新编数学与信息类专业系列教材

初等数论

及其在信息科学中的应用

朱 萍 编著

清华大学出版社

新编数学与信息类专业系列教材

初等数论

及其在信息科学中的应用

朱　萍　编著

清华大学出版社
北京

内 容 简 介

本书是一本关于初等数论及其在密码学中应用的基础教材. 全书共分 5 章. 第 1 章和第 2 章分别介绍整除性和同余理论. 第 3 章讨论前两章知识在古典密码学和 RSA 公钥密码体制中的应用. 第 4 章介绍二次剩余及其在硬币抛掷和零知识证明中的应用. 第 5 章介绍阶、原根和离散对数的概念及其在伪随机数生成、ElGamal 公钥密码体制和椭圆曲线密码中的应用. 每章后面都配有习题, 书末附有习题答案及提示. 另外, 在附录中, 我们按照章节顺序列出了两种常用数学软件 Maple 和 Mathematica 用于数论计算的有关命令.

本书可以作为综合性和工科院校数学专业和信息科学相关专业的初等数论本科生课程教材, 也可作为相关领域中的教学科研人员以及工程技术人员的参考书.

图书在版编目(CIP)数据

初等数论及其在信息科学中的应用/朱萍编著. --北京：清华大学出版社, 2010.9
(新编数学与信息类专业系列教材)
ISBN 978-7-302-23800-3

Ⅰ. ①初… Ⅱ. ①朱… Ⅲ. ①初等数论—应用—信息技术 Ⅳ. ①G202 ②O156.1

中国版本图书馆 CIP 数据核字 (2010) 第 173147 号

责任编辑：石　磊
责任校对：刘玉霞
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**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
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：170×230　**印　张**：11　**字　数**：209 千字
版　　次：2010 年 9 月第 1 版　　**印　　次**：2010 年 9 月第1 次印刷
印　　数：1～3000
定　　价：20.00 元

产品编号：038024-01

前　言

数论是研究数的规律, 特别是整数性质的数学分支, 而初等数论主要是用整数的四则运算方法研究整数性质的数论分支, 它是数学中最古老的分支之一. 著名数学家哈代 (G. H. Hardy) 说过, "初等数论应当是一种极好的早期数学教育素材. 它需要的预备知识很少, 材料很实在, 可以触摸得到, 又为人们所熟悉; 它所用的推理过程非常简单, 有普遍意义, 而且为数不多; 在数学科学中它非常独特, 因为它能激发人们的天然好奇心. 花上一个月的时光, 进行富有智慧的数论启蒙教育, 它将会带来双倍效益, 双倍作用, 比起同等数量的给工程技术人员上的微积分来说, 更将是十倍地有趣."①

近几十年来, 初等数论在物理学、化学、生物学、计算机科学、密码学、编码理论、数字信息和电气工程等领域得到了广泛而深入的应用, 以至于华盛顿大学布兰克 (B. E. Blank) 教授曾说: "现今如果你教一门数论课程, 计算机专业的学生很可能比数学专业的学生更感兴趣. 许多人较少关心能被表成两个平方和的整数, 但更关心 Alice 如何与 Bob 进行保密通信."

基于初等数论的上述特点和教学的需要, 本书以经典理论与现代应用相结合的方式, 比较系统地介绍了初等数论的基本概念和方法. 本书的写作目的是双重的: 一是希望能使数学专业的学生在掌握初等数论基本概念的同时, 体会到这些概念和结果在信息科学, 特别是密码学中的应用价值, 从而激发他们对数论的学习兴趣; 二是希望通过初等数论在信息科学中的具体应用, 帮助信息科学相关专业的学生克服害怕数学的心理, 理解并掌握初等数论的基本概念, 为 "密码学" 和 "信息安全" 等课程奠定基础. 本书的初稿内容曾多次在北京大学 (曹永知副教授主讲) 和北京邮电大学 (作者主讲) 为计算机专业、通信专业和应用数学专业的学生讲授过, 均收到了良好效果.

在本书的编写过程中, 我们力求系统性、实用性和可读性相结合. 系统性方面, 就初等数论本身而言, 本书覆盖了它的基本知识; 就应用而言, 我们介绍了几种常见的古典密码体制和目前公认为安全的三种公钥密码体制. 实用性方面, 由于课时的限制, 我们尽量选取初等数论中有较强应用背景的知识和有代表性的例子. 为了增强本书的可读性, 书中大多由浅入深地介绍概念和性质, 同时也注意介绍概

① 摘自: (美) 阿尔伯特 • H. 贝勒著. 数论妙趣 —— 数学女王的盛情款待. 谈祥柏译, 上海: 上海教育出版社, 1998.5.

念的由来及相互之间的联系. 在附录中, 我们列出了两种常用数学软件 Maple 和 Mathematica 用于数论计算的有关命令, 为读者使用计算机计算数论函数 (尤其是进行有关涉及大整数的计算) 提供了方便. 本书绝大多数内容只需要读者具有中学数学知识便可领会, 当然, 了解一点概率论、数学分析、抽象代数和计算复杂性知识对于深入理解本书内容也是十分有益的.

本书可以作为综合性和工科院校数学专业及信息科学相关专业的初等数论本科生课程教材, 建议授课 32~48 学时. 同时, 也可作为相关领域中的教学、科研人员以及工程技术人员的参考书.

曹永知副教授在使用本书初稿时提出了不少修改意见, 谨此表示谢意. 本书的出版还得到了国家自然科学基金的资助, 基金号: 61070251. 正如潘承洞先生和潘承彪先生所言, "要写好一本初等数论的教材绝非易事." 由于水平有限, 书中难免存在不妥之处, 敬请读者批评指正.

作 者

2009 年 12 月于北京

目　录

第 1 章　整除性 ····· 1
1.1　整除 ····· 1
1.2　最大公因数与欧几里得算法 ····· 3
1.3　最小公倍数 ····· 8
1.4　一次不定方程 ····· 10
1.5　算术基本定理 ····· 14
1.6　厄拉多塞筛法 ····· 16
1.7　素数分布 ····· 19
习题一 ····· 22

第 2 章　同余 ····· 24
2.1　同余定义及基本性质 ····· 24
2.2　剩余系 ····· 27
2.3　欧拉函数与默比乌斯函数 ····· 32
2.4　一次同余方程 ····· 40
2.5　中国剩余定理 ····· 42
2.6　模为素数的高次同余方程 ····· 47
2.7　模为合数的高次同余方程 ····· 51
2.8　伪素数和素性测试 ····· 55
习题二 ····· 61

第 3 章　RSA 密码体制 ····· 64
3.1　密码学基本概念 ····· 64
3.2　几种简单密码体制及其破译 ····· 68
3.3　RSA 公钥密码体制 ····· 77
3.4　RSA 的实现 ····· 79
3.5　RSA 的安全性讨论 ····· 82
习题三 ····· 84

第 4 章　二次剩余 ····· 86
4.1　概念及判别 ····· 86

4.2 勒让德符号 ····· 89
4.3 二次同余方程 ····· 99
4.4 雅可比符号 ····· 105
4.5 二次剩余的应用 ····· 109
习题四 ····· 114

第 5 章 原根及其应用 ····· 117
5.1 整数的阶 ····· 117
5.2 原根 ····· 122
5.3 一般既约剩余系的构造 ····· 129
5.4 离散对数 ····· 131
5.5 伪随机数 ····· 135
5.6 ElGamal 密码体制 ····· 140
5.7 椭圆曲线密码 ····· 143
习题五 ····· 148

附录 A 抽象代数基本概念 ····· 149

附录 B 数学软件 Maple 和 Mathematica 中的一些与数论相关的命令 ····· 153
B.1 Maple 中的一些与数论相关的命令 ····· 153
B.2 Mathematica 中的一些与数论相关的命令 ····· 155

习题答案及提示 ····· 158

索引 ····· 167

参考文献 ····· 170

第1章 整 除 性

人类从计数开始就和自然数打交道, 后来由于实践需要, 数的概念进一步扩充到整数. 数论这门学科最初是从研究整数开始的, 所以叫做整数论. 后来整数论又进一步发展, 就叫做数论了. 确切地说, 数论就是研究数的规律, 特别是整数性质的数学分支. 初等数论主要是用整数的四则运算方法来研究整数性质 (特别是一些特殊类型的正整数的性质及其关系) 的数学分支.

初等数论中得到的整数的许多性质都要直接或间接地涉及整除性, 整除性是初等数论的基础, 因此这章我们首先讨论整除性的基本理论.

1.1 整 除

我们知道, **自然数**或者**正整数**指的是数 $1,2,\cdots$, 而**整数**指的是数 $0,\pm1,\pm2,\cdots$. 全体整数的集合记作 $\mathbb{Z}$, 而全体正整数或自然数的集合记作 $\mathbb{Z}^+$.

显然, 对任意 $a,b\in\mathbb{Z}$, 有 $a+b,a-b,ab\in\mathbb{Z}$, 即 $\mathbb{Z}$ 关于加、减、乘是封闭的, 但存在 $a,b\in\mathbb{Z}$, 使得 $a/b\notin\mathbb{Z}$. 因此我们需要考虑整除, 即研究什么时候 $a/b\in\mathbb{Z}$. 为此, 我们引入下面的概念.

定义 1.1.1 设 $a,b\in\mathbb{Z}$, 且 $b\neq0$. 如果存在 $q\in\mathbb{Z}$, 使得 $a=bq$, 则称 b**整除**a, 记作 $b|a$. 此时, b 叫做 a 的**因数**, a 叫做 b 的**倍数**.

如果 b 不能整除 a, 则用记号 $b\nmid a$ 表示.

对任意整数 a, 显然 $1|a$, 即 1 是任意整数的因数; 当 $a\neq0$ 时, 有 $a|0$ 和 $a|a$, 即 0 是任意整数的倍数, 任意非零整数是自身的因数也是自身的倍数.

如果一个整数是 2 的倍数, 我们称它为**偶数**; 否则称它为**奇数**.

因为一个非零数的因数的绝对值不大于该数本身的绝对值, 所以任一非零数的因数只有有限多个.

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1.1 设 $a,b,c\in\mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

(2) 如果 $b|a$, $c\neq0$, 那么 $cb|ca$.

(3) 如果 $c|a$, $c|b$, 那么对任意 $m,n\in\mathbb{Z}$, 有 $c|ma+nb$.

(4) *如果* $b|a$, $a|b$, *那么* $a=b$ *或* $a=-b$.

因为 $|a|$ 和 a 的所有因数都相同, 所以我们讨论因数时可以只就正整数来讨论.

下面是整除的基本定理, 也称为**带余除法**, 它是初等数论的证明中最基本、最常用的工具.

定理 1.1.1 *设* $a,b\in\mathbb{Z}$, *且* $b\neq 0$, *则存在惟一的* $q,r\in\mathbb{Z}$, *使得*

$$a=bq+r,\quad 0\leqslant r<|b|. \tag{1.1}$$

证明 考虑整数序列

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

则 a 必在上述序列的某相邻两项之间. 不妨假定

$$q|b|\leqslant a<(q+1)|b|.$$

于是 $0\leqslant a-q|b|<|b|$, 令 $r=a-q|b|$, 则有 $0\leqslant r<|b|$. 因此, 当 $b>0$ 时, 有 $a=bq+r$; 当 $b<0$ 时, 有 $a=b(-q)+r$. 这样, 我们就证明了 q 和 r 的存在性.

下面证明 q,r 的惟一性. 假设存在另外一组 $q',r'\in\mathbb{Z}$, 使得 (1.1) 式成立, 即 $a=bq'+r'$, $0\leqslant r'<|b|$, 则有

$$-|b|<r-r'=b(q'-q)<|b|.$$

因此 $b(q'-q)=0$, 从而 $r-r'=0$, 即 $q'=q$, $r'=r$, 所以惟一性成立. □

例如, 当 $a=17,b=5$ 时, $17=5\times 3+2$, 这时 $q=3$, $r=2$; 而 $a=-17,b=5$ 时, $-17=5\times(-4)+3$, 这时 $q=-4$, $r=3$.

定义 1.1.2 *称* (1.1) *式中的* q *为用* b *除* a *得出的***不完全商**, *称* r *为用* b *除* a *得到的***最小非负余数**, *也简称为***余数**, *常记作* $\langle a\rangle_b$ *或* $a \bmod b$.

约定 1.1.1 *在不致引起混淆时,* $\langle a\rangle_b$ *中的* b *常略去不写. 为方便起见, 以后除非特别说明, 我们总假定除数* b *以及因数都大于零.*

作为带余除法的一个重要应用, 我们考虑整数的基 b ($b\geqslant 2$) 表示. 我们知道, 通常所用的数都是十进制的, 而计算机上用的数是二进制、八进制及十六进制的. 下面的定理给出一个数能用不同进制表示的依据.

定理 1.1.2 *设* $b\geqslant 2$ *是给定的正整数, 那么任意正整数* n *可以惟一表示为*

$$n=r_kb^k+r_{k-1}b^{k-1}+\cdots+r_1b+r_0,$$

这里整数 $k \geqslant 0$, 整数 r_i $(i = 0, 1, \cdots, k)$ 满足 $0 \leqslant r_i < b$, $r_k \neq 0$.

证明 对给定的正整数 n, 必存在惟一的整数 $k \geqslant 0$, 使得 $b^k \leqslant n < b^{k+1}$. 由带余除法, 存在惟一的 $q_0, r_0 \in \mathbb{Z}$, 使得

$$n = bq_0 + r_0, \quad 0 \leqslant r_0 < b. \tag{1.2}$$

下面对 k 进行归纳证明. 当 $k = 0$ 时, 则有 $q_0 = 0$, $1 \leqslant r_0 < b$, 这时结论显然成立.

假设结论对 $k = m \geqslant 0$ 成立, 那么当 $k = m + 1$ 时, (1.2) 式中的 q_0 必满足 $b^m \leqslant q_0 < b^{m+1}$. 由归纳假设知, q_0 可以惟一表示为

$$q_0 = s_m b^m + s_{m-1} b^{m-1} + \cdots + s_1 b + s_0,$$

其中整数 s_j $(j = 0, 1, \cdots, m)$ 满足 $0 \leqslant s_j < b$, $s_m \neq 0$. 因此我们有

$$n = s_m b^{m+1} + s_{m-1} b^m + \cdots + s_1 b^2 + s_0 b + r_0,$$

易见, 这种表示是满足定理要求的惟一表示, 否则与上面 q_0 的惟一表示性矛盾. 因此结论对 $m + 1$ 也成立. □

如果取 $b = 2$, 那么任意正整数 n 可以表示为 2 的乘幂之和, 即

$$n = 2^k + r_{k-1} 2^{k-1} + \cdots + r_1 2 + r_0,$$

其中, 整数 $k \geqslant 0$, r_i $(i = 0, 1, \cdots, k-1)$ 是 0 或 1.

在本节的最后, 我们给出余数的几个基本性质.

定理 1.1.3 设 $a_1, a_2, b \in \mathbb{Z}$, 且 $b > 0$, 则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$.

(2) $\langle a_1 - a_2 \rangle = \langle \langle a_1 \rangle - \langle a_2 \rangle \rangle$.

(3) $\langle a_1 a_2 \rangle = \langle \langle a_1 \rangle \langle a_2 \rangle \rangle$.

证明 (1)~(3) 的证明类似, 这里仅证明 (1). 设 $a_1 = bq_1 + \langle a_1 \rangle$, $a_2 = bq_2 + \langle a_2 \rangle$, $\langle a_1 \rangle + \langle a_2 \rangle = bq_3 + \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$. 于是

$$\begin{aligned} a_1 + a_2 &= b(q_1 + q_2) + \langle a_1 \rangle + \langle a_2 \rangle \\ &= b(q_1 + q_2 + q_3) + \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle, \end{aligned}$$

因此 $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$, 所以断言 (1) 成立. □

1.2 最大公因数与欧几里得算法

上节讨论了单个数的因数和倍数, 接下来要讨论多个数的因数和倍数, 研究它们最大公因数和最小公倍数的存在性及求法.

定义 1.2.1 设 $a_1, a_2, \cdots, a_n$ 是不全为零的整数. 如果存在 $d \in \mathbb{Z}$, 使得 $d|a_i (i = 1, 2, \cdots, n)$, 则 d 叫做 $a_1, a_2, \cdots, a_n$ 的一个**公因数**. 公因数中最大的一个叫做**最大公因数**, 记作 $(a_1, a_2, \cdots, a_n)$. 若 $(a_1, a_2, \cdots, a_n) = 1$, 则称 $a_1, a_2, \cdots, a_n$ **互素**.

定义 1.2.1 是良定义的. 事实上, 显然 1 是 $a_1, a_2, \cdots, a_n$ 的一个公因数, 因为任意非零数的因数只有有限多个, 所以 $a_1, a_2, \cdots, a_n$ ($a_1, a_2, \cdots, a_n$ 不全为零) 的公因数也只有有限多个, 因此最大公因数 $(a_1, a_2, \cdots, a_n)$ 的确惟一存在, 并且 $(a_1, a_2, \cdots, a_n) \geqslant 1$. 例如, $(24, -36, 18) = 6$, $(49, 64) = 1$.

因为 $(a, 1) = 1$, 所以 1 与任何数均互素. 当 $a \neq 0$ 时, $(a, 0) = |a|$. 更一般地, 因为 $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$, 又因为一组不全为零的整数的最大公因数等于它们当中全体非零整数的最大公因数, 所以不妨设 $a_i > 0$ $(i = 1, 2, \cdots, n)$.

下面先讨论两个数的最大公因数.

定理 1.2.1 设 a, b, c 是不全为零的整数, 若存在 $q \in \mathbb{Z}$, 使得 $a = bq + c$, 则 $(a, b) = (b, c)$.

证明 由 $(b, c)|b$, $(b, c)|c$ 及 $a = bq + c$, 知 $(b, c)|a$, 因此 (b, c) 是 a 和 b 的公因数. 但 (a, b) 是 a 和 b 的最大公因数, 所以 $(b, c) \leqslant (a, b)$. 类似地, 可以得到 $(a, b) \leqslant (b, c)$, 于是 $(a, b) = (b, c)$. □

定理 1.2.1 的更直接表述是 $(a + bq, b) = (a, b)$, 其中 $a, b, q \in \mathbb{Z}$, 且 a, b 不全为零.

下面的欧几里得算法, 也称作辗转相除法, 是由古希腊数学家欧几里得于公元前 3 世纪提出的, 它提供了一种求两个正整数的最大公因数的有效方法.

定理 1.2.2 设整数 $a > 0, b > 0$. 令 $r_0 = a, r_1 = b$, 由带余除法, 不妨假设

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n, \end{aligned} \tag{1.3}$$

那么 (a, b) 就是 (1.3) 式中最后一个非零的余数, 即 $(a, b) = r_n$.

证明 因为 $r_1 > r_2 > r_3 > \cdots$, 所以存在正整数 n, 使得 $r_{n+1} = 0$, 从而上面的算法可以终止.

由定理 1.2.1, 我们有

$$(a,b)=(r_0,r_1)=(r_1,r_2)=(r_2,r_3)=\cdots=(r_{n-1},r_n)=(r_n,0)=r_n,$$

即 r_n 就是所求的 (a,b). □

欧几里得算法可以在多项式时间内完成. 事实上, 不妨设正整数 $a>b$, 那么求 (a,b) 最多需要进行 $O(\log b)$ 步除法①, 因此欧几里得算法有多项式时间复杂度.

例 1.2.1 求 $(963,657)$.

解 由带余除法得

$$\begin{aligned}963&=657\times1+306,\\657&=306\times2+45,\\306&=45\times6+36\\45&=36\times1+9,\\36&=9\times4,\end{aligned}$$

故 $(963,657)=9$. □

定理 1.2.3 设整数 a,b 不全为零, 则存在 $s,t\in\mathbb{Z}$, 使得

$$sa+tb=(a,b). \tag{1.4}$$

证明 如果整数 a,b 有一个为零, 那么结论显然成立.

下面考虑 $a>0$, $b>0$ 的情形. 此时, 根据带余除法, 由 (1.3) 式中 $r_n=r_{n-2}-r_{n-1}q_{n-1}$ 和 $r_{n-1}=r_{n-3}-r_{n-2}q_{n-2}$ 得

$$\begin{aligned}r_n&=r_{n-2}-(r_{n-3}-r_{n-2}q_{n-2})q_{n-1}\\&=r_{n-2}(1+q_{n-1}q_{n-2})-r_{n-3}q_{n-1},\end{aligned}$$

再将 $r_{n-2}=r_{n-4}-r_{n-3}q_{n-3}$ 代入上式, 如此继续下去, 最后可得 $r_n=sr_0+tr_1$, 即 $(a,b)=sa+tb$, 其中 s,t 是两个整数.

如果 $a<0$ 或 $b<0$, 那么对正整数 $|a|,|b|$, 由前面的证明知, 存在 $s',t'\in\mathbb{Z}$, 使得 $s'|a|+t'|b|=(a,b)$, 所以存在 $s,t\in\mathbb{Z}$, 使得 $sa+tb=(a,b)$. 因此定理成立. □

注意, 满足 (1.4) 式的 s,t 可能不惟一. 一个简单的例子是

$$(4,2)=1\times4+(-1)\times2=2\times4+(-3)\times2.$$

① 没有接触过算法复杂性知识的读者可以参阅算法方面的书籍, 也可以忽略本书中与大 O 记号有关的内容.

例 1.2.2 求一组整数 s,t, 使得

$$963s+657t=(963,657).$$

解 由例 1.2.1 的求解得

$$\begin{aligned}(963,657)=9&=45-36\times 1\\&=45-(306-45\times 6)\times 1=45\times 7-306\times 1\\&=(657-306\times 2)\times 7-306=306\times(-15)+657\times 7\\&=(963-657\times 1)\times(-15)+657\times 7\\&=(-15)\times 963+22\times 657,\end{aligned}$$

因此取 $s=-15$, $t=22$, 则可满足 $963s+657t=(963,657)$. □

特别地, 当 a,b 互素时, 由定理 1.2.3 可得下面的结论.

推论 1.2.1 设整数 a,b 不全为零, 则 $(a,b)=1$ 当且仅当存在 $s,t\in\mathbb{Z}$, 使得 $sa+tb=1$.

作为定理 1.2.3 的推论, 我们易见 a,b 的任意公因数一定是它们最大公因数的因数.

推论 1.2.2 如果 $d|a$, 且 $d|b$, 那么 $d|(a,b)$.

利用欧几里得算法, 我们还可得到更多关于最大公因数的基本性质.

命题 1.2.1 设 $a,b,c\in\mathbb{Z}$, 则 $(ac,bc)=(a,b)|c|$.

证明 用 $|c|$ 乘 (1.3) 式中各式, (1.3) 式中的 r_i $(0\leqslant i\leqslant n)$ 就变成了 $r_i|c|$, 所以由定理 1.2.2 知, $(ac,bc)=(a,b)|c|$. □

例如, $(48,36)=(4,3)\times 12=12$.

由命题 1.2.1, 我们有如下推论.

推论 1.2.3 设 d 是一正整数, 那么 $d=(a,b)$ 的充要条件是 $(a/d,b/d)=1$.

证明 由命题 1.2.1 知

$$\left(\frac{a}{d},\frac{b}{d}\right)d=\left(\frac{a}{d}\cdot d,\frac{b}{d}\cdot d\right)=(a,b),$$

因此, 如果 $d=(a,b)$, 那么 $(a/d,b/d)=1$; 反过来, 如果 $(a/d,b/d)=1$, 那么 $d=(a,b)$. □

利用推论 1.2.3 的充分性部分, 可以判断一个数 d 是否是 a,b 的最大公因数. 下面的命题给出了另外一种判断方法.

命题 1.2.2 *设 d 是正整数, a,b 是不全为零的整数, 则 $d=(a,b)$ 的充要条件是*

(1) $d|a$, *且* $d|b$;

(2) *如果* $c\in\mathbb{Z}$ *满足* $c|a$ *和* $c|b$, *那么* $c|d$.

证明 由推论 1.2.2 可知, 必要性显然成立. 下面考虑充分性. 由条件 (1) 知, d 是 a,b 的公因数, 因此 $d\leqslant(a,b)$. 另一方面, 由条件 (2) 可以得到 $(a,b)|d$, 所以 $(a,b)\leqslant d$, 于是 $d=(a,b)$, 从而充分性成立. □

命题 1.2.3 *如果* $(a,b)=1$, *那么* $(a,bc)=(a,c)$.

证明 因为 $(a,bc)|ac$, $(a,bc)|bc$, 所以 $(a,bc)|(ac,bc)$. 而由命题 1.2.1 知 $(ac,bc)=(a,b)|c|=|c|$, 因此 $(a,bc)|c$. 又因为 $(a,bc)|a$, 所以 $(a,bc)|(a,c)$. 反过来, 显然有 $(a,c)|a$, $(a,c)|bc$, 因此 $(a,c)|(a,bc)$, 于是 $(a,bc)=(a,c)$. □

例如, $(20,973\times15)=(20,15)=5$.

由命题 1.2.3 容易得出下面几个常用的结果.

推论 1.2.4 (1) *如果* $(a,b)=1$, $a|bc$, *那么* $a|c$.

(2) *如果* $(a,b)=1$, $a|c$, $b|c$, *那么* $ab|c$.

(3) *如果* $(a,b)=1$, $(a,c)=1$, *那么* $(a,bc)=1$.

证明 (1) 由条件及命题 1.2.3, 有 $(a,c)=(a,bc)=a$, 因此 $a|c$.

(2) 因为 $b|c$, 所以存在 $d\in\mathbb{Z}$, 使得 $c=bd$. 由 $a|c$ 知 $a|bd$, 进而由 (1) 得 $a|d$, 于是 $ab|bd$, 即 $ab|c$.

(3) 由命题 1.2.3, 我们有 $(a,bc)=(a,c)=1$. □

下面的定理提供了求 n $(n\geqslant3)$ 个数的最大公因数的方法.

定理 1.2.4 *设 $a_1,a_2,\cdots,a_n$ 是 n 个不全为零的整数, 则*

$$(a_1,a_2,\cdots,a_n)=((a_1,a_2),a_3,\cdots,a_n). \tag{1.5}$$

证明 由推论 1.2.2 知, $a_1,a_2,\cdots,a_n$ 的任意公因数一定是 $(a_1,a_2),a_3,\cdots,a_n$ 的公因数; 反过来, $(a_1,a_2),a_3,\cdots,a_n$ 的任意公因数一定是 $a_1,a_2,\cdots,a_n$ 的公因数. 由此可见, $a_1,a_2,\cdots,a_n$ 和 $(a_1,a_2),a_3,\cdots,a_n$ 必有相同的最大公因数, 即 $(a_1,a_2,\cdots,a_n)=((a_1,a_2),a_3,\cdots,a_n)$. □

定理 1.2.4 表明, 如果想求 $a_1, a_2, \cdots, a_n$ 的最大公因数, 那么可以先求 a_1, a_2 的最大公因数 (a_1, a_2), 记作 d_2, 然后求 d_2, a_3 的最大公因数 (d_2, a_3), 记作 d_3, 依次下去, 最后求 d_{n-1}, a_n 的最大公因数 (d_{n-1}, a_n), 记作 d_n, 那么 d_n 即为所求.

作为定理 1.2.3 的推广, 我们有下面的结果.

定理 1.2.5 设整数 $a_1, a_2, \cdots, a_n$ 不全为零, 则存在 $s_1, s_2, \cdots, s_n \in \mathbb{Z}$, 使得

$$s_1a_1 + s_2a_2 + \cdots + s_na_n = (a_1, a_2, \cdots, a_n).$$

证明 由定理 1.2.3 和定理 1.2.4 易证. □

1.3 最小公倍数

上节我们介绍了最大公因数, 下面我们来讨论最小公倍数.

定义 1.3.1 设 $a_1, a_2, \cdots, a_n$ 是全不为零的整数, 若 $a_i | m$ $(1 \leqslant i \leqslant n)$, 则称 m 为这 n 个数的一个**公倍数**. $a_1, a_2, \cdots, a_n$ 的所有公倍数中最小的正公倍数称为这 n 个数的**最小公倍数**, 记作 $[a_1, a_2, \cdots, a_n]$.

因为 $|a_1a_2\cdots a_n|$ 就是 $a_1, a_2, \cdots, a_n$ 的一个正公倍数, 所以最小公倍数存在. 另外, 由于任何正整数都不是 0 的倍数, 因此讨论最小公倍数时总假定这些整数均不为零. 又因为 $[a_1, a_2, \cdots, a_n] = [|a_1|, |a_2|, \cdots, |a_n|]$, 所以只对正整数讨论它们的最小公倍数即可.

下面先讨论两个整数的最小公倍数. 最小公倍数与公倍数之间有着与最大公因数与公因数之间类似的关系.

定理 1.3.1 整数 a, b 的公倍数是它们的最小公倍数的倍数.

证明 设 k 是 a, b 的一个公倍数, 并假设用 $m = [a, b]$ 除 k 得

$$k = mq + r, \quad 0 \leqslant r < m.$$

因为 $a|k$, $a|m$, 所以 $a|r$. 同理有 $b|r$, 所以 r 是 a, b 的一个倍数. 因为 $0 \leqslant r < m$, 且 m 是 a, b 的最小公倍数, 所以 $r = 0$, 即 $k = mq$. 因此定理成立. □

由定理 1.3.1, 显然有 $\{a, b\text{的公倍数}\} = \{k[a, b] | k \in \mathbb{Z}\}$. 下面命题给出一种判断一个数 m 是否是 a, b 的最小公倍数的方法.

命题 1.3.1 设 m 是正整数, a, b 是全不为零的整数, 则 $m = [a, b]$ 的充要条件是

(1) $a|m$, 且 $b|m$;

(2) *如果存在* $n \in \mathbb{Z}$, *满足* $a|n$ *和* $b|n$, *那么* $m|n$.

证明 由定理 1.3.1, 必要性显然成立. 下面考虑充分性. 由条件 (1) 知, m 是 a, b 的公倍数, 因此 $[a, b] \leqslant m$. 另一方面, 由条件 (2) 可得 $m|[a, b]$, 所以 $m \leqslant [a, b]$, 于是 $m = [a, b]$, 从而充分性成立. □

下面定理给出最小公倍数与最大公因数之间的重要关系.

定理 1.3.2 *如果整数* a, b *均不为零, 那么*

$$[a, b] = \frac{|ab|}{(a, b)}.$$

证明 为了简单起见, 假设 $[a, b] = m$, $(a, b) = d$. 因为 $a|m$, 所以 $ab|mb$; 同理, 因为 $b|m$, 所以 $ab|ma$. 因此 $ab|(ma, mb)$, 所以 $ab|m(a, b)$, 即 $ab|md$.

另一方面, 我们有 $a\left|\frac{ab}{d}\right.$, $b\left|\frac{ab}{d}\right.$, 即 $\frac{ab}{d}$ 是 a, b 的一个公倍数. 由定理 1.3.1, 我们有 $m\left|\frac{ab}{d}\right.$, 因此 $md|ab$, 从而 $md = ab$ 或 $md = -ab$, 即 $md = |ab|$, 所以定理成立. □

定理 1.3.2 表明, 求最小公倍数可以转化为求最大公因数. 例如

$$[48, -32] = \frac{48 \times 32}{(48, -32)} = \frac{48 \times 32}{16(3, -2)} = 96.$$

与定理 1.2.4 类似, 下面的定理提供了求 n $(n \geqslant 3)$ 个数的最小公倍数的方法.

定理 1.3.3 *设* $a_1, a_2, \cdots, a_n$ *是* n *个全不为零的整数, 则*

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

证明 由定理 1.3.1 知, $a_1, a_2, \cdots, a_n$ 的任意公倍数一定是 $[a_1, a_2], a_3, \cdots, a_n$ 的公倍数; 反过来, $[a_1, a_2], a_3, \cdots, a_n$ 的任意公倍数一定是 $a_1, a_2, \cdots, a_n$ 的公倍数. 因此, $a_1, a_2, \cdots, a_n$ 和 $[a_1, a_2], a_3, \cdots, a_n$ 必有相同的最小公倍数, 即 $[a_1, a_2, \cdots, a_n] = [[a_1, a_2], a_3, \cdots, a_n]$. □

借助定理 1.3.3, 定理 1.3.2 中的公式可以推广到任意多个数的情形. 例如对于三个数, 我们有下面的公式.

命题 1.3.2 *设整数* a, b, c *均不为零, 则*

$$[a, b, c] = \frac{|abc|}{(ab, ac, bc)}.$$

证明 反复使用定理 1.3.2, 我们有

$$\begin{aligned}[a,b,c]&=[[a,b],c]=\frac{[a,b]|c|}{([a,b],c)}\\&=\frac{|abc|}{(a,b)([a,b],c)}=\frac{|abc|}{(ab,(a,b)c)}\\&=\frac{|abc|}{(ab,ac,bc)}.\end{aligned}$$

□

1.4 一次不定方程

不定方程是一类特殊的方程, 其特点是方程的个数少于未知数的个数, 且它的解受到某种限制 (如整数或正整数等). 公元 3 世纪初, 古希腊数学家丢番图 (Diophantus) 曾大力研究过这类方程, 因此不定方程也叫做**丢番图方程**. 本节主要讨论一次不定方程的求解问题.

设整数 $k\geqslant 2$, $a_1,a_2,\cdots,a_k,c\in\mathbb{Z}$, 且 $a_1,a_2,\cdots,a_k$ 均不为零, 未知数 $x_1,x_2,\cdots,x_k$ 取值为整数的方程 $a_1x_1+a_2x_2+\cdots+a_kx_k=c$ 称为 k 元**一次不定方程**, $a_1,a_2,\cdots,a_k$ 称为它的系数. 事实上, 丢番图研究的是这类方程的有理数解, 当然一个不定方程有有理数解并不意味着有整数解, 例如方程 $2x+2y=5$ 有无穷多个有理数解, 但却没有整数解.

我们先讨论二元一次不定方程. 显然, x,y 是不定方程 $ax+by=c$ 的整数解当且仅当点 (x,y) 是平面内直线 $ax+by=c$ 上的整点 (即横坐标和纵坐标均为整数的点).

早在公元 7 世纪, 印度数学家婆罗摩笈多 (Brahmagupta) 便开始一次不定方程一般解的研究. 下面是这方面有关的主要定理.

定理 1.4.1 *设 $a,b,c\in\mathbb{Z}$, a,b 均不为零, $d=(a,b)$.*

(1) 二元一次不定方程

$$ax+by=c \tag{1.6}$$

有整数解当且仅当 $d|c$.

(2) 当方程 (1.6) 有解时, 它的解与不定方程

$$\frac{a}{d}x+\frac{b}{d}y=\frac{c}{d} \tag{1.7}$$

的解相同.

(3) 如果 $x=x_0$, $y=y_0$ 是方程 (1.6) 的一组特解, 那么它的全部解可表为

$$x=x_0+\frac{b}{d}t,\quad y=y_0-\frac{a}{d}t,$$