普通高等学校信息与计算科学专业系列丛书

教育科学“十五”国家规划课题研究成果

代数与通信

冯克勤　刘凤梅　编著

高等教育出版社
HIGHER EDUCATION PRESS

普通高等学校信息与计算科学专业系列丛书

教育科学“十五”国家规划课题研究成果

代数与通信

冯克勤　刘凤梅　编著

高等教育出版社

内容提要

本书包括两部分。第一部分为有关数学知识，内容包括初等数论和抽象代数。初等数论讲述整除性、同余式、原根与指数等本课程所需内容；抽象代数主要讲述有限交换群、多项式环和有限域。第二部分讲述数论、代数和组合学在通信中的一些主要应用，包括广义布尔函数和它的有限傅里叶变换、移位寄存器序列、纠错码和信息安全。

本书可作为高等学校数学系信息专业本科生和计算机与通信系本科生或研究生的专业基础课或选修课教材或参考书。

图书在版编目(CIP)数据

代数与通信/冯克勤，刘凤梅编著. —北京：高等教育出版社，2005.5

ISBN 7-04-016629-1

Ⅰ.代… Ⅱ.①冯…②刘… Ⅲ.代数-应用-通信-高等学校-教材 Ⅳ.TN91

中国版本图书馆 CIP 数据核字(2005)第 024377 号

出版发行	高等教育出版社	购书热线	010-58581118
社　　址	北京市西城区德外大街 4 号	免费咨询	800-810-0598
邮政编码	100011	网　　址	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
经　　销	北京蓝色畅想图书发行有限公司	网上订购	http://www.landraco.com
印　　刷	北京人卫印刷厂		http://www.landraco.com.cn
开　　本	787×960　1/16	版　　次	2005 年 5 月第 1 版
印　　张	15.5	印　　次	2005 年 5 月第 1 次印刷
字　　数	280 000	定　　价	19.70 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　16629-00

前　言

20世纪中期数字计算机的出现和数字通信的飞速发展，对于人类社会和生活影响巨大，计算机科学和通信技术的进步不仅得益于数学，而且也促进了数学的发展。计算和通信的数字化之前，所用的数学工具主要是以傅里叶分析和拉普拉斯变换为代表的解析方法。数字化之后则更多地采用初等数论、代数（包括线性代数和近世代数）和组合学方法，近年来甚至使用了代数几何、代数数论、群表示论等更高深的数论与代数知识，这对于信息科学产生了深刻的影响。目前在日本、印度、澳大利亚及欧美许多国家，数论和代数已成为计算机专家和通信工程师从事研究和开发不可缺少的数学工具，是促使通信技术重大变革和原创性研究的基本推动力之一。

中国的计算机科学和信息技术正在快速地发展。信息科学技术和产业领域不仅需要大量技术人才，也需要受过良好训练的数学人才。但是就整体而言，中国高等学校的数学教育在代数方面是不充分的。线性代数作为必修课程情况好一些，近世代数在多数学校仅为选修课，学生在学过之后往往不能将其成为自己今后从事研究和工作的工具。开设初等数论的学校则更少，而数论课本在接触近世代数之前就应学习的（中学生也可学点数论），因为数论中的整除性、因子分解、同余类、原根与指数、线性代数中的向量空间和线性映射是近世代数中许多抽象代数结构和概念（如有限交换群、唯一因子分解整环、有限域、生成元和元素的阶、同态和同构等）的具体模型和样板。

本书是为准备投身于信息技术和计算机科学领域的高年级大学生而编写的。内容为两部分：一部分是讲述信息技术和计算机科学中所需的数论和代数学基本知识，另一部分是介绍这些数学知识在一些信息科学领域的应用。主要目的是为学生在以后的信息技术和计算机科学领域工作中打下良好的数学基础，希望他们喜欢这些数学，至少不怕它们，同时对这些数学在信息领域应用的一些方面有一个概括的了解。我们相信，具有良好数学修养的年轻人在我国信息事业中将会发挥重要而特有的作用。

就本书内容而言，涉及数学和信息两大领域。数学方面包括初等数论、线性代数和近世代数，而信息方面则涉及到纠错码的代数理论、布尔函数和序列分析、现代密码学和信息安全。要详细论述每个论题都需要专门的课程。所以我们只讲述在信息领域工作所需的最基本的数论和代数知识，对于这些数学知识

在信息科学中的应用也只作起步性的介绍。本书不涉及当前信息领域研究前沿所需的更高深的数论和代数知识(代数数论、代数几何、群表示理论),也不涉及信息科学在新世纪的一些新兴领域(如量子通信和量子计算)。但是,对于有志于攀登当今信息科学和技术高峰的年轻学子,本书介绍的数学是不可逾越的基础。

本书第一部分介绍数学知识。我们假定读者系统地学过线性代数,本书中将自由地使用线性代数的一些基本结果、概念和技巧,这些结果、概念和技巧不仅对于实数域和复数域上的向量空间适用,而且在任意域上也适用。事实上,我们今后主要讲述有限域上的向量空间和线性变换。我们也假定读者学过近世代数,知道什么是群、环、域。本书中复习近世代数基本概念时,重点介绍有限交换群、多项式环和有限域。许多结果略去证明,但是作了一些解释并举例说明,希望这对于学过近世代数的读者也能有益。由于不少学校不开设初等数论的课程,我们先讲初等数论,它对于进一步学习近世代数和通信中的应用是基本的和重要的,所以在讲数论时采用了比较代数化的方式。一些结果的证明只作些提示,补足证明是一个很好的训练。另一些结果则讲述证明,部分原因是由于这些结果的重要性,更重要的原因是这些证明对理解概念有益,或者体现该学科中的思考方式。每节后面有不少习题,它们对于深入理解所学的概念和结果是重要的。

本书第二部分讲述数论和代数(以及组合学)在通信中的应用。半个多世纪以来,这种应用是非常广泛而且也非常深刻的。我们挑选有以下一些内容:

(1) 布尔函数和有限傅里叶变换。就像通常傅里叶变换是分析连续信号频谱的基本工具一样,有限傅里叶变换是分析脉冲(或叫离散)信号的基本工具。我们将介绍通信中要求的布尔函数各种性质(平衡性、相关免疫性、自相关性、非线性性等),给出构造具有良好性能布尔函数的数论和组合方法。

(2) 移位寄存器序列(更数学化的名称是有限域上的递归序列),主要讲述线性情形,但也涉及非线性情形。重点介绍同步通信中采用的 m 序列和流密码中广泛采用的 M 序列。线性移存器序列的数学工具是线性代数,但在本书中我们使用有限域上的多项式理论和形式幂级数环,因为根据多年经验,后一种讲述方式更为直接和易于应用,更便于为读者接受。非线性移存器序列的数学工具为组合学与图论。

(3) 纠错码的代数理论。这是迄今为止在通信中最系统的数学理论,也是数学应用最充分的一个领域。它要解决的问题是通信的可靠性(纠错)。我们介绍纠错码理论的主要数学问题,并介绍一些重要的纠错码和译码算法。

(4) 公钥系统和信息安全。公钥系统是现代密码学的核心。本书介绍公钥系统的基本思想和两种最重要的体制(大数分解和离散对数),讲述它们用于加

密、数字签名、密钥管理(包括密钥分配、交换和共享)等方面的简单例子和安全性分析。

对于本书的大部分内容,作者从1974年起在中国科学技术大学、中国科学院研究生院和清华大学为大学生、研究生以及为应用部门的学员讲授过多次(其中代数几何码、量子纠错码、认证码、椭圆曲线算法和数域筛法等则属于研究生课程和讨论班内容,未列入本书)。由于读者对象不同,每次讲授的方式和侧重面也有所不同。现在作为高等学校数学系信息专业的选修课,在内容的取舍和深度方面是否合适,还需教学实践的进一步考验。对于数论和代数修养较好的学生,有可能一学期讲完(可以挑选部分内容),一般情形则需要两个学期。讲授时可以按本书次序先讲数学再讲应用,也可直接讲通信应用,同时将所需数学知识穿插其中。我们诚挚地欢迎来自老师、同学和各方面人士的批评和建议,以便将来修改得更加完善和适用。

冯克勤,刘凤梅

2003年于清华

目　录

第一部分　数论与代数

第二部分　通信应用

第一部分

数论与代数

第 I 章
初等数论

初等数论是研究整数性质和不定方程(组)整数解(和有理数解)的一门学问,它与几何学是最古老的两个数学分支.数论起源于三千多年以前的世界文明古国(埃及、巴比伦、印度、中国),中国古代数论成就以勾股定理($x^2+y^2=z^2$的正整数解)、中国剩余定理和祖冲之的疏率和密率(用有理数$\frac{22}{7}$和$\frac{355}{113}$逼近圆周率)而闻名于世,现代中国数论成就以陈景润关于哥德巴赫问题的工作为代表.公元前300年至公元300年,古希腊的数论取得辉煌的理性发展(带余除法、唯一因子分解定理、素数的无穷性、$x^2+y^2=z^2$全部正整数解,……).近代数论兴起于17世纪,法国是18世纪的世界数论中心(代表人物有费马、拉格朗日、勒让德、拉普拉斯.只有欧拉不是法国人),19世纪的数论中心转到德国(代表人物有高斯、戴德金、狄利克雷、黎曼、希尔伯特).费马在17世纪提出的一系列数论猜想对数论发展起了很大的推动作用.正是这些猜想促使欧拉和高斯等人系统研究整数的性质,到18世纪末,他们建立了完整的初等数论,并且解决了费马几乎所有的猜想,唯一未解决的是"$n\geqslant 3$时,$x^n+y^n=z^n$没有正整数解".20世纪以来数论一直是十分活跃的研究领域并且不断取得丰富成果.一个重大标志是怀尔斯于1994年证明了费马猜想.另一个标志是2002年在北京举行的国际数学家大会上,获得菲尔兹数学奖的两位年轻人都主要基于数论的成就.

数论被高斯称为"数学的皇后".20世纪中期以来,数论又成为科学与技术的"仆人".特别在计算机和信息科学技术领域,数论与代数、组合学等离散性数学一起发挥愈来愈大的作用.本书只介绍与通信领域直接相关的初等数论知识.除了二元一次不定方程之外,本书完全不涉及不定方程整数解问题,尽管整数解和有理数解问题是数论发展的最重要和永恒的动力.此外,我们在讲述数论时,更着重以"代数"的方式和视野,这对于理解近世代数(第二章)是有益的.

§1.1 整除性和唯一因子分解

A. 整除性

我们今后用$\mathbb{Z}$表示整数集合.整数之间可进行加、减、乘运算,加法和乘法满

足结合律和交换律,加法和乘法之间还有分配律. 这样的数学结构在近世代数中称为(交换)环,所以$\mathbb{Z}$也叫做是整数环.

整数范围内除法不一定可进行. 即若a,b为整数,$a\neq0$,则$\frac{b}{a}$不一定为整数. 这就引发出初等数论中第一个重要概念:整除性.

定义 1.1.1 设$a,b\in\mathbb{Z}$,$a\neq0$. 如果存在$c\in\mathbb{Z}$,使得$b=ac$(即$\frac{b}{a}\in\mathbb{Z}$)则称a整除b,表示成$a\mid b$,并且称a为b的一个因子(或约数),而b叫a的倍数. 如果$\frac{b}{a}$不是整数,称a不整除b,表示成$a\nmid b$.

以下是关于整除性的最基本性质(对于$x\mid y$,均指$x,y\in\mathbb{Z}$并且$x\neq0$)

引理 1.1.2 (1) 若$a\mid b,b\mid c$,则$a\mid c$.

(2) $a\mid b$并且$b\mid a\Leftrightarrow a=\pm b$.

(3) 若$a\mid b,a\mid c$,则对任意$x,y\in\mathbb{Z}$,均有$a\mid bx+cy$.

□

定义 1.1.3 对于实数α,用$[\alpha]$表示不超过α的最大整数,叫做α的整数部分,而$\alpha-[\alpha]$叫做α的分数部分,表示成$\{\alpha\}$. 于是,每个实数α唯一表示成

$$\alpha=[\alpha]+\{\alpha\},[\alpha]\in\mathbb{Z},0\leqslant\{\alpha\}<1.$$

例如:$[\pi]=3,[2.1]=2,\{2.1\}=0.1,[-2.1]=-3,\{-2.1\}=0.9$.

下面关于整数的性质是在中学就学过的,起始于公元前3世纪欧几里得时代,作为初等数论的出发点.

定理 1.1.4(带余除法) 设$a,b\in\mathbb{Z}$,$b\geqslant1$,则存在唯一确定的整数q(商)和r(余数),使得

$$a=qb+r,0\leqslant r<b.$$

事实上,$q=\left[\frac{a}{b}\right]$.

□

作为带余除法的一个直接应用,我们证明整数集合的一个重要性质.

引理 1.1.5 设S是一个整数非空集合,并且满足以下两个条件

(A) 若$a,b\in S$,则$a\pm b\in S$;

(B) 若$a\in S$,则对每个整数x,均有$ax\in S$,

则存在唯一的整数$d\geqslant0$,使得S是由d的所有倍数构成的,即

$$S=d\mathbb{Z}=\{dy:y\in\mathbb{Z}\}.$$

证明 若$S=\{0\}$,则取$d=0$即可. 以下设S包含非零整数a. 由条件(A)知$0=a-a\in S$,于是$-a=0-a\in S$,所以S中必包含正整数(a和$-a$两者之一).

令 d 是集合 S 当中最小的正整数，我们来证 $S=d\mathbb{Z}$. 首先，由 $d\in S$ 和条件(B)可知 $d\mathbb{Z}\subseteq S$，进而对 S 中每个整数 a，我们有带余除法

$$a=qd+r,\quad q,r\in\mathbb{Z},\quad 0\leqslant r<d.$$

由 $a,d\in S$ 和条件(A)，(B)可知 $r=a-qd\in S$. 但是 $0\leqslant r<d$ 而 d 是 S 中最小正整数，可知 $r=0$. 这表明 $a=qd\in d\mathbb{Z}$，因此 $S\subseteq d\mathbb{Z}$. 这就表明 $S=d\mathbb{Z}$. 最后，满足 $S=d\mathbb{Z}$ 的正整数 d 必然是 S 中最小的正整数，从而是唯一的.

□

定义 1.1.6 设 p 是大于 1 的整数，如果 p 的正因子只有 1 和 p，称 p 为素数(prime number，也叫质数).

例：2,3,5,7,11,13,17,19,…都是素数. 100 以内共有 25 个素数，应当记住.

定理 1.1.7(欧几里得) 素数有无穷多个.

证明 用反证法(这也可能是历史上第一次用反证法). 首先，素数是存在的. 进而，假若只有有限多素数 $p_1,p_2,\cdots,p_s(s\geqslant 1)$，考虑正整数 $n=p_1\cdot p_2\cdot\cdots\cdot p_s+1\geqslant 2$，则 n 必有素因子 p. 但是 $p_1,p_2,\cdots,p_s$ 均不能整除 n，从而 p 是 $p_1,p_2,\cdots,p_s$ 以外的素数. 这导致矛盾. 所以假设不成立，即素数有无限多个.

□

关于素数有许多有趣的问题，其中不少问题至今未解决. 这里列举几个.

(i) **素数判定** 给了一个正整数 n，如何判定它是否为素数？根据定义，若 $2,3,\cdots,n-1$ 均除不尽 n，则 n 为素数. 但是当 n 很大时，这个算法太花时间. 历史上，人们不断地寻求素数判定的更好算法. 特别是近年来，通信中需要使用大素数(例如 100 位左右的素数)，于是这件事受到更大的关注. 2002 年 8 月印度数学家第一次得到素数判定的“多项式”算法(即判别 n 是否为素数，该算法所花的时间是 $\log_2 n$ 的多项式数量级). 在计算复杂性理论中，这表明素数判定问题是不困难的.

(ii) **哥德巴赫问题** 1742 年，普鲁士驻俄国公使哥德巴赫(Goldbach)给欧拉的信中提出猜想：每个大于 2 的偶数均可表成两个素数之和. 这个问题至今未能解决. 目前最好结果是由陈景润证明的：每个充分大的偶数均可表成 $p+p'$，其中 p 为素数，p' 是素数或两个素数之积.

(iii) **孪生素数**(twin primes) 若 n 和 $n+2$ 均为素数，称 $\{n,n+2\}$ 为孪生素数对. 例如 $\{3,5\},\{5,7\},\{11,13\},\{17,19\}$ 等. 人们猜想有无限多个孪生素数对，但这个猜想至今仍未得到证明.

(iv) **素数的分布** 孪生素数猜想是说，有无穷多彼此相距为 2 的素数对. 另一方面，对每个大整数 n，总有连续 n 个正整数均不为素数(如 $(n+1)!+2,(n+1)!+3,\cdots,(n+1)!+n+1$). 这表明素数在正整数中的分布很不规则. 我们以 $\pi(n)$ 表示不超过 n 的正整数中素数的个数. 例如 $\pi(10)=4,\pi(100)=$

25. 素数有无限多个这件事可表成

$$\lim_{n\to\infty}\pi(n)=+\infty.$$

不超过 n 的所有正整数共有 n 个. 所以素数在正整数中的比例为$\frac{\pi(n)}{n}$. 可以证明

$$\lim_{n\to\infty}\frac{\pi(n)}{n}=0.$$

这表明素数在正整数中的分布是“稀疏”的. 进而可以证明

$$\lim_{n\to\infty}\frac{\pi(n)}{\frac{n}{\ln n}}=1 \quad (\text{素数定理}).$$

塞尔贝格给出了它的初等证明(即不用微积分的证明),获了 1950 年菲尔兹数学奖.

1. 若 n 为奇数,证明 $8\mid n^2-1$.

2. 若 n 为奇数并且 $n\geqslant 5$,则 $n\left|\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n-1}\right)(n-1)!\right.$.

3. 若 m 和 n 是正整数,$m\geqslant 3$,证明 $2^m-1\nmid 2^n+1$.

4. 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 为实数($n\geqslant 2$),证明

$$[\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]\leqslant[\alpha_1+\alpha_2+\cdots+\alpha_n]\leqslant[\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]+n-1.$$

$$[2\alpha_1]+[2\alpha_2]\geqslant[\alpha_1]+[\alpha_2]+[\alpha_1+\alpha_2].$$

5. 设 n 为大于 1 的整数,证明

(1) $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$不是整数.

(2) $1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$不是整数.

6. 证明

(1) 形如 $4m+3(m\in\mathbb{Z})$ 的素数有无限多个.

(2) 形如 $6m+5(m\in\mathbb{Z})$ 的素数有无限多个.

7. 设 $n\geqslant 2$ 为正整数. 如果 n 没有小于等于$\sqrt{n}$的素数因子,则 n 为素数.

B. 最大公因子和最小公倍数

设 $a_1,a_2,\cdots,a_n(n\geqslant 2)$ 是不全为零的整数,则它们的公因子(公约数)只有有限多个,其最大公因子表示成$(a_1,a_2,\cdots,a_n)$(必为正整数). 如果$(a_1,a_2,\cdots,a_n)=1$,称这组整数是互素的.

类似地,设 $a_1,a_2,\cdots,a_n$ 均是非零整数,则它们有正的公倍数(例如 $|a_1a_2\cdots$

$a_n \neq 0$). 从而存在最小正公倍数,简称最小公倍数,表示成$[a_1, a_2, \cdots, a_n]$.

以下是最大公因子的一些基本性质(我们只叙述两个整数的情形,不难推广到一般情形).

引理 1.1.8 设 a 和 b 是不全为零的整数,则

(1) $(a,b) = (b,a), (a,b) = (|a|, b)$.

(2) 当 $a \neq 0$ 时,$(a,a) = |a|$.

(3) 对任意整数 l,$(a,b) = (a, b+la)$.

□

由上述引理的(3)可以得到求最大公因子的辗转相除法.

下面是最大公因子的一个主要应用.

定理 1.1.9 设 $a_1, a_2, \cdots, a_n$ 是不全为零的整数,$d = (a_1, a_2, \cdots, a_n)$,则对每个整数 l,不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = l \qquad (*)$$

有整数解当且仅当 $d \mid l$.

证明 考虑集合

$$S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : x_1, x_2, \cdots, x_n \in \mathbb{Z}\},$$

这也即是使方程(*)有整数解的所有整数 l 组成的集合. 这个集合是非空的,并且包含正整数(若 $a_i \neq 0$,则 $|a_i| \in S$). 容易验证集合 S 满足引理 1.1.5 中的两个条件. 于是存在正整数 D,使得 $S = D\mathbb{Z}$. 我们只需再证 $D = d$. 由集合 S 的定义和引理 1.1.2(3)可知 d 是 S 中每个整数的因子. 由于 $D \in D\mathbb{Z} = S$,所以 $d \mid D$. 特别地,$d \leqslant D$. 另一方面,易知 $a_1, a_2, \cdots, a_n$ 均属于 S,从而 D 是 $a_1, a_2, \cdots, a_n$ 的公因子,而 d 是 $a_1, a_2, \cdots, a_n$ 的最大公因子,因此 $D \leqslant d$. 于是 $D = d$.

□

现在可以得到最大公因子的进一步性质.

引理 1.1.10 设 $a_1, a_2, \cdots, a_n$ 是不全为零的整数.

(1) $a_1, a_2, \cdots, a_n$ 的每个公因子都是它们最大公因子的因子.

(2) 若 $a_1 \neq 0$,则 $(a_1, a_2, \cdots, a_n) = ((a_1, a_2), a_3, \cdots, a_n)$.

(3) 对于正整数 m,$m(a_1, a_2, \cdots, a_n) = (ma_1, ma_2, \cdots, ma_n)$.

(4) 若 $(a_1, a_2, \cdots, a_n) = d$,则 $\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = 1$.

(5) 对于整数 m,若 $(a_i, m) = 1 (1 \leqslant i \leqslant n)$,则 $(a_1, a_2, \cdots, a_n, m) = 1$.

(6) 若 $a, b, c \in \mathbb{Z}$,$c \neq 0$,$c \mid ab$,$(c,b) = 1$,则 $c \mid a$. 特别对素数 p,由 $p \mid ab$ 可得 $p \mid a$ 或 $p \mid b$.

证明 (1) 记 $d = (a_1, a_2, \cdots, a_n)$. 由定理 1.1.9 知存在整数 $x_1, x_2, \cdots, x_n$ 使得 $d = a_1x_1 + a_2x_2 + \cdots + a_nx_n$. 如果 d' 是 $a_1, a_2, \cdots, a_n$ 的公因子,则

$d' \mid a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$.

(2) 设 $d = (a_1, a_2, \cdots, a_n)$, $d' = ((a_1, a_2), a_3, \cdots, a_n)$. 易知 d' 是 $a_1, a_2, \cdots, a_n$ 的公因子,从而 $d' \leqslant d$. 另一方面,由于 d 为 $a_1, a_2, \cdots, a_n$ 的公因子,由(1)知 $d \mid (a_1, a_2)$,于是 d 是 $(a_1, a_2), a_3, \cdots, a_n$ 的公因子. 所以 $d \leqslant d'$. 于是 $d = d'$.

(3) 记 $d = (a_1, a_2, \cdots, a_n)$, $e = (ma_1, ma_2, \cdots, ma_n)$,要证 $e = md$. 由于 md 是 $ma_1, ma_2, \cdots, ma_n$ 的公因子,可知 $md \mid e$. 另一方面,存在整数 $x_1, x_2, \cdots, x_n$,使 $a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$. 于是 $(ma_1)x_1 + (ma_2)x_2 + \cdots + (ma_n)x_n = md$. 由定理 1.1.9 知 $e \mid md$. 于是 $e = md$.

(4) $\frac{a_i}{d}(1 \leqslant i \leqslant n)$ 均为整数,由(3)知

$$d = (a_1, a_2, \cdots, a_n) = d\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right).$$

于是 $\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = 1$.

(5) 这里只证 $n = 2$ 情形(一般情形可用归纳法). 设 $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. 由定理 1.1.9 知存在整数 x, y, x', y',使得

$$ax + my = 1, \quad bx' + my' = 1.$$

于是

$$1 = (ax + my)(bx' + my') = ab(xx') + m(axy' + bx'y + myy'),$$

再由定理 1.1.9 可知 $(ab, m) = 1$.

(6) 由假设 $(b, c) = 1$ 知,存在 $x, y \in \mathbb{Z}$,使得 $bx + cy = 1$. 由假设 $c \mid ab$ 可知, $c \mid abx + acy = a(bx + cy) = a$. 特别对素数 p,如果 $p \mid ab$ 但是 $p \nmid a$,则 $(p, a) = 1$. 于是 $p \mid b$.

□

最小公倍数有与最大公因子类似的性质.

引理 1.1.11 设 $a_1, a_2, \cdots, a_n$ 均是非零整数.

(1) $a_1, a_2, \cdots, a_n$ 的每个公倍数都是它们最小公倍数 $[a_1, a_2, \cdots, a_n]$ 的倍数.

(2) $[a_1, a_2, \cdots, a_n] = [[a_1, a_2], a_3, \cdots, a_n]$.

(3) 对于正整数 m, $[ma_1, ma_2, \cdots, ma_n] = m[a_1, a_2, \cdots, a_n]$.

(4) 设 $a, b \in \mathbb{Z}$, $ab \neq 0$. 则 $(a, b)[a, b] = |ab|$.

(5) 若 $a_1, a_2, \cdots, a_n$ 两两互素,则 $[a_1, a_2, \cdots, a_n] = |a_1a_2\cdots a_n|$.

证明 (1) 以 S 表示 $a_1, a_2, \cdots, a_n$ 的所有公倍数组成的集合. 这是非空集合并且包含正整数 $d = [a_1, a_2, \cdots, a_n]$. 验证集合 S 满足引理 1.1.5 中两个条件. 于是 $S = d'\mathbb{Z}$,其中 d' 是 S 中最小正整数,从而 $d' = d$,即 $S = d\mathbb{Z}$. 于是对 $a_1, a_2, \cdots,$

a_n的公倍数 m,$m \in S = d\mathbb{Z}$,即 $d \mid m$.

(2)和(3)的证明类似于引理 1.1.10 的(2)和(3)的证明.

(4) 不妨设 a,b 均是正整数. 先证$(a,b)=1$ 时的情形. 由定义知有 $x,y \in \mathbb{Z}$,使得

$$ax = [a,b] = by,$$

因此 $b \mid ax$. 由$(a,b)=1$ 知 $b \mid x$,于是 $ab \mid ax = [a,b]$. 但是 ab 是 a 和 b 的公倍数,由(1)知$[a,b] \mid ab$,因此 $ab = [a,b] = (a,b)[a,b]$.

对于一般情形,令 $d = (a,b)$,则$\left(\frac{a}{d},\frac{b}{d}\right)=1$. 由上面所证知$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{ab}{d^2}$.

但是$[a,b] = d\left[\frac{a}{d},\frac{b}{d}\right]=\frac{ab}{d}$,这表明

$$ab = d[a,b] = (a,b)[a,b].$$

(5) 由$(a_1,a_2)=1$ 可知$[a_1,a_2] = |a_1a_2|$. 由$(a_1,a_3)=(a_2,a_3)=1$ 可得$(a_1a_2,a_3)=1$(引理 1.1.10(6)). 从而

$$[a_1,a_2,a_3] = [[a_1,a_2],a_3] = [|a_1a_2|,a_3] = |a_1a_2a_3|.$$

再用归纳法即得一般情形.

□

定理 1.1.9 给出多元一次方程存在整数解的充分必要条件. 现在对二元情形,可以给出方程 $ax+by=n$ 全部整数解的表达式. 不妨设 a 和 b 均是非零整数(若 $a \neq 0, b=0$,则 $ax=n$ 有整数解当且仅当 $a \mid n$). 令 $d=(a,b)$,由定理 1.1.9 可知当 $d \nmid n$ 时,$ax+by=n$ 无整数解. 当 $d \mid n$ 时,令 $a=a'd, b=b'd, n=n'd$,则 $a',b',n' \in \mathbb{Z}$ 并且原方程等价于 $a'x+b'y=n'$,其中$(a',b')=1$. 从而归结于方程中 x,y 的系数互素情形.

定理 1.1.12 设 a 和 b 是非零整数,$(a,b)=1$,则对每个整数 n,方程 $ax+by=n$ 均有整数解,并且若$(x,y)=(x_0,y_0)$是方程的一组整数解,则此方程的全部整数解为

$$\begin{cases} x = x_0 + bt, \\ y = y_0 - at \end{cases} \quad (t \in \mathbb{Z}). \tag{*}$$

证明 由定理 1.1.9 知 $ax+by=n$ 必有整数解$(x,y)=(x_0,y_0)$,即 $ax_0+by_0=n$. 对于任意整数解(x,y),$ax+by=n$,则 $a(x-x_0)+b(y-y_0)=n-n=0$. 于是 $a(x-x_0)=-b(y-y_0)$. 特别地,$b \mid a(x-x_0)$. 由假设$(a,b)=1$ 可知 $b \mid (x-x_0)$. 因此 $x=x_0+bt$ $(t \in \mathbb{Z})$. 所以 $-b(y-y_0)=a(x-x_0)=abt$,即 $y-y_0=-at$. 于是 $y=y_0-at$. 这就给出整数解(x,y)必有(*)的形式. 反过来,容易验证由公式(*)表示的(x,y)必为原方程的整数解.

□