmod p$,所以 $ac=bc+kp$,也就是 $c(a-b)=kp$。

因为 c 和 p 没有除 1 以外的公因子,因此上式要成立必须满足下面两个条件中的一个:①c 能整除 k;②$a=b$。

以下针对条件②,分两种情况讨论。

如果②不成立,则 $c\mid kp$。

因为 c 和 p 没有公因子,因此显然 $c\mid k$,所以 $k=ck'$。

因此,$c(a-b)=kp$ 可以表示为 $c(a-b)=ck'p$。

由:$a-b=k'p$,得出 $a\equiv b \bmod p$。

如果②成立,即 $a=b$,则 $a\equiv b \bmod p$ 显然成立。故得证。

同余关系跟通常意义的相等关系极为相似。在同余的基本运算中,存在以下基本定理。

定理 模的同余关系满足如下性质。

(1) $a=a\bmod n$(自反性)。

(2) 若 $a=b\bmod n$,则 $b=a\bmod n$(对称性)。

(3) 若 $a=b\bmod n$ 且 $b=c\bmod n$,则 $a=c\bmod n$(传递性)。

证明略。

定理 若 $a=b\bmod n$ 且 $c=d\bmod n$,则 $a\pm c=b\pm d\bmod n$,$ac=bd\bmod n$。

证明:因 $a=b\bmod n$,$c=d\bmod n$,所以 $a=kn+b$,$c=hn+d$,故 $a\pm c=(k\pm h)n+(b\pm d)$,从而 $a\pm c=b\pm d\bmod n$。

同理可证:$ac=bd\bmod n$。

定理 若 $ac=bd\bmod n$ 且 $c=d\bmod n$ 及 $(c,n)=1$,则 $a=b\bmod n$。此时,(c,n) 表示 c 和 n 的最大公因子,$(c,n)=1$ 表示 c 与 n 互素。

证明:由 $(a-b)c+b(c-d)=ac-bd=0 \mod n$,可得 $n\mid(a-b)c$。

因为 $(c,n)=1$,故得 $n\mid(a-b)$,因此 $a=b\bmod n$。

(注意:上定理中,若 c 与 n 不互素,则此定理不成立。)

例如,$3\times2=1\times2 \bmod 4$,且 $2=2 \bmod 4$,但 $3\neq1(\bmod 4)$。

定理 若 $ac=bc\bmod n$,$d=(c,n)$,则 $a=b\bmod n/d$。

例如,因 $42=7 \bmod 5$,即 $6\times7=7 \bmod 5$,$d=(c,n)=(7,5)=1$,所以 $6=1 \bmod 5$。

例 求使 2^n+1 能被 3 整除的一切自然数 n。

解:因为 $2\equiv-1(\bmod 3)$,所以 $2^n\equiv(-1)^n(\bmod 3)$。

则 $2^n+1\equiv(-1)^n+1(\bmod 3)$,

因此,当 n 为奇数时,2^n+1 能被 3 整除;

当 n 为偶数时,2^n+1 不能被 3 整除。

此为试读,需要完整PDF请访问: www.ertongbook.com