普通高等教育“十一五”规划教材
21世纪大学数学创新教材

丛书主编　陈　化

初等数论

胡典顺　徐汉文　编著

科学出版社
www.sciencep.com

普通高等教育“十一五”规划教材

21世纪大学数学创新教材

丛书主编　**陈　化**

初等数论

胡典顺　徐汉文　编　著

科学出版社

北　京

内 容 简 介

本书共分7章，内容包括整除理论、不定方程、同余、同余方程、二次同余式与平方剩余、原根与指标以及连分数等. 书中配有例题和习题，并且每个例题和习题都提供了非常详细的解答和思维过程.

本书可作为高等院校数学与应用数学相关专业学生的教材，也可供高中数学教师以及数学爱好者参考.

图书在版编目(CIP)数据

初等数论/胡典顺，徐汉文编著. —北京：科学出版社，2010.6

普通高等教育"十一五"规划教材. 21世纪大学数学创新教材

ISBN 978-7-03-027924-8

Ⅰ. 初… Ⅱ. ①胡…②徐… Ⅲ. 初等数论—高等学校—教材

Ⅳ. O156.1

中国版本图书馆CIP数据核字(2010)第110122号

责任编辑：吉正霞/责任校对：董艳辉

责任印制：彭 超/封面设计：苏 波

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

武汉市首壹印务有限公司

科学出版社发行 各地新华书店经销

*

2010年6月第 一 版 开本：B5(720×1000)

2010年6月第一次印刷 印张：13 1/4

印数：1—3 000 字数：253 000

定价：23.80元

(如有印装质量问题，我社负责调换)

《21世纪大学数学创新教材》丛书编委会

《21世纪大学数学创新教材》丛书序

《21世纪大学数学创新教材》为大学本科数学系列教材，大致划分为公共数学类、专业数学类两大块，创新是其主要特色和要求. 经组编委员会审定，列选科学出版社普通高等教育“十一五”规划教材.

一、组编机构

《21世纪大学数学创新教材》丛书由多所985和211大学联合组编：

二、教材特色

创新是本套教材的主要特色和要求，创造双重品牌：

先进. 把握教改、课改动态和学科发展前沿，学科、课程的先进理念、知识和方法原则上都要写进教材或体现在教材结构及内容中.

知识与方法创新. 重点教材、高层次教材，应体现知识、方法、结构、内容等方面的创新，有所建树，有所创造，有所贡献.

教学实践创新. 教材适用，教师好教，学生好学，是教材的基本标准. 应紧跟和引领教学实践，在教学方法、教材结构、知识组织、详略把握、内容安排上有独到之处.

继承与创新. 创新须与继承相结合，是继承基础上的创新；创新需转变为参编者、授课者的思想和行为，避免文化冲突.

三、指导思想

遵循国家教育部高等学校数学与统计学教学指导委员会关于课程教学的基本要求，力求教材体系完整，结构严谨，层次分明，深入浅出，循序渐进，阐述精炼，富有启发性，让学生打下坚实的理论基础. 除上述一般性要求外，还应具备下列特点：

(1) 恰当融入现代数学的新思想、新观点、新结果，使学生有较新的学术视野.

(2) 体现现代数学创新思维，着力培养学生运用现代数学软件的能力，使教材真正成为基于现代数学软件的、将数学软件融合到具体教学内容中的现代精品教材.

(3) 在内容取舍、材料组织、叙述方式等方面具有较高水准和自身特色.

(4) 数学专业教材要求同步给出重要概念的英文词汇，章末列出中文小结，布置若干道(少量)英文习题，并要求学生用英文解答. 章末列出习题和思考题，并列出可进一步深入阅读的文献. 书末给出中英文对照名词索引.

(5) 公共数学教材具有概括性和简易性，注重强化学生的实验训练和实际动手能力，加强内容的实用性，注重案例分析，提高学生应用数学知识和数学方法解决实际问题的能力.

四、主编职责

丛书组编委员会和出版社确定全套丛书的编写原则、指导思想和编写规范，在这一框架下，每本教材的主编对本书具有明确的责权利：

1. 拟定指导思想

按照丛书的指导思想和特色要求，拟出编写本书的指导思想和编写说明.

2. 明确创新点

教改、课改动态，学科发展前沿，先进理念、知识和方法，如何引人教材；知识和内容创新闪光点及其编写方法；教学实践创新的具体操作；创新与继承的关系把握及其主客体融合.

3. 把握教材质量

质量是图书的生命，保持和发扬科学出版社“三高”、“三严”的传统特色，创出品牌；适用性是教材的生命力所在，应明确读者对象，篇幅要结合大部分学校对课程学时数的要求.

4. 掌握教材编写环节

(1) 把握教材编写人员水平，原则上要求博士、副教授以上，有多年课程教学经历，熟悉课程和学科领域的发展状况，有教材编写经验，有扎实的文字功底.

(2) 充分注意著作权问题，不侵犯他人著作权.

(3) 讨论、拟定教材提纲，并负责编写组的编写分工、协调与组织.

(4) 拟就内容简介、前言、目录、样章，统稿、定稿，确定交稿时间.

(5) 负责出版事宜，敦促编写组成员使用本教材，并优先选用本系列教材.

《21世纪大学数学创新教材》组编委员会

2009年6月

前　言

初等数论是研究整数性质的一门源远流长的学科，该学科的特点是理论易懂，习题难做. 例如，“哥德巴赫猜想”问题容易理解，能够引起人们的兴趣，但是要解决它却非常困难. 近几十年来，数论在理论和应用上取得了令人瞩目的进展. 我国新一轮数学课程改革在选修系列 4 中设置了“初等数论选讲”这一专题. 为了适应这一形势，越来越多的高校开设了初等数论课程.

本书着重介绍了初等数论中常用的基础知识、基本方法和基本技巧. 本书选材精练，理论联系实际，重难点突出，例题、习题丰富，难度适中，并且每一个例题、习题都给出了思维过程和完整解答，便于自学，让学习者能在短期内窥见初等数论的真髓. 本书特别适合高等院校数学与应用数学相关专业的学生以及师范院校数学系的学生作为《初等数论》的教材使用.

本书是在作者承担的华中师范大学教学研究项目《初等数论》网络课程建设以及作者的《初等数论》课程讲义的基础上修改而成. 作者根据多年的初等数论教学和研究的经验，在编写中，尽量想突破初等数论“题目难做、技巧性强”的瓶颈，力争通俗易懂，展现问题解决的思维过程，让学习者掌握初等数论的基本知识和基本思想方法，取得较好的学习效果.

本书的主要内容有：整数的可除性的基本概念和理论，最大公因数与辗转相除，最小公倍数，算术基本定理，高斯函数及其应用；二元一次不定方程，多元一次不定方程以及勾股数；同余的概念及其基本性质，剩余类及完全剩余系，简化剩余系与欧拉函数，欧拉定理、费马小定理及其对循环小数的应用；一次同余式，孙子定理，高次同余式的解数及解法，质数模的同余式；一般二次同余式，单质数的平方剩余与平方非剩余，勒让德符号，雅可比符号等；指数及其基本性质，原根存在的条件，指标及 n 次剩余等；连分数的性质，佩尔方程等.

本书在编写的过程中，我们参阅了国内外相关文献资料，同时得到了华中师范大学数学与统计学学院领导的大力支持，在此致以诚挚谢意！本书初稿在使用过程中，华中师范大学数学与统计学学院徐学文副教授提出了宝贵的意见或建议；华中师范大学数学与统计学学院历届本科生对某些问题提出了创造性的解答. 最后，我们向支持本书出版的科学出版社表示衷心感谢！

由于我们水平有限，书中可能出现的错误和疏漏在所难免，敬请专家和读者批评指正.

若需要本书的 PowerPoint 课件，请发邮件至：shulun04@yahoo.com.cn.

胡典顺

2010 年 3 月

目　录

第1章 整除理论

1.1 数的整除性

定义 1.1.1 设 a,b 是整数，$b\neq 0$，如果存在整数 c，使得 $a=bc$ 成立，则称 b 整除 a，记作 $b\mid a$；如果不存在整数 c，使得 $a=bc$ 成立，则称 b 不整除 a，记作 $b\nmid a$.

另外，每个非零整数 a 都有约数 $1,-1,a,-a$，这 4 个数称为 a 的平凡约数，a 的另外的约数称为非平凡约数.

性质 1.1.1 (i) $a\mid b\Rightarrow \pm a\mid \pm b$；

(ii) $a\mid b,b\mid c\Rightarrow a\mid c$；

(iii) $b\mid a_i(i=1,2,\cdots,k)\Rightarrow b\mid a_1x_1+a_2x_2+\cdots+a_kx_k$（其中 x_i 是任意整数）；

(iv) $b\mid a\Rightarrow bc\mid ac$（其中 c 是任意的非零整数）；

(v) $b\mid a,a\neq 0\Rightarrow |b|\leqslant |a|$；

(vi) $b\mid a,|a|<|b|\Rightarrow a=0$.

证 (i) 因 $a\mid b$，故 $b=aq$，即 $\pm b=\pm aq$，故 $\pm a\mid \pm b$；

(ii) 因 $a\mid b,b\mid c$，故 $b=q_1a,c=q_2b$，则 $c=q_1q_2a$，故 $a\mid c$；

(iii) 因为 $b\mid a_i(i=1,2,\cdots,k)$，所以

$$a_i=q_ib\quad (i=1,2,\cdots,k)$$

$$a_ix_i=q_ix_ib\quad (i=1,2,\cdots,k)$$

故
$$a_1x_1+a_2x_2+\cdots+a_kx_k=b(q_1x_1+q_2x_2+\cdots+q_kx_k)$$

因此
$$b\mid a_1x_1+a_2x_2+\cdots+a_kx_k\quad (\text{其中 } x_i \text{ 是任意整数})$$

(iv) 因 $b\mid a$，故 $a=bq$，即 $ac=bcq$，则 $bc\mid ac$（其中 c 是任意的非零整数）；

(v) 因 $b\mid a$，故 $a=bq$，即 $|a|=|b||q|$，又因 $a\neq 0$，则 $q\neq 0$，故 $|q|\geqslant 1$，故 $|b|\leqslant |a|$；

(vi) 因 $b\mid a$，故 $a=bq$，由(v)知，若 $a\neq 0$，则 $|b|\leqslant |a|$ 与 $|a|<|b|$ 矛盾，故 $a=0$.

例 1.1.1 已知 $a,b,c,d,t\in \mathbf{Z}$，且 $t\mid 10a-b,t\mid 10c-d$. 求证：$t\mid ad-bc$.

证 因 $ad-bc=c(10a-b)-a(10c-d)$，又 $t\mid 10a-b,t\mid 10c-d$，故 $t\mid ad-bc$.

例 1.1.2 设 a,b 是两个给定的非零整数，且有整数 x,y，使得 $ax+by=1$. 求证：若 $a\mid n,b\mid n$，则 $ab\mid n$.

证 因为 $n = n(ax+by) = nax + nby$，又 $ab \mid na$，$ab \mid nb$，所以 $ab \mid n$.

例 1.1.3 已知 $a,b,c,d \in \mathbf{Z}$，且 $a-c \mid ab+cd$. 求证：$a-c \mid ad+bc$.

证 因为 $a-c \mid (a-c)(b-d)$，所以 $a-c \mid ab+cd-(ad+bc)$，又 $a-c \mid ab+cd$，故 $a-c \mid ad+bc$.

习 题 1.1

1. 证明：若 $3 \mid n$ 且 $7 \mid n$，则 $21 \mid n$.

2. 证明：设 $a = 2k-1$，$k \in \mathbf{Z}$，若 $a \mid 2n$，则 $a \mid n$.

3. 证明：设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 是整系数多项式，若 $d \mid b-c$，则 $d \mid f(b) - f(c)$.

4. 证明：若 $m-p \mid mn+pq$，则 $m-p \mid mq+np$.

5. 在已知数列 1,4,8,10,16,19,21,25,30,43 中，相邻若干个数之和能被 11 整除的数组共有多少组？

6. 已知 $6 \mid a+b+c$. 求证：$6 \mid a^3+b^3+c^3$.

1.2 素数与合数

定义 1.2.1 若整数 $a \neq 0, \pm 1$，并且只有约数 $\pm 1, \pm a$，则称 a 是素数（或质数），否则称 a 为合数.

注意：① 素数也称为不可约数，它总是指正整数；② 由定义知，全体正整数可以分为 1、素数、合数三类.

定理 1.2.1 任何大于 1 的整数 a 都至少有一个素约数.

证 若 a 是素数，则定理是显然的.

若 a 不是素数，那么它有两个以上的正的非平凡约数，可设它们为 $d_1, d_2, \cdots, d_k (k \geqslant 2)$. 不妨设 d_1 是其中最小的，若 d_1 不是素数，则存在 e_1, e_2，使得 $d_1 = e_1 e_2$，因此，e_1 和 e_2 也是 a 的正的非平凡约数，这与 d_1 的最小性矛盾.

推论 1.2.1 如果 a 是大于 1 的正整数，则 a 的大于 1 的最小约数必为素数.

推论 1.2.2 任何大于 1 的合数 a 必有一个不超过 $\sqrt{a}$ 的素约数.

证 若 $a = d_1 d_2$，其中 $d_1 > 1$ 是最小素约数，则 $d_1^2 \leqslant a$，所以结论成立.

定理 1.2.2 素数的个数是无限的.

证 假设正整数中只有有限个素数，设为 $p_1, p_2, \cdots, p_k$.

令 $N = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$，则 $N > 1$，由定理 1.2.1 知，N 有一素因数 p，这里 $p \neq p_i (i = 1,2,\cdots,k)$，否则 $p \mid p_1 \cdot p_2 \cdot \cdots \cdot p_k$，又因 $p \mid N = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$，故 $p \mid 1$，这与 p 是素数矛盾，所以 p 是上面 k 个素数以外的素数，得证.

例 1.2.1 设 $A=\{d_1,d_2,\cdots,d_k\}$ 是 n 的所有约数的集合，则 $B=\left\{\frac{n}{d_1},\frac{n}{d_2},\cdots,\frac{n}{d_k}\right\}$ 也是 n 的所有约数的集合.

证 注意下列三点：(1) A 和 B 的元素个数相同；

(2) 若 $d_i\in A$，即 $d_i\mid n$，则 $\frac{n}{d_i}\mid n$，反之亦然；

(3) 若 $d_i\neq d_j$，则 $\frac{n}{d_i}\neq\frac{n}{d_j}$. 易知结论成立.

例 1.2.2 以 $d(n)$ 表示 n 的正约数的个数. 例如 $d(1)=1,d(2)=2,d(3)=2,d(4)=3,\cdots$. 问 $d(1)+d(2)+\cdots+d(2005)$ 是否为偶数？

解 对于 n 的每个约数 d，都有 $n=d\cdot\frac{n}{d}$，因此，n 的正约数 d 与 $\frac{n}{d}$ 是成对出现的，只有当 $d=\frac{n}{d}$，即 $n=d^2$ 时，d 与 $\frac{n}{d}$ 才是同一个数，故当且仅当 n 是完全平方数时，$d(n)$ 是奇数.

由于 $44^2<2005<45^2$，所以在 $d(1),d(2),\cdots,d(2005)$ 中恰好有 44 个奇数，因此 $d(1)+d(2)+\cdots+d(2005)$ 为偶数.

例 1.2.3 若 n 是奇数，则 $8\mid n^2-1$.

证 令 $n=2k+1$，则 $n^2-1=4k(k+1)$，k 与 $k+1$ 一奇一偶，故 $8\mid n^2-1$.

例 1.2.4 用例 1.2.2 中的记号，问 $d^2(1)+d^2(2)+\cdots+d^2(2005)$ 被 4 除的余数是多少？

解 由例 1.2.2 知，$d(1),d(2),\cdots,d(2005)$ 中有 44 个奇数，不妨设为 $a_i(i=1,2,\cdots,44)$ 其余都是偶数. 又 $4\mid(a_1^2-1)+(a_2^2-1)+\cdots+(a_{44}^2-1)+44$，所以，所求余数是 0.

例 1.2.5 设 $a_1,a_2,\cdots,a_n$ 是整数，且 $a_1+a_2+\cdots+a_n=0$，$a_1a_2\cdots a_n=n$，则 $4\mid n$.

证 若 n 是奇数，则 $a_1,a_2,\cdots,a_n$ 都是奇数，故 $a_1+a_2+\cdots+a_n=0$ 不可能，所以 $2\mid n$. 即在 $a_1,a_2,\cdots,a_n$ 中至少有一个偶数.

如果只有一个偶数，不妨设为 a_1，则 2 不整除 $a_i(2\leqslant i\leqslant n)$. 由 $a_2+a_3+\cdots+a_n=-a_1$ 知，左边是 $(n-1)$ 个奇数的和，右边是偶数，这是不可能的. 所以，在 $a_1,a_2,\cdots,a_n$ 中至少有两个偶数，即 $4\mid n$.

例 1.2.6 试找出 2005 个连续的合数.

解 令 $N=2006!$，则 $N+2,N+3,N+4,\cdots,N+2006$ 均为合数.

注意：一般地，n 个相邻的合数是 $(n+1)!+2,(n+1)!+3,\cdots,(n+1)!+n+1$.

习 题 1.2

1. 设 r 是正奇数. 证明：对任意的正整数 n，有 $n+2\nmid 1^r+2^r+\cdots+n^r$.

2. 证明：存在无穷多个正整数 a，使得 $n^4+a(n=1,2,\cdots)$ 都是合数.

3. 证明：存在无穷多个自然数 n，使得 n 不能表示为 $a^2+p(a>0$ 是整数，p 为素数）的形式.

4. 设 p 是 n 的最小素约数，$n=pn_1,n_1>1$. 证明：若 $p>\sqrt[3]{n}$，则 n_1 是素数.

5. 设 a 是自然数，问 a^4-3a^2+9 是素数还是合数？

6. 若 n 是合数. 证明：n 位数 $\underbrace{11\cdots1}_{n个}$ 也是合数.

7. 试证：形如 $3n+2$ 的素数有无穷多个.

8. 求三个素数，使得它们的积为和的 5 倍.

1.3 带余数除法

定理 1.3.1 若 a,b 是两个整数，且 $b>0$，则存在两个整数 q 及 r，使得

$$a=qb+r \quad (0\leqslant r<b) \tag{1.3.1}$$

成立，且 q 和 r 是唯一的. 式中，q 称为 a 被 b 除的商；r 称为 a 被 b 除的余数.

证 作整数序列

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

则 a 必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

$$a=bq+r \quad (0\leqslant r<b)$$

下面证明 q,r 的唯一性，设 q_1,r_1 是满足 $a=bq+r\ (0\leqslant r<b)$ 的两个整数，则

$$a=bq_1+r_1 \quad (0\leqslant r_1<b)$$

因而

$$bq+r=bq_1+r_1$$

于是

$$b(q-q_1)=r_1-r$$

故

$$b|q-q_1|=|r_1-r|$$

由于 $0\leqslant r,r_1<b$，所以上式右边是小于 b 的. 如果 $q\neq q_1$，则上式左边大于等于 b. 这是不可能的，因此 $q=q_1,r_1=r$.

例 1.3.1 设 $a,b,x,y\in\mathbf{Z},k$ 和 m 是正整数，并且 $a=a_1m+r_1\ (0\leqslant r_1<m)$，$b=b_1m+r_2\ (0\leqslant r_2<m)$，则 $ax+by$ 和 ab 被 m 除的余数分别与 r_1x+r_2y 和 r_1r_2 被 m 除的余数相同. 特别地，a^k 与 r_1^k 被 m 除的余数相同.

证 因为

$$ax+by=(a_1m+r_1)x+(b_1m+r_2)y$$
$$=(a_1x+b_1y)m+(r_1x+r_2y)$$

若 r_1x+r_2y 被 m 除的余数是 r，即

$$r_1x+r_2y=qm+r \quad (0\leqslant r<m)$$

则

$$ax+by=(a_1x+b_1y+q)m+r \quad (0\leqslant r<m)$$

即 $ax+by$ 被 m 除的余数也是 r. 同理可证其他结论.

例 1.3.2 任给的 5 个整数中，必有 3 个数之和被 3 整除.

证 设

$$a_i=3q_i+r_i \quad (0\leqslant r_i<3, i=1,2,3,4,5)$$

(1) 若在 r_i 中数 0,1,2 都出现，不妨设 $r_1=0, r_2=1, r_3=2$，则 $a_1+a_2+a_3=3(q_1+q_2+q_3)+3$ 成立；

(2) 若在 r_i 中数 0,1,2 至少有一个不出现，则至少有三个 r_i 取相同的值，令 $r_1=r_2=r_3=r(r=0,1$ 或 $2)$，则 $a_1+a_2+a_3=3(q_1+q_2+q_3)+3r$ 成立.

例 1.3.3 设 $a_0,a_1,\cdots,a_n\in\mathbf{Z}, f(x)=a_nx^n+\cdots+a_1x+a_0$. 已知 $f(0)$ 与 $f(1)$ 都不是 3 的倍数. 证明：若方程 $f(x)=0$ 有整数解，则 $3\mid f(-1)$.

证 对于任意整数 x，都有

$$x=3q+r \quad (0\leqslant r<3)$$

(1) 若 $r=0$，即 $x=3q$，则

$$f(x)=f(3q)=a_n(3q)^n+\cdots+a_1(3q)+a_0$$
$$=3Q_1+a_0=3Q_1+f(0), \quad Q_1\in\mathbf{Z}$$

因为 $f(0)$ 不是 3 的倍数，所以 $f(x)\neq 0$；

(2) 若 $r=1$，即 $x=3q+1$，则

$$f(x)=f(3q+1)=a_n(3q+1)^n+\cdots+a_1(3q+1)+a_0$$
$$=3Q_2+a_n+\cdots+a_1+a_0=3Q_2+f(1), \quad Q_2\in\mathbf{Z}$$

同理，可知

$$f(x)\neq 0$$

综上，若 $f(x)=0$ 有整数解，则

$$x=3q'+2=3q-1$$

于是

$$0=f(x)=f(3q-1)$$
$$=a_n(3q-1)^n+\cdots+a_1(3q-1)+a_0$$
$$=3Q_3+a_0-a_1+a_2-\cdots+(-1)^na_n$$
$$=3Q_3+f(-1), \quad Q_3\in\mathbf{Z}$$

所以

$$3\mid f(-1)$$

习　题　1.3

1. 设 $3|a^2+b^2$. 证明：$3|a$ 且 $3|b$.

2. 设 n,k 是正整数. 证明：n^k 与 n^{k+4} 的个位数字相同.

3. 证明：对于任何整数 n,m，等式 $n^2+(n+1)^2=m^2+2$ 不可能成立.

4. 已知 n 是整数. 证明：$3|n(n+1)(2n+1)$.

5. 证明：形如 $3n-1$ 的数不是平方数.

6. 证明：对任意的整数 x,y，$x^2+y^2\neq 4k+3$，其中 k 为整数.

7. 已知 $9|a^2+b^2+c^2$. 求证：$9|a^2-b^2$ 或 $9|a^2-c^2$ 或 $9|b^2-c^2$.

8. 若 ax_0+by_0 是形如 $ax+by$（x,y 是任意整数，a,b 是两个不全为零的整数）的数中的最小正数，则 $(ax_0+by_0)|(ax+by)$，其中 x,y 是任意整数.

9. 若 a,b 是任意两个整数，且 $b\neq 0$. 证明：存在两个整数 s,t 使得 $a=bs+t\left(|t|\leqslant\frac{|b|}{2}\right)$ 成立. 并且当 b 是奇数时，s,t 是唯一存在的. 当 b 是偶数时，结果又如何？

1.4　最大公约数

定义 1.4.1　整数 $a_1,a_2,\cdots,a_k(k\geqslant 2)$，若整数 d 是它们之中每一个数的因数，那么 d 就叫做 $a_1,a_2,\cdots,a_k$ 的一个公因数. 整数 $a_1,a_2,\cdots,a_k$ 的公因数中最大的一个叫做最大公因数（或最大公约数），记作 $(a_1,a_2,\cdots,a_k)$. 若 $(a_1,a_2,\cdots,a_k)=1$，就说 $a_1,a_2,\cdots,a_k$ 互质或互素. 若 $a_1,a_2,\cdots,a_k$ 中每两个整数互质，就说它们两两互质.

定理 1.4.1　(i) $(a_1,a_2,\cdots,a_k)=(|a_1|,|a_2|,\cdots,|a_k|)$；

(ii) $(a,1)=1,(a,0)=|a|,(a,a)=|a|$；

(iii) $(a,b)=(b,a)$；

(iv) 若 p 是素数，a 是整数，则 $(p,a)=1$ 或 $p|a$；

(v) 若 $a=pb+r$，则 $(a,b)=(b,r)$.

证　(i) 设 d 是 $a_1,a_2,\cdots,a_k$ 的任一公因数，即 $d|a_i(i=1,2,\cdots,k)$. 显然 $d\big||a_i|(i=1,2,\cdots,k)$，故 d 也是 $|a_1|,|a_2|,\cdots,|a_k|$ 的一个公因数.

同理可证，$|a_1|,|a_2|,\cdots,|a_k|$ 的任一公因数 d' 也是 $a_1,a_2,\cdots,a_k$ 的一个公因数，这样就可证得 $|a_1|,|a_2|,\cdots,|a_k|$ 与 $a_1,a_2,\cdots,a_k$ 有相同的公因数，因而它们的最大公因数也相同，即 $(a_1,a_2,\cdots,a_k)=(|a_1|,|a_2|,\cdots,|a_k|)$.

(ii)，(iii) 显然成立；

(iv) 设$(p,a)=d$,则$d|p,d|a$,由$d|p$得$d=1$或p,前者推出$(p,a)=1$,后者推出$p|a$;

(v) 若$d|a,d|b$,则$d|r=a-pb$. 反之,若$d|b,d|r$,则$d|a=pb+r$. 因此a与b的全体公约数的集合就是b与r的全体公约数的集合,这两个集合中最大正整数当然相等,所以$(a,b)=(b,r)$.

定理 1.4.2 若$a,b(b>0)$是任意两个整数,且

$$\begin{aligned}
&a=bq_1+r_1 \quad (0<r_1<b)\\
&b=r_1q_2+r_2 \quad (0<r_2<r_1)\\
&\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n \quad (0<r_n<r_{n-1})\\
&r_{n-1}=r_nq_{n+1}+r_{n+1} \quad (r_{n+1}=0)
\end{aligned} \tag{1.4.1}$$

则

$$(a,b)=r_n$$

证 $r_n=(0,r_n)=(r_{n+1},r_n)=(r_n,r_{n-1})=\cdots=(r_1,b)=(a,b)$.

定理 1.4.3 设a,b是任意两个不全为零的整数.

(i) 若m是任意一个正整数,则

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

(ii) 若δ是a,b的任意一个公约数,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 (i) 当a,b中有一个为0时,定理显然成立,设a,b都不为0. 由定理1.4.1,有

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

即

$$(a,b)m=(|a|,|b|)m$$

因此不妨假设a,b都是正整数. 在式(1.4.1)中,把各式两边同乘以m,即得

$$\begin{aligned}
&am=(bm)q_1+r_1m \quad (0<r_1m<bm)\\
&bm=(r_1m)q_2+r_2m \quad (0<r_2m<r_1m)\\
&\cdots\cdots\\
&r_{n-2}m=(r_{n-1}m)q_n+r_nm \quad (0<r_nm<r_{n-1}m)\\
&r_{n-1}m=(r_nm)q_{n+1}
\end{aligned}$$

由定理1.4.2得

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

因而得证;

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

所以$\left(\frac{a}{\delta},\frac{b}{\delta}\right) = \frac{(a,b)}{|\delta|}$成立. 当$\delta = (a,b)$时,上式即

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right) = 1$$

例 1.4.1 证明:若n是正整数,则$\frac{21n+4}{14n+3}$是既约分数.

证 由$a = bq + r\ (0 \leqslant r < b)$,则$(a,b) = (b,r)$,得

$$(21n+4,14n+3) = (7n+1,14n+3) = (7n+1,1) = 1$$

所以,$\frac{21n+4}{14n+3}$是既约分数.

例 1.4.2 设a,b是整数,且$9 \mid a^2 + ab + b^2$,则$3 \mid (a,b)$.

证 因$9 \mid a^2 + ab + b^2$,则$9 \mid (a-b)^2 + 3ab$,故$3 \mid (a-b)^2 + 3ab$,即$3 \mid (a-b)^2$,即$3 \mid a-b$,即$9 \mid (a-b)^2$,即$9 \mid 3ab$,即$3 \mid ab$,故$3 \mid a$或$3 \mid b$.

若$3 \mid a$,且$3 \mid a-b$,故$3 \mid b$;若$3 \mid b$,且$3 \mid a-b$,故$3 \mid a$;故$3 \mid (a,b)$.

例 1.4.3 证明:$121 \nmid n^2 + 2n + 12, n \in \mathbf{Z}$.

证 若$121 \mid n^2 + 2n + 12 = (n+1)^2 + 11$,则$11 \mid (n+1)^2 + 11$,故$11 \mid (n+1)^2$,即$11 \mid n+1$,则$121 \mid (n+1)^2$,又$121 \mid (n+1)^2 + 11$,故$121 \mid 11$,这是不可能的,故$121 \nmid n^2 + 2n + 12, n \in \mathbf{Z}$.

例 1.4.4 证明本节例 1.4.1 中的$n \leqslant \frac{2\log b}{\log 2}$.

证 对$a = bq_1 + r_1\ (0 < r_1 < b)$,有$a > 2r_1$,则

$$b > r_1$$

同理,$b = r_1 q_2 + r_2\ (0 < r_2 < r_1)$,则

$$b > 2r_2$$

$r_1 = r_2 q_3 + r_3\ (0 < r_3 < r_2)$,则

$$r_1 > 2r_3$$

……

$r_{n-2} = r_{n-1} q_n + r_n\ (0 < r_n < r_{n-1})$,则

$$r_{n-2} > 2r_n$$

把以上不等式相乘得

$$b^2 r_1 \cdot \cdots \cdot r_{n-2} > 2^{n-1} r_1 \cdot \cdots \cdot r_n$$

即

$$b^2 > 2^{n-1} r_{n-1} \cdot r_n$$

则