高等学校网络空间安全专业“十三五”规划教材

信息安全数学基础

主编　常相茂　周玉倩

西安电子科技大学出版社
http://www.xduph.com

高等学校网络空间安全专业“十三五”规划教材

信息安全数学基础

主　编　常相茂　周玉倩

西安电子科技大学出版社

内 容 简 介

本书系统地介绍了与信息安全相关的初等数论、抽象代数和椭圆曲线方面的数学知识，还增加了部分信息安全知识和程序设计内容，将数学知识、信息安全以及应用实践紧密结合起来。本书在内容编排上注重趣味化引导和知识点的实例说明，尽量使学习过程变得轻松有趣。

本书可作为信息安全、计算机科学与技术、通信工程等专业的本科生和研究生的教学用书，也可作为信息安全专业人员的参考用书。

图书在版编目(CIP)数据

信息安全数学基础/常相茂，周玉倩主编. —西安：西安电子科技大学出版社，2019.3
ISBN 978-7-5606-5208-5

Ⅰ. ① 信… Ⅱ. ① 常… ② 周… Ⅲ. ① 信息安全—应用数学—高等学校—教材 Ⅳ. ① TP309 ② O29

中国版本图书馆 CIP 数据核字(2019)第 025235 号

策划编辑 陈 婷
责任编辑 许青青
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西天意印务有限责任公司
版 次 2019 年 3 月第 1 版 2019 年 3 月第 1 次印刷
开 本 787 毫米×960 毫米 1/16 印张 9.5
字 数 147 千字
印 数 1～3000 册
定 价 25.00 元
ISBN 978-7-5606-5208-5/TP
XDUP 5510001-1

高等学校网络空间安全专业“十三五”规划教材

编审专家委员会

前　言

信息技术的广泛应用和网络技术的飞速发展正在全面改变着人们的生产生活方式，深刻影响着人类社会的历史发展进程。信息网络技术带来了信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体以及国家主权的新疆域。与此同时，信息网络技术也给国家政治、经济、社会以及国防安全带来了严峻的安全风险和挑战。在此新形势下，国家对信息安全人才的需求越来越迫切，信息安全人才的舞台正变得越来越精彩。

信息安全是计算机、数学、信息科学等多学科交叉的科学，数学在信息安全中有着重要的地位和作用。在信息安全与密码学的学习和研究中，信息安全模型的建立、密码体制的设计、安全性的证明以与密码体制的形式化分析等涉及数论、抽象代数等数学知识。虽然这些知识有专门的数学教材和课程，但信息安全专业与数学专业对这些知识的侧重点有着较大的差异，信息安全专业更注重数学知识在信息安全方面的应用，而数学专业更注重数学理论的完备性和严谨性，因此，应在内容选取和讲授方法上区别对待，设计专门针对信息安全专业的数学基础教材。

本书选取与信息安全相关的初等数论、抽象代数和椭圆曲线的部分数学知识作为主要内容。每章开始都列举了几个与本章内容相关的趣味问题，引导读者对本章内容产生兴趣，以提高学习的积极性。对书中涉及的概念、性质和方法，设计了大量相关的例题，以降低学习的难度，提高学生对知识的应用能力。除第 1 章作为基础知识外，其余各章均安排了与信息安全直接相关的小节，用于建立数学知识和信息安全知识之间的对应关系，使读者认识到所学数学知识的用武之地。由于信息安全知识一般会有专门的课程讲授，因此这些小节都标记了星号，用于和主体数学内容相区分。在每章都安排了实验环节，用于提高读者的动手能力和对知识的应用能力。在每章的最后还设计了趣味阅读环节(与各章内容相关的趣味数学知识或者数学家的趣味故事)，以进一步提高读者的学习兴趣。为了突出重点，降低学习难度，本书有选择地略去了部分定理较为繁琐的证明过程，学有余力的读者可以自行查阅参考书目或其他相关资料。

本书共6章，分为三大部分。第1～3章介绍整除、同余、同余式、平方剩余、原根和指标等初等数论内容，第4、5章介绍代数系统、群、环和有限域等抽象代数内容，第6章介绍椭圆曲线的内容。建议学习本书的总学时为56学时，授课教师可根据学生情况及教学时间，适当选取课堂讲授内容。

本书得到了“南京航空航天大学研究生教育教学改革研究项目”的支持。

本书由常相茂和周玉倩主编，其中第1～4章由常相茂编写，第5、6章由周玉倩编写。常相茂负责全书的统稿工作。

尽管作者对书稿进行了多次修改和订正，但由于时间仓促和水平有限，书中不当之处在所难免，恳请读者批评指正，并在此先致感谢之意。

作　者

2018年11月

目　录

第 1 章　整数的可除性

在开始本章的学习之前，先考虑如下三个问题：

(1) 3 和 4 的最大公因数是 1，6 和 10 的最大公因数是 2，那么你知道65 539和 4 294 967 299 的最大公因数怎么求吗？

(2) 2、3、5、7 是素数，那么你能找出 10 000 以内的所有素数吗？

(3) 12 可以分解成 3 乘以 4，进一步分解成 3 乘以 2 再乘以 2，那么你知道 1 684 309 也可以分解成素数的乘积吗？

上面的问题都是我们小学时就已经学过的知识，但当处理大整数时就有必要进一步学习了。掌握整除、最大公因数、最小公倍数、整数唯一分解定理、素数等基本概念和性质，掌握求解最大公因数、解二元一次不定方程的一般性方法，是本章的学习目的。

1.1　整除的概念及带余除法

定义 1.1　设 a、b 是任意两个整数，其中 $b\neq 0$，如果存在一个整数 q 使得 $a=bq$，则称 b 整除 a 或 a 被 b 整除，记作 $b\mid a$，此时 b 叫作 a 的因数，a 叫作 b 的倍数。

若使得 $a=bq$ 成立的整数 q 不存在，则称 b 不整除 a，记作 $b\nmid a$。

整除的概念虽然简单，但它是数论的基本概念，后续的学习中将会不断地用到整除的概念和性质。从整除的定义出发，很容易得到如下关于整除的一些性质。

定理 1.1　设 a 是 b 的倍数，b 是 c 的倍数，则 a 是 c 的倍数，即

$$b\mid a,\ c\mid b\Rightarrow c\mid a$$

证　由于 $b\mid a$，$c\mid b$，即存在两个整数 a_1、b_1，使得 $a=a_1b$，$b=b_1c$，因此

$$a=(a_1b_1)c$$

又 a_1b_1 是一个整数，故 $c\mid a$。

定理 1.2 若 m 整除 a，m 整除 b，则 m 整除 $a\pm b$，即

$$m|a,\ m|b\Rightarrow m|a\pm b$$

证 由于 m 整除 a，m 整除 b，即存在两个整数 a_1、b_1，使得 $a=a_1m$，$b=b_1m$，因此

$$a\pm b=(a_1\pm b_1)m$$

又 $a_1\pm b_1$ 是整数，故 $m|a\pm b$。

用同样的方法，可以证明定理 1.3。

定理 1.3 若 $m|a_1$，$m|a_2$，…，$m|a_n$，q_1，q_2，…，q_n 为任意 n 个整数，则

$$m|q_1a_1+q_2a_2+\cdots+q_na_n$$

【例 1.1】 设 n 为任意非零整数，若 $n|93$，$n|92$，则 $n=1$ 或 -1。

证 由 $n|93$、$n|92$ 及定理 1.2 得

$$n|93-92,\ n|92-93$$

即 $n|1$，$n|-1$，而整除 ±1 的非零整数只有 1 或者 -1，因此 $n=1$ 或 -1。

【例 1.2】 设 x、y 为任意整数，若 $17|2x+3y$，则 $17|9x+5y$。

证 由 $17|2x+3y$ 可得

$$17|26x+39y$$

显然

$$17|17x+34y$$

故

$$17|(26x+39y)-(17x+34y)$$

即

$$17|9x+5y\ .$$

当两个整数不是整除关系时，有如下重要的定理。

定理 1.4(带余除法或欧几里德除法) 若 a、b 是两个整数，其中 $b>0$，则存在两个唯一的整数 q 和 r，使得

$$a=bq+r\quad(0\leqslant r<b)\tag{1-1}$$

成立。

证 做整数序列：

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

则 a 在上述序列的某两项之间，即存在一个整数 q，使得

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

成立，令 $a-qb=r$，则 $a=bq+r$，而 $0\leqslant r<b$。

下面证明 q 和 r 的唯一性。

假设 q_1、r_1 是满足式(1-1)的另外两个整数，则 $a=bq_1+r_1$ $(0\leqslant r_1<b)$，因而 $bq_1+r_1=bq+r$，于是 $b(q-q_1)=r_1-r$，故 $b|q-q_1|=|r_1-r|$。由于 r 和 r_1 都是小于 b 的正数，因此上式右边小于 b。如果 $q\neq q_1$，则上式左边 $\geqslant b$。两个结论矛盾，因此，$q=q_1$，$r=r_1$。 □

式(1-1)中的 r 称为非负最小剩余，若要求 $|r|\leqslant b/2$，则定理 1.4 显然依旧成立，此时 r 称为绝对最小剩余。

整除的很多基本性质都可以从定理 1.4 推导出来，可以说本章最主要的部分是建立在定理 1.4 的基础之上的。

显然，我们可以得到如下推论：

推论　若 $a=bq+r$，则 $b|a$ 当且仅当 $r=0$。

该推论是证明 $b|a$ 的一个常用技巧：先假设 $a=bq+r$，推出 $r=0$，则 $b|a$。

【例 1.3】　设 $b=15$，当 $a=-81$ 时，求出带余除法中的 q 和 r。

解　由于

$$-81=-6\times 15+9$$

因此

$$q=-6,\ r=9$$

多项式也可以做类似于整数的带余除法，关于整系数多项式的带余除法，有如下定理：

定理 1.5(整系数多项式的带余除法)　设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ 为 n 次整系数多项式，$g(x)=x^m+b_{m-1}x^{m-1}+\cdots+b_0$ 是首项系数为 1 的 $m(m\geqslant 1)$次整系数多项式，则存在整系数多项式 $q(x)$和 $r(x)$，使得 $f(x)=g(x)q(x)+r(x)$，其中 $r(x)$的次数小于 $g(x)$的次数。

证　若 $n<m$，取 $q(x)=0$，$r(x)=f(x)$即可。

若 $n\geqslant m$，对 $f(x)$的次数 n 作数学归纳法：

$n=m$ 时，令 $q(x)=a_n$，$r(x)=f(x)-a_ng(x)$即为所求。

假设 $n\leqslant m+k$ 时成立，对于 $n=m+k+1$，做如下多项式减法：

$$f(x)-a_nx^{n-m}g(x)=(a_{n-1}-a_nb_{m-1})x^{n-1}+\cdots+(a_{n-m}-a_nb_0)x^{n-m}+a_{n-m-1}x^{n-m-1}+\cdots+a_1x+a_0$$

可以看出，$f(x)-a_nx^{n-m}g(x)$是次数小于等于 $m+k$ 的多项式，由

数学归纳法得

$$f(x)-a_n x^{n-m}g(x)=g(x)q_1(x)+r_1(x)$$

其中，$r_1(x)$的次数小于$g(x)$的次数。令$q(x)=a_n x^{n-m}+q_1(x)$，$r(x)=r_1(x)$，则有

$$f(x)=g(x)q(x)+r(x)$$

根据归纳假设，结论成立。□

由上述定理得知，整系数多项式要做带余除法，被除的多项式$g(x)$的首项系数必须为1，若多项式的系数都为实数，则不需要这个要求。

【例1.4】 求x^3+2x^2+1除以x^2+5所得的余式。

解

$$x^3+2x^2+1=(x^2+5)\cdot x+2x^2-5x+1$$
$$2x^2-5x+1=(x^2+5)\cdot 2+(-5x-9)$$

故

$$x^3+2x^2+1=(x^2+5)\cdot(x+2)+(-5x-9)$$

余式为$-5x-9$。

1.2 最大公因数和辗转相除法

有了带余除法，就可以着手学习确定整数的最大公因数是否存在及其实际求法了，在此之前，需要先学习最大公因数的定义及其性质。

定义1.2 设$a_1, a_2, \cdots, a_n$是$n(n\geqslant 2)$个整数，若整数d是它们之中每个数的因数，那么d就叫作$a_1, a_2, \cdots, a_n$的一个公因数。整数$a_1, a_2, \cdots, a_n$的公因数中最大的一个叫作最大公因数，记作$(a_1, a_2, \cdots, a_n)$。若$(a_1, a_2, \cdots, a_n)=1$，则说$a_1, a_2, \cdots, a_n$互质或互素；若$a_1, a_2, \cdots, a_n$中任意两个数都互质，则说它们两两互质。

显然，$(a_1, a_2, \cdots, a_n)=(|a_1|, |a_2|, \cdots, |a_n|)$，因此，在求整数的最大公因数时，只需求对应正整数的最大公因数即可。

定理1.6 若b是任一正整数，则

(1) 0与b的公因数都是b的因数，b的因数也都是0与b的公因数；

(2) $(0, b)=b$。

证 (1) 显然，0与b的公因数就是b的因数，由于任何非零整数都是0的因数，因此b的因数也就是0与b的公因数。

(2) 由于b的最大因数是b，而0与b的最大公因数是b的最大因数，

因此$(0, b)=b$。 □

定理 1.7　设 a、b、c 是任意三个不全为 0 的整数，且 $a=bq+c$，其中 q 是非零整数，则 a、b 与 b、c 有相同的公因数，因而$(a, b)=(b, c)$。

证　设 d 是 a、b 的任一公因数，由定义得，$d|a$，$d|b$，由定理 1.3 得，d 是 $c=a+(-q)b$ 的因数，因而 d 是 b、c 的一个公因数。——采用同法可证 b、c 的任一公因数是 a、b 的一个公因数，于是定理的前一部分获证。第二部分显然随之成立。 □

由定理 1.6 与定理 1.7，我们可以得到一种求最大公因数的一般性方法，即辗转相除法(又称欧几里德算法)。除了求最大公因数外，辗转相除法还可以推出最大公因数的一些重要性质，也是解一次不定方程的基本工具。下面具体介绍辗转相除法。

设 a、b 是任意两个正整数，由带余除法，有下列等式：

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ \vdots & \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} + r_{n+1} & r_{n+1} = 0 \end{cases} \tag{1-2}$$

由于 r_i 不断减小，因此总可以得到一个余数是零的等式，即 $r_{n+1}=0$。

定理 1.8　若 a、b 是任意两个正整数，则$(a, b)=r_n$。

证　由定理 1.6 和定理 1.7 得

$$\begin{aligned} r_n &= (0, r_n) = (r_{n+1}, r_n) = (r_n, r_{n-1}) \\ &= \cdots = (r_1, b) = (a, b) \end{aligned}$$ □

在利用式(1-2)求最大公因数时，为了简化求解过程，也可以要求带余除法中的余数为绝对最小剩余，此时 a、b 的最大公因数为 r_n 的绝对值。

【例 1.5】　计算(543, 21)。

解

$$543=21\times25+18$$
$$21=18+3$$
$$18=3\times6+0$$

所以(543, 21)=3。

注：实际计算中，可以根据需要在每一步带余除法中使用绝对最小余数或非负最小余数，如例 1.5 中使用绝对最小余数，则计算步骤为

$$543=21\times 26-3$$

$$21=3\times 7+0$$

显然，采用绝对最小余数比使用非负最小余数的计算步骤要少一些。

【例 1.6】 计算(1859，1573)。

解

$$1859=1573\times 1+286$$

$$1573=286\times 5+143$$

$$286=143\times 2+0$$

所以(1859，1573)=143。

推论 a、b 的公因数与(a, b)的因数相同。

证 设 d 是a、b 的任一公因数，则 $d|a$，$d|b$，由式(1-2)中第一式可知，$d|a-bq_1$，即 $d|r_1$。同理，由式(1-2)中第二式可知，$d|r_2$。如此继续下去，最终得到 $d|r_n$，即 $d|(a, b)$。

设 h 为(a, b)的任一因数，则 $h|(a, b)$，由整除的传递性知，$h|a$，$h|b$，故 h 是a、b 的公因数。

综上所述，a、b 的公因数与$(a$、$b)$的因数相同。 □

两个以上整数的最大公因数怎么求呢？

设 a_1，a_2，…，a_n 是任意n 个整数，令$(a_1, a_2)=d_2$，$(d_2, a_3)=d_3$，…，$(d_{n-1}, a_n)=d_n$，于是有如下结论：

定理 1.9 若 a_1，a_2，…，a_n 是任意n 个整数，则$(a_1, a_2, \cdots, a_n)=d_n$。

证 $d_n|a_n$，由 $d_n|d_{n-1}$，$d_{n-1}|a_{n-1}$，$d_{n-1}|d_{n-2}$ 可得 $d_n|a_{n-1}$，$d_n|d_{n-2}$，由此类推，最后得到$d_n|a_n$，$d_n|a_{n-1}$，…，$d_n|a_1$，即 d_n 是a_1，a_2，…，a_n 的一个公因数。又设 d 是a_1，a_2，…，a_n 的任一个公因数，则 $d|a_1$，$d|a_2$，由上述推论知，$d|d_2$，同理可得 $d|d_3$，由此类推，最后得到 $d|d_n$，因而 $d\leqslant d_n$。故

$$(a_1, a_2, \cdots, a_n)=d_n$$ □

【例 1.7】 计算最大公因数(120，150，210，35)。

解

$$(120, 150)=(120, 30)=30$$

$$(30, 210)=30$$

$$(30, 35)=(30, 5)=5$$

所以

$$(120, 150, 210, 35)=5$$

1.3　整除的进一步性质及最小公倍数

由式(1-2)可得，$r_n=r_{n-2}-r_{n-1}q_n$，$r_{n-1}=r_{n-3}-r_{n-2}q_{n-1}$，于是

$$r_n=r_{n-2}(1+q_nq_{n-1})-r_{n-3}q_n$$

再将 $r_{n-2}=r_{n-4}-r_{n-3}q_{n-2}$ 代入上式，如此继续下去，最后可得 $r_n=sa+tb$，其中 s 和 t 是两个整数，于是有如下结论：

定理 1.10　若 a、b 是任意两个正整数，则存在两个整数 s 和 t，使得

$$(a,b)=sa+tb$$

【例 1.8】　用辗转相除法求 $a=288$，$b=158$ 的最大公因数和 s、t，使得 $(a,b)=sa+tb$。

解　因为

$$288=158\times2-28$$
$$158=28\times6-10$$
$$28=10\times3-2$$
$$10=2\times5$$

所以

$$(a,b)=2$$

再由

$$\begin{aligned}2&=10\times3-28=(28\times6-158)\times3-28\\&=28\times17-158\times3\\&=(158\times2-288)\times17-158\times3\\&=31\times158-17\times288\end{aligned}$$

可得 $s=31$，$t=-17$。

定理 1.11　设 a、b 是任意两个不全为零的整数。

(1) 若 m 是任一正整数，则 $(am,bm)=(a,b)m$；

(2) 若 δ 是 a、b 的任一公因数，则 $\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{|\delta|}$，特别地，$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$。

证　当 a、b 有一个为 0 时，定理显然成立。现设 a、b 都不为零，又由于任意两个整数的最大公因数必为正数，因此不妨设 a、b 都为正整数。

(1) 在式(1-2)中，把各式两边同时乘以 m，再由定理 1.8 即得

$$(am, bm)=r_n m=(a, b)m$$

(2) 因为

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right)|\delta|=\left(\frac{|a|}{|\delta|}|\delta|, \frac{|b|}{|\delta|}|\delta|\right)$$
$$=(|a|, |b|)=(a, b)$$

所以

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right)=\frac{(a, b)}{|\delta|}$$ □

定理 1.12 若 a、b、c 是三个整数，$(a, c)=1$，则

(1) ab、c 与 b、c 有相同的公因数；

(2) $(ab, c)=(b, c)$。

证 (1) 由题设及定理 1.9 可知，存在两个整数 s 和 t 满足等式：

$$as+ct=1$$

两边乘以 b，即得

$$(ab)s+c(bt)=b$$

设 d 是 ab 与 c 的任一公因数，由上式及定理 1.3 可得，$d|b$，因而 d 是 b、c 的一个公因数。反之，b、c 的任一公因数显然是 ab、c 的一个公因数，故(1)获证。

(2) 由(1)即知$(ab, c)=(b, c)$。 □

推论 若 $c|ab$，$(a, c)=1$，则 $c|b$。

证 由定理 1.12 知：

$$(b, c)=(ab, c)=|c|$$

故 $|c||b$，因而 $c|b$。 □

【例 1.9】 证明两个整数 a、b 互质的充分与必要条件是：存在两个整数 s 和 t 满足条件

$$as+bt=1$$

证 由定理 1.10 知，必要性成立。

下面证明充分性：设$(a, b)=d$，则 $d|a$，$d|b$，故 $d|as+bt$，而 $as+bt=1$，因此 $d=1$，即 a、b 互质。

定义 1.3 设 a_1，a_2，…，a_n 是 $n(n\geqslant 2)$个整数，若整数 m 是它们之中每个数的倍数，那么 m 就叫作 a_1，a_2，…，a_n 的一个公倍数。整数 a_1，a_2，…，a_n 的一切公倍数中的最小正数叫作最小公倍数，记作$[a_1$，

$a_2, \cdots, a_n]$。

因为乘积$|a_1||a_2|\cdots|a_n|$就是$a_1, a_2, \cdots, a_n$的一个公倍数，所以最小公倍数是存在的。

由于任何正整数都不是 0 的倍数，因此讨论整数的最小公倍数时，总是假定这些整数都不是 0。

和最大公因数一样，有$[a_1, a_2, \cdots, a_n]=[|a_1|, |a_2|, \cdots, |a_n|]$，所以只需对正整数讨论它们的最小公倍数。

我们先讨论两个正整数的最小公倍数。

定理 1.13　设 a、b 是任意两个正整数，则

(1) a、b 的所有公倍数就是$[a, b]$的所有倍数；

(2) $[a, b]=\dfrac{ab}{(a, b)}$。

证　设 m 是 a、b 的任一公倍数，由定义可设

$$m=ak=bk'$$

令 $a=a_1(a, b)$，$b=b_1(a, b)$，由上式即得

$$a_1k=b_1k'$$

由于$(a_1, b_1)=1$，因此由定理 1.12 的推论知，$b_1|k$，故

$$m=ak=ab_1t=\frac{ab}{(a, b)}t$$

其中，t 满足等式 $k=b_1t$。

反过来，当 t 为任一整数时，$\dfrac{ab}{(a, b)}t$ 为 a、b 的一个公倍数。

故 $m=\dfrac{ab}{(a, b)}t$ 可以表示 a、b 的一切公倍数，令 $t=1$，即得到最小的正数，因此$[a, b]=\dfrac{ab}{(a, b)}$，即(2)获证。

又 $m=\dfrac{ab}{(a, b)}t$，(1) 亦获证。　□

现在讨论两个以上整数的最小公倍数。设 $a_1, a_2, \cdots, a_n$ 是 $n(n\geqslant 2)$ 个正整数，令$[a_1, a_2]=m_2$，$[m_2, a_3]=m_3$，$\cdots$，$[m_{n-1}, a_n]=m_n$，于是有：

定理 1.14　若 $a_1, a_2, \cdots, a_n$ 是 $n(n\geqslant 2)$ 个正整数，则

$$[a_1, a_2, \cdots, a_n]=m_n$$

证　由于