信息与计算科学教学丛书

初等数论
（第二版）

胡典顺　徐汉文　编著

科学出版社

信息与计算科学教学丛书

初等数论

（第二版）

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、连分数等. 书中配有大量例题和不同层次的习题，并且每个例题和习题都提供了详细的解答，供教师教学和学生学习时选用.

本书可作为高等院校数学与应用数学相关专业的教材，也可作为数学竞赛的参考用书，还可供高中数学教师及数学爱好者参考.

图书在版编目(CIP)数据

初等数论/胡典顺，徐汉文编著. —2版. —北京：科学出版社，2017.8

(信息与计算科学教学丛书)

ISBN 978-7-03-054126-0

Ⅰ.①初… Ⅱ.①胡… ②徐… Ⅲ.①初等数论 Ⅳ.①O156.1

中国版本图书馆CIP数据核字(2017)第191539号

责任编辑：高 嵘 王 晶/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印刷

科学出版社发行 各地新华书店经销

*

2010年6月第 一 版 开本：787×1092 1/16

2017年8月第 二 版 印张：13

2017年8月第一次印刷 字数：310 000

定价：32.00元

(如有印装质量问题，我社负责调换)

第二版前言

《初等数论》第一版自 2010 年出版以来已经过多次印刷，很多读者对本书给予了积极的评价，不少高校教师选用本书作为《初等数论》这一门课程的教材. 这一切对我们来说既是一种激励，也是一种鞭策，促使我们对第一版进行修改，本次修订就是结合读者反馈意见的基础上进行的.

第二版《初等数论》在框架结构上没有本质的变化，主要变化体现在以下几个方面：

1. 对第一版的疏漏进行了修改；

2. 对相关章节内容结构进行了适当调整，包括删除相关内容和增补了一些新内容，从而使本书内容更加丰富，方便教师的教学；

3. 第一版教材中所有习题都给出了详细的解答，在第二版教材中，考虑到不同学校教师教学的需求，书末为第 1～5 章增加了一个新的部分，即“挑战自我”. 这部分题目都有一定难度，不少题目选自不同级别的数学竞赛题目，题目没有给出答案，供学有余力的同学课后思考. 同时，这部分内容也可以作为老师在课堂上开展研究性学习，让大家共同探索，进一步提高同学们学习本课程的兴趣.

最后，我们向支持本书出版的科学出版社表示衷心感谢！

我们将向采纳本书作为教材的教师免费提供 PowerPoint 课件，请发邮件至：hdsh@mail. ccnu. edu. cn 联系.

胡典顺

2016 年 3 月

第一版前言

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教授提出了宝贵的意见和建议；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。

胡典顺

2010 年 3 月

目　录

第1章　整除理论

1.1　整除的性质

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 $1,-1,a,-a$，这四个数称为 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

(1) $a\mid b\Rightarrow \pm a\mid \pm b$;

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

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

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

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

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

证明　(1) 因 $a\mid b$，故 $b=aq$，即 $\pm b=\pm aq$，故 $\pm a\mid \pm b$;

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

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

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

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

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

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

(4) 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）;

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

(6) 因 $b\mid a$，故 $a=bq$，由(5)知，若 $a\neq 0$，则 $|b|\leqslant |a|$ 与 $|a|<|b|$ 矛盾，因此 $a=0$.

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：$t\mid ad-bc$.

证明　$ad-bc=c(10a-b)-a(10c-d)$，因 $t\mid 10a-b,t\mid 10c-d$，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 $ab\mid n$.

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

例 1.1.3　试证任意一个整数与它的各位数字之和的差能被 9 整除，且这个整数与其数字作任意顺序调换后所成的整数的差，也能被 9 整除.

证明 不妨设 $m>0$,且 $m=a_1+10a_2+\cdots+10^{n-1}a_n$. 则

$$m-(a_1+a_2+\cdots+a_n)=9(a_2+11a_3+\cdots+\underbrace{11\cdots1}_{n-1\text{个}})$$

易知 $$9\mid m-(a_1+a_2+\cdots+a_n).$$

设 $b_1,b_2,\cdots,b_n$ 是 $a_1,a_2,\cdots,a_n$ 的另一个排列,$m'=b_1+10b_2+\cdots+10^{n-1}b_n$.

记 $\alpha=a_1+a_2+\cdots+a_n$,则 $\alpha=b_1+b_2+\cdots+b_n$.

已证 $9\mid m-\alpha$. 则 $9\mid m'-\alpha$,则必有 $9\mid m-m'$.

习 题 1.1

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

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

3. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整系数多项式,若 $d\mid b-c$,则 $d\mid f(b)-f(c)$.

4. 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 $a\neq0,\pm1$,并且只有约数 $\pm1,\pm a$,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三类:1、素数、合数.

定理 1.2.1 任何大于 1 的整数 a 都至少有一个素约数.

证明 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 $d_1,d_2,\cdots,d_k$ $(k\geqslant2)$. 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 $d_1=e_1e_2$,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.

证明 若 $a=d_1d_2$,其中 $d_1>1$ 是最小素约数,则 $d_1^2\leqslant a$,因此结论成立.

定理 1.2.2 素数的个数是无限的.

证明 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 $p\mid1$,这与 p 是素数矛盾. 因此 p 是上面 k 个素数以外的素数,得证.

定理 1.2.3　若 p 是一质数，a 是任一整数，则 a 能被 p 整除或 p 与 a 互质.

证明　因为 $(p,a)\mid p$，$(p,a)>0$，由素数的定义 $(p,a)=1$ 或 $(p,a)=p$，所以 $(p,a)=1$ 或 $p\mid a$.

推论 1.2.3　设 $a_1,a_2,\cdots,a_n$ 是 n 个整数，p 是素数，若 $p\mid a_1a_2\cdots a_n$，则 p 一定能整除某一个 a_i.

证明　假设 $a_1,a_2,\cdots,a_n$ 都不能被 p 整除，则由定理 1.2.3 知，$(p,a_i)=1$ $(i=1,2,\cdots,n)$. 因此 $(p,a_1a_2\cdots a_n)=1$，这与 $p\mid a_1a_2\cdots a_n$ 矛盾，结论成立.

定理 1.2.4　任何大于 1 的整数 a 可以写成素数之积，即 $a=p_1p_2\cdots p_n$，其中 p_i $(1\leqslant i\leqslant n)$是素数.

证明　当 a 是素数时，定理成立；当 a 是合数时，则必存在素数 p_1，且 $1<p_1\leqslant\sqrt{a}$，故 $a=p_1a_1$ $(1<a_1<a)$.

若 a_1 是素数，则可知定理成立；若 a_1 是合数，同理，则必有素数 p_2，以及适合 $1<a_2<a_1$ 的正整数 a_2，使 $a=p_1p_2a_2$ 成立. 由于 a 是有限的，所以有限次地重复上述过程可得 $a=p_1p_2\cdots p_n$，其中 $p_1,p_2,\cdots,p_n$ 均为素数.

定理 1.2.5(算术基本定理)　任何大于 1 的整数 a 可以唯一地表示成

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} \tag{1.2.1}$$

其中，$p_1,p_2,\cdots,p_n$ 是素数，$p_1<p_2<\cdots<p_n$，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是正整数.

证明　由定理 1.2.4 知，任何大于 1 的整数可表示成(1.2.1)的形式，因此，只需证明式(1.2.1)的唯一性. 事实上，只需证明定理 1.2.4 中表达形式的唯一性.

假设 p_i $(1\leqslant i\leqslant n)$ 与 q_i $(1\leqslant i\leqslant k)$ 都是素数，$p_1<p_2<\cdots<p_n$，$q_1<q_2<\cdots<q_k$，且 $a=p_1p_2\cdots p_n=q_1q_2\cdots q_k$，又 $p_1\mid a=q_1q_2\cdots q_k$，则必有某个 q_j，使得 $p_1\mid q_j$，从而 $p_1=q_j$. 同理，又有某个 p_i，使得 $q_1\mid p_i$，所以 $q_1=p_i$. 又 $p_1\leqslant p_2\leqslant\cdots\leqslant p_n$，$q_1\leqslant q_2\leqslant\cdots\leqslant q_k$，可知 $p_1=q_1$.

重复上述过程，得到 $n=k$，$p_i=q_i$，结论成立.

定理 1.2.5 中的记号 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 是 a 的标准分解式.

推论 1.2.4　设 a 是一个大于 1 的整数，且 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，$\alpha_i$ $(i=1,2,\cdots,n)$是正整数，则 a 的正因数 d 可以表示成 $d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ $(\alpha_i\geqslant\beta_i\geqslant0,i=1,2,\cdots,n)$的形式.

证明　若 $d\mid a$，则 $a=dq$，又 a 的标准分解式是唯一的，故 d 的标准分解式中出现的素数都在 p_j $(1\leqslant j\leqslant n)$中出现，且 p_j 在 d 的标准分解式中出现的指数 $\beta_j\leqslant\alpha_j$. 反过来，当 $\beta_j\leqslant\alpha_j$ 时，显然 d 整除 a.

推论 1.2.5　设 a,b 是任意两个正整数，且

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},\quad b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}\quad(\alpha_i\geqslant0,\beta_i\geqslant0;\ i=1,2,\cdots,n)$$

则

$$(a,b)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_n^{\gamma_n},\quad [a,b]=p_1^{\delta_1}p_2^{\delta_2}\cdots p_n^{\delta_n}$$

其中

$$\gamma_i=\min\{\alpha_i,\beta_i\},\quad \delta_i=\max\{\alpha_i,\beta_i\}\quad(i=1,2,\cdots,n)$$

注意：已知 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 是 a 的标准分解式，则 a 的不同的正约数个数等于 $(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_n)$.

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.

证明 (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 $\frac{n}{d_i}\neq\frac{n}{d_j}$.

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 $d(1)+d(2)+\cdots+d(2\,005)$ 是否为偶数?

解 因为 n 的每个约数 d,都有 $n=d\cdot\frac{n}{d}$,所以 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. 因此当且仅当 n 是完全平方数时,$d(n)$ 是奇数.

因为 $44^2<2\,005<45^2$,所以在 $d(1),d(2),\cdots,d(2\,005)$ 中恰好有 44 个奇数,因此 $d(1)+d(2)+\cdots+d(2\,005)$ 为偶数.

例 1.2.3 若 n 是奇数,则 $8\mid n^2-1$.

证明 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 $d^2(1)+d^2(2)+\cdots+d^2(2\,005)$ 被 4 除的余数是多少?

解 由例 1.2.2 知,$d(1),d(2),\cdots,d(2\,005)$ 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 $4\mid n$.

证明 若 n 是奇数,则 $a_1,a_2,\cdots,a_n$ 都是奇数,则 $a_1+a_2+\cdots+a_n=0$ 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 假设 $n>2$,试证:n 与 $n!$ 之间至少有一个素数.

证明 设不大于 n 的素数为 $p_1,p_2,\cdots,p_k$,作 $q=p_1\cdot p_2\cdot\cdots\cdot p_k-1$,显然 q 有异于 p_i 的素因数 p,易知 $p>n$,又 $p<q<n!-1<n!$. 即 p 为满足条件的素数.

例 1.2.7 证明:在 $1,2,\cdots,2n$ 中任取 $n+1$ 个数,其中至少有一个能被另一个整除.

证明 记 $i=2^{a_i}\lambda_i$,$2\nmid\lambda_i$,$i=1,2,\cdots,2n$,则 λ_i 为 $1,2,\cdots,2n$ 中的奇数,即 λ_i 只能取 n 个数值,在 $n+1$ 个这样的数中,必存在 $\lambda_i=\lambda_j$ $(i\neq j)$,于是易知,i 与 j 成倍数关系.

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. 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.

4. 设 a 是自然数，问 a^4-3a^2+9 是素数还是合数？

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

6. 试证：形如 $3n+2$ 的素数有无穷多个.

7. 求三个素数，使得它们的积为和的 5 倍.

8. (1) 迪波瓦尔(DeBouvelles)曾断言：对所有 $n\geqslant1$，$6n-1$ 和 $6n+1$ 中至少有一个是素数. 举例说明他的断言错了；

(2) 证明：有无穷多 n 个，使 $6n-1$ 和 $6n+1$ 同时为合数.

9. 设 a,b 是正整数. 证明：$(a,b)[a,b]=ab$.

10. 设 a,b 是正整数. 证明：存在 a_1,a_2,b_1,b_2，使得 $a=a_1a_2,b=b_1b_2,(a_2,b_2)=1$，并且 $[a,b]=a_2b_2$.

1.3　最大公约数

定义 1.3.1　整数 $a_1,a_2,\cdots,a_k$ $(k\geqslant2)$，若整数 d 是它们之中每一个数的因数，那么 d 就称为 $a_1,a_2,\cdots,a_k$ 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称为最大公因数(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 1.3.1　(1) $(a_1,a_2,\cdots,a_k)=(|a_1|,|a_2|,\cdots,|a_k|)$；

(2) $(a,1)=1,(a,0)=|a|,(a,a)=|a|$；

(3) $(a,b)=(b,a)$；

(4) 若 p 是素数，a 是整数，则 $(p,a)=1$ 或 $p\mid a$；

(5) 若 $a=pb+r$，则 $(a,b)=(b,r)$.

证明　(1) 设 d 是 $a_1,a_2,\cdots,a_k$ 的任一公因数，即 $d\mid a_i(i=1,2,\cdots,k)$. 显然 $d\mid|a_i|$ $(i=1,2,\cdots,k)$，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 $(a_1,a_2,\cdots,a_k)=(|a_1|,|a_2|,\cdots,|a_k|)$.

(2)，(3) 显然成立；

(4) 设 $(p,a)=d$，则 $d\mid p,d\mid a$，由 $d\mid p$ 得 $d=1$ 或 p，前者推出 $(p,a)=1$，后者推出 $p\mid a$；

(5) 若 $d\mid a,d\mid b$，则 $d\mid r=a-pb$. 反之，若 $d\mid b,d\mid r$，则 $d\mid a=pb+r$. 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 1.3.2　若 a,b $(b>0)$ 是任意两个整数，且

$$\begin{aligned}
&a = bq_1 + r_1, 0 < r_1 < b\\
&b = r_1q_2 + r_2, 0 < r_2 < r_1\\
&\cdots\cdots\\
&r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}\\
&r_{n-1} = r_nq_{n+1} + r_{n+1}, r_{n+1} = 0
\end{aligned} \tag{1.3.1}$$

则

$$(a,b) = r_n$$

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

定理 1.3.3 设 a,b 是任意两个不全为零的整数.

(1) 若 m 是任意一个正整数,则

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

(2) 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

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

证明 (1) 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 1.3.1,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(1.3.1)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 1.3.2,得

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

因而得证;

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

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

证明 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，$\dfrac{21n+4}{14n+3}$ 是既约分数.

例 1.3.2　设 a,b 是整数，且 $9 \mid a^2+ab+b^2$，则 $3 \mid (a,b)$.

证明　因 $9 \mid a^2+ab+b^2$，则 $9 \mid (a-b)^2+3ab$，故 $3 \mid (a-b)^2+3ab$，即 $3 \mid (a-b)^2$，$3 \mid a-b$，$9 \mid (a-b)^2$，$9 \mid 3ab$，$3 \mid ab$. 因此 $3 \mid a$ 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 1.3.3　设 $m,n>0$，$mn \mid (m^2+n^2)$，则 $m=n$.

证明　设 $(m,n)=d$，则 $m=m_1d$，$n=n_1d$，其中 $(m_1,n_1)=1$. 于是，已知条件转化为 $m_1n_1 \mid (m_1^2+n_1^2)$，有 $m_1 \mid (m_1^2+n_1^2)$，从而转化为 $m_1 \mid n_1^2$. 但是，因 $(m_1,n_1)=1$，故 $(m_1,n_1^2)=1$，结合 $m_1 \mid n_1^2$ 知，必有 $m_1=1$，同时 $n_1=1$，因此 $m=n$.

例 1.3.4　证明定理 1.3.2 中的 $n \leqslant \dfrac{2\lg b}{\lg 2}$.

证明　对 $a=bq_1+r_1$，$0<r_1<b$，有 $a>2r_1$，则

$$b>r_1$$

同理，$b=r_1q_2+r_2$，$0<r_2<r_1$，则

$$b>2r_2$$

$r_1=r_2q_3+r_3$，$0<r_3<r_2$，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

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

即

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

则

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

得证.

习　题　1.3

1. 求(1) $(-1857,1573)$；

(2) $(30,45,84)$；

(3) $(2n-1,n-2)$.

2. 证明：若 $a>0$ 且 $(b,c)=1$，则 $(a,bc)=(a,b)(a,c)$.

3. 证明：若 $(a,4)=(b,4)=2$，则 $(a+b,4)=4$.

4. 证明：$(a,b,c)(ab,bc,ca)=(a,b)(b,c)(c,a)$.

5. 若$(a,b)=1,c\mid a+b$,则$(c,a)=(c,b)=1$.

6. 证明:从任意5个互素的三位数中,能选出4个数是互素的.

7. 设k,l是给定的两个正整数.证明:有无穷多个正整数$m\geqslant k$,使得C_m^k与l互素.

1.4 最小公倍数

定义 1.4.1 整数$a_1,a_2,\cdots,a_n$的公共倍数称为$a_1,a_2,\cdots,a_n$的公倍数,$a_1,a_2,\cdots,a_n$的正公倍数中的最小的一个称为$a_1,a_2,\cdots,a_n$的最小公倍数,记作$[a_1,a_2,\cdots,a_n]$.

定理 1.4.1 (1) $[a,1]=|a|,[a,a]=|a|$;

(2) $[a,b]=[b,a]$;

(3) $[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]$;

(4) 若$a\mid b$,则$[a,b]=|b|$.

证明 (1),(2)显然;

(3) 设$m_1=[a_1,a_2,\cdots,a_n],m_2=[|a_1|,|a_2|,\cdots,|a_n|]$,则由$a_i\mid m_1$推出$|a_i|\mid m_1$,即$m_2\mid m_1$.同理可得$m_1\mid m_2$,故$m_1=m_2$;

(4) 显然$a\mid|b|,b\mid|b|$,又若$a\mid m',b\mid m',m'>0$,则$|b|\leqslant m'$,故$[a,b]=|b|$.

定理 1.4.2 对任意正整数a,b,有$[a,b]=\dfrac{ab}{(a,b)}$.

证明 设m是a与b的一个公倍数,则

$$m=ak_1,\quad m=bk_2$$

故
$$ak_1=bk_2$$

于是
$$\frac{a}{(a,b)}k_1=\frac{b}{(a,b)}k_2$$

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

故
$$\frac{b}{(a,b)}\mid k_1$$

即
$$k_1=\frac{b}{(a,b)}t\quad(t\text{是整数})$$

从而
$$m=ak_1=\frac{ab}{(a,b)}t$$

另一方面,对于任意的整数t,由$m=\dfrac{ab}{(a,b)}t$所确定的m显然是a与b的公倍数,因此a与b的公倍数必是$m=\dfrac{ab}{(a,b)}t$的形式,当$t=1$时,得到最小公倍数$[a,b]=\dfrac{ab}{(a,b)}$.

推论 1.4.1 两个整数的任何公倍数可以被它们的最小公倍数整除.

证明 因为$m=\dfrac{ab}{(a,b)}t$是a与b的公倍数的形式,且$t=1$时是最小公倍数,所以结论成立.

推论 1.4.2 设m,a,b是正整数,则$[ma,mb]=m[a,b]$.

证明　$$[ma,mb]=\frac{ma\cdot mb}{(ma,mb)}=\frac{m^2ab}{m(a,b)}=\frac{mab}{(a,b)}=m[a,b]$$

定理 1.4.3　若 $a_1,a_2,\cdots,a_n$ 是 n $(n\geqslant 2)$ 个正整数，记 $[a_1,a_2]=m_2,[m_2,a_3]=m_3,\cdots,[m_{n-2},a_{n-1}]=m_{n-1},[m_{n-1},a_n]=m_n$，则 $[a_1,a_2,\cdots,a_n]=m_n$.

证明　由 $[a_1,a_2]=m_2,[m_2,a_3]=m_3,\cdots,[m_{n-1},a_n]=m_n$ 知，$m_i\mid m_{i+1}$ $(i=2,3,\cdots,n-1)$，且 $a_1\mid m_2,a_i\mid m_i$ $(i=2,3,\cdots,n)$，故 m_n 是 $a_1,a_2,\cdots,a_n$ 的一个公倍数；另一方面，设 m 是 $a_1,a_2,\cdots,a_n$ 的任意一个公倍数，则 $a_1\mid m,a_2\mid m$，由推论 1.4.1，得 $m_2\mid m$. 又 $a_3\mid m$，同样由推论 1.4.1，得 $m_3\mid m$. 依此类推，最后可得 $m_n\mid m$，因此 $m_n\leqslant|m|$，$m_n=[a_1,a_2,\cdots,a_n]$.

例 1.4.1　设 a,b,c 是正整数，则 $[a,b,c](ab,bc,ca)=abc$.

证明　由定理 1.4.3 知

$$[a,b,c]=[[a,b],c]$$

又

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

故

$$[a,b,c]=[[a,b],c]=\frac{[a,b]c}{([a,b],c)}$$

又

$$\begin{aligned}(ab,bc,ca)&=(ab,(bc,ca))=(ab,c(a,b))\\&=\left(ab,\frac{abc}{[a,b]}\right)=\frac{(ab[a,b],abc)}{[a,b]}\\&=\frac{ab([a,b],c)}{[a,b]}\end{aligned}$$

以上两式相乘可知结论成立.

例 1.4.2　求正整数 a,b，使得 $a+b=120,(a,b)=24,[a,b]=144$.

解　因 $ab=(a,b)[a,b]=24\times 144=3456$，又 $a+b=120$，故 $a=48,b=72$ 或 $a=72,b=48$.

例 1.4.3　设 a,b 是正整数，证明 $(a+b)[a,b]=a[b,a+b]$.

证明　因 $(a+b)[a,b]=(a+b)\cdot\frac{ab}{(a,b)}=a\cdot\frac{b(a+b)}{(a,b)}$

又

$$b(a+b)=[b,a+b](b,a+b)$$

而

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

故

$$b(a+b)=[b,a+b](a,b)$$

即

$$\frac{b(a+b)}{(a,b)}=[b,a+b]$$

因此结论成立.

例 1.4.4　设 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个整系数多项式，且 a_0,a_n 都不是零，则方程 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ 的有理根只能是以 a_0 的因数作分子，以 a_n 的因数作分母的既约分数，并由此推出整数系多项式 $\sqrt{2}$ 不是有理数.

证明　设 $x=\frac{q}{p}$ 是方程 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ 的有理根，其中 $(p,q)=1$.

把 $x=\frac{q}{p}$ 代入该方程,有

$$\begin{aligned}
&a_n\left(\frac{q}{p}\right)^n+a_{n-1}\left(\frac{q}{p}\right)^{n-1}+\cdots+a_1\frac{q}{p}+a_0=0\\
\Rightarrow&a_nq^n+a_{n-1}q^{n-1}p+\cdots+a_1qp^{n-1}+a_0p^n=0\\
\Rightarrow&a_0p^n=-q(a_nq^{n-1}+a_{n-1}q^{n-2}p+\cdots+a_1p^{n-1})\\
&a_nq^n=-p(a_{n-1}q^{n-1}+a_1qp^{n-2}+\cdots+a_0p^{n-1})\\
\Rightarrow&q\mid a_0p^n,p\mid a_nq^n.
\end{aligned}$$

由 $$(p,q)=1\Rightarrow q\mid a_0,p\mid a_n$$

又 $x^2-2=0$ 以 $\sqrt{2}$ 为正根,而 $x^2-2=0$ 的有理根只能为 $\pm1,\pm2$,它们都不可能等于 $\sqrt{2}$,故 $\sqrt{2}$ 不为有理数.

习 题 1.4

1. 求[221,391,136].
2. $[a,b,c]=abc$ 的充要条件是:$(a,b)=(b,c)=(c,a)=1$.
3. 设 a,b 是正整数.证明:若 $[a,b]=(a,b)$,则 $a=b$.
4. 证明:设 $(m,a)=1$,则 $(m,ab)=(m,b)$.
5. 证明:$(a,uv)\mid(a,u)(a,v)$.

1.5 辗转相除法

定理 1.5.1 若 a,b 是两个整数,且 $b>0$,则存在两个整数 q 及 r,使得 $a=qb+r$ $(0\leqslant r<b)$ 成立,且 q 和 r 是唯一的.

证明 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 $a=bq+r,0\leqslant r<b$.

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 $a=bq_1+r_1$ $(0\leqslant r_1<b)$,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 $\geqslant b$.这是不可能的,因此 $q=q_1,r_1=r$.

定义 1.5.1 设 a 和 b 是整数,$b>0$,依次作带余数除法:

$$\begin{aligned}
&a=bq_1+r_1 && (0<r_1<b)\\
&b=r_1q_2+r_2 && (0<r_2<r_1)\\
&\cdots\cdots && \\
&r_{n-2}=r_{n-1}q_n+r_n && (0<r_n<r_{n-1})\\
&r_{n-1}=r_nq_{n+1}+r_{n+1} && (r_{n+1}=0)
\end{aligned}\tag{1.5.1}$$