高等学校通用教材

初等数论

王丹华　杨海文　刘咏梅　编著

CHUDENG SHULUN

北京航空航天大学出版社

高等学校通用教材

初等数论

王丹华　杨海文　刘咏梅　编著

北京航空航天大学出版社

内容简介

本书共分八章，内容包括整除理论、同余、不定方程、同余方程、二次同余方程、原根和指数、实数的表示以及初等数论应用举例。书中配有大量习题，书末附有答案与提示以及一些与数论相关的阅读材料。

本书积累了作者多年的教学经验，结合国内现有相关文献资料精心组织，编写时力求做到深入浅出、循序渐进、突出重点、结构严谨、例题典型、注重基础和强调适用。

本书可作为高等院校数学专业和计算机相关专业学生的教材，也可供高中数学教师教学参考。

图书在版编目(CIP)数据

初等数论/王丹华，杨海文，刘咏梅编著. —北京：北京航空航天大学出版社，2008.3

ISBN 978-7-81124-275-1

Ⅰ.初… Ⅱ.①王…②杨…③刘… Ⅲ.初等数论 Ⅳ.O156.1

中国版本图书馆 CIP 数据核字(2007)第 192530 号

初等数论

王丹华 杨海文 刘咏梅 编著

责任编辑 宋淑娟

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(100083) 发行部电话：(010)82317024 传真：(010)82328026

http://www.buaapress.com.cn E-mail:bhpress@263.net

北京市松源印刷有限公司印装 各地书店经销

*

开本：787×960 1/16 印张：13.5 字数：302 千字

2008 年 3 月第 1 版 2008 年 3 月第 1 次印刷 印数：4 000 册

ISBN 978-7-81124-275-1 定价：18.00 元

前　言

初等数论是数学的一个源远流长的分支。初等数论也称整数论，主要研究整数的性质和方程的整数解，数论中最经典和最基本的概念、方法及结论构成了初等数论的主要内容。初等数论不仅是数学思维的体操，在当前计算机时代和信息社会中，初等数论和其他离散数学分支（如组合数学、图论和近世代数等）一样，在计算机科学、通信工程、离散控制系统和代数编码等许多领域得到日益广泛的实际应用。初等数论不仅是数学工作者，而且也是许多从事应用和实际工作的工程技术人员不可缺少的数学基础知识。

本书介绍初等数论中整数的整除性、同余、不定方程、同余方程、二次同余方程、原根和指数、实数的表示以及初等数论的应用等内容。它不仅适合作为高等院校数学专业和计算机相关专业学生的教材，也可作为高中数学教师的教学参考书。

本书注重思维与兴趣的融合。每章开始通过引述部分达到各章之间的自然过渡；在章节内容叙述中，对重要方法给出必要的评注，达到深刻理解的目的；每章结尾给予概括性的小结；在本书最后，给出数论中几大经典问题的介绍，以增强教材的可读性。

本书适合教学和自学的双重需要，根据作者多年对初等数论的教学实践，结合高校初等数论课程的教学大纲编写而成，编写时力求做到深入浅出、循序渐进、突出重点、结构严谨、例题典型、注重基础和强调适用。书中在注重基本概念和基本方法的归纳总结的同时，也为每一节安排了丰富的实例和习题，为了减轻习题解题难度，还给出了参考答案或提示。本书第1、4和8章由杨海文执笔，第2、3章由刘咏梅执笔，第5、6和7章由王丹华执笔，附录由杨海文执笔，最后由王丹华和杨海文统纂定稿。本书中打“*”的章节，可视学时情况选讲或不讲。

本教材在编写过程中参考了较多国内现有相关文献资料，同时得到了井冈山大学、江西师范大学领导和北京航空航天大学出版社的大力支持，谨此致以衷心的谢忱。

限于作者水平，不妥之处在所难免，敬请广大读者不吝批评指教。

编　者

2007年9月

目 录

第 1 章　整除理论

本章介绍初等数论的最基础理论——整除理论. 因任何两个整数的和、差、积都是整数，但商却不一定是整数，由此对整数的整除性进行讨论. 整除理论包括整除、带余数除法、辗转相除法、最大公因数与最小公倍数、素数与合数以及算术基本定理，其中算术基本定理和最大公因数性质是整除理论的核心内容，带余数除法是整除理论的重要工具.

1.1　数的整除性

说到数，离不开数的代数运算. 已经知道，两个整数的和、差、积仍然是整数，但是用不等于零的整数去除另一个整数所得的商却不一定是整数. 为此，引入初等数论中的第一个基本概念——数的整除性. 下面从整除的概念、性质及应用来认识数的整除性.

定义　设 a,b 是两个整数，$b\neq 0$，如果存在整数 c，使得 $a=bc$，则称 ***a* 被 *b* 整除或 *b* 整除 *a***，记为 $b\mid a$. 并称 a 是 b 的**倍数**，b 是 a 的**因数**(或**约数**). 如果不存在整数 c，使得 $a=bc$ 成立，则称 ***a* 不被 *b* 整除**或 ***b* 不整除 *a***，记为 $b\nmid a$.

显然，每个非零整数至少有 ± 1 和 $\pm a$ 作为它的因数，称它们为 a 的**平凡因数**；a 的异于 ± 1 和 $\pm a$ 的因数，称为 a 的**非平凡因数**，或 a 的**真因数**.

注　除特别声明外，本书中所用字母都表示整数.

由整除定义易推出如下结论.

定理 1.1.1　设 a,b,c 是整数，下面的结论成立：

(ⅰ) 若 $b\mid c$，且 $c\mid a$，则 $b\mid a$. (整除传递性)

(ⅱ) 若 $b\mid a$，且 $b\mid c$，则对任意整数 k,l，有 $b\mid (ka+lc)$.

一般，若 $b\mid a_i (i=1,2,\cdots,n)$，则 $b\mid (a_1x_1+a_2x_2+\cdots+a_nx_n)$，其中 $x_i (i=1,2,\cdots,n)$ 是任意整数.

(ⅲ) 若 $b\mid a$，且 $c\neq 0$，则 $bc\mid ac$；反之亦然.

(ⅳ) 若 $b\mid a$，$a\neq 0$，则 $|b|\leqslant |a|$；若 $b\mid a$，且 $|a|<|b|$，则 $a=0$；若 $b\mid a$，且 $a\mid b$，$a>0$，$b>0$，则 $a=b$.

证明　(ⅰ)由整除定义及 $b\mid c$，$c\mid a$ 知，存在两个整数 a_1,c_1 使得 $a=a_1c$，$c=c_1b$，因此 $a=(a_1c_1)b$，由于 a_1c_1 是整数，故 $b\mid a$.

(ⅱ) ～ (ⅳ)的结论类似可证.

证毕.

注　为了证明 $b\mid a$，最基本的方法是将 a 分解为 b 与某个整数之积，即 $a=bc$，其中 c 是整

数. 这样的分解,常常通过在某些代数式的分解公式中取特殊值而产生. 如:

(Ⅰ) 若 n 是正整数,则 $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1})$;

(Ⅱ) 若 n 是正奇数,则在上式中以 $(-b)$ 代换 b,得

$$a^n+b^n=(a+b)(a^{n-1}-a^{n-2}b+\cdots-ab^{n-2}+b^{n-1})$$

例 1 证明 $10\underbrace{\cdots}_{50个0}01$ 能被 1 001 整除.

证明 由分解公式(Ⅱ),有

$$10\underbrace{\cdots}_{50个0}01=10^{51}+1=(10^3)^{17}+1=(10^3+1)[(10^3)^{16}-(10^3)^{15}+\cdots-10^3+1]$$

所以,$10^3+1=1\ 001$ 整除 $10\underbrace{\cdots}_{50个0}01$. 证毕.

例 2 若 n 是奇数,证明:$8\mid(n^2-1)$.

证明 设 $n=2k+1(k\in\mathbf{Z})$,则 $n^2-1=(2k+1)^2-1=4k(k+1)$. 由于 k 和 $k+1$ 中必有一个是偶数,所以 $8\mid(n^2-1)$. 证毕.

注 由此得到一个重要且常用的结论:任何奇数的平方与 1 的差都能被 8 整除. 诸如此类的结论还有:任何整数的平方被 4 除的余数为 0 或 1,被 3 除的余数为 0 或 1;任何整数的立方被 9 除的余数为 0,1 或 8,等等. 解题后可及时总结归纳,并灵活运用这些性质.

例 3 设 $m>n\geqslant 0$,证明:$(2^{2^n}+1)\mid(2^{2^m}-1)$.

证明 由于 $m>n\geqslant 0$,故 $m-n-1\geqslant 0$. 在分解公式(Ⅰ)中,令 $a=2^{2^{n+1}}$,$b=1$,则

$$2^{2^m}-1=(2^{2^{n+1}})^{2^{m-n-1}}-1=(2^{2^{n+1}}-1)[(2^{2^{n+1}})^{2^{m-n-1}-1}+\cdots+2^{2^{n+1}}+1]$$

所以 $(2^{2^{n+1}}-1)\mid(2^{2^m}-1)$. 又 $2^{2^{n+1}}-1=(2^{2^n}+1)(2^{2^n}-1)$,因此 $(2^{2^n}+1)\mid(2^{2^{n+1}}-1)$.

由定理 1.1.1 之(ⅰ)知 $(2^{2^n}+1)\mid(2^{2^m}-1)$. 证毕.

注 1 在例 3 中,形如 $F_n=2^{2^n}+1(n\in\mathbf{N})$ 的数称为**费马数**. 当 $m>n\geqslant 0$ 时,费马数满足 $F_n\mid(F_n-2)$,即存在整数 t,使得 $F_m-2=t\cdot F_n$.

注 2 在例 3 中,直接证明 $(2^{2^n}+1)\mid(2^{2^m}-1)$ 不易入手,因此尝试选择适当的中间量 $(2^{2^{n+1}}-1)$,使之满足定理 1.1.1 之(ⅰ)的条件,再利用整除的传递性导出所证结论.

例 4 设正整数 n 的十进制表示为 $n=\overline{a_k\cdots a_1a_0}(0\leqslant a_i\leqslant 9,0\leqslant i\leqslant k,a_k\neq 0)$,且

$$S(n)=a_k+a_{k-1}+\cdots+a_1+a_0$$

证明:$9\mid n$ 的充分必要条件是 $9\mid S(n)$.

证明 由于

$$n=a_k\times 10^k+\cdots+a_1\times 10+a_0,\quad S(n)=a_k+a_{k-1}+\cdots+a_1+a_0$$

所以

$$n-S(n)=a_k(10^k-1)+\cdots+a_1(10-1)$$

对于所有的 $0\leqslant i\leqslant k$,有 $9\mid(10^i-1)$,故上式右端 k 个加项中的每一项都是 9 的倍数,由定理 1.1.1 之(ⅱ)知,它们的和也被 9 整除,即 $9\mid[n-S(n)]$,从而 $9\mid n\Leftrightarrow 9\mid S(n)$. 证毕.

注 一个十进制整数被另一个正整数整除的条件(如例 4 及习题 1.1 的第 2 题),称为**整**

除的数字特征. 例 4 得出十进制正整数 n 被 9 整除的数字特征是:9 整除 n 的各位数字之和.

习题 1.1

1. 设 n 是奇数,证明:$16\mid(n^4+4n^2+11)$.

2. 设正整数 n 的十进制表示为 $n=\overline{a_k\cdots a_1a_0}(0\leqslant a_i\leqslant 9,0\leqslant i\leqslant k,a_k\neq 0)$,$n$ 的个位为起始数字的正、负交错之和 $T(n)=a_0-a_1+\cdots+(-1)^ka_k$,证明:$11\mid n$ 的充分必要条件是 $11\mid T(n)$.

3. 10 个男孩和 n 个女孩共买了 n^2+8n+2 本书,已知他们每人买的书本数量相同,且女孩人数多于男孩人数,问女孩人数是多少?

4. 证明:一个整数 a 若不能被 6 整除,则 a^2+23 必能被 24 整除.

5. 已知整数 m,n,p,g 适合 $(m-p)\mid(mn+pq)$,证明:$(m-p)\mid(mq+np)$.

6. 若 a,b,c 为整数,且 $a^3+b^3+c^3$ 是 24 的倍数,求证:$(a^5+b^5+c^5)+4(a+b+c)$是 120 的倍数.

7. 设 $a_1,a_2,\cdots,a_n$是整数,且 $a_1+a_2+\cdots+a_n=0,a_1a_2\cdots a_n=n$,证明:$n$ 必是 4 的倍数.

8. 设 $M=5^{2\,003}+7^{2\,004}+9^{2\,005}+11^{2\,006}$,求证:$8\mid M$. 将此题进行推广并证明你的结论.

1.2　带余数除法

对任意两个整数 $a,b(b\neq 0)$,a 未必能被 b 整除. 为了能在整数范围内研究除法,引入整数的除法算法——带余数除法,它是初等数论证明中最重要、最基本且最常用的工具. 本节中将介绍带余数除法及其简单应用. 一般约定,以 **Z** 表示所有整数的集合,**N** 表示所有正整数的集合. 除特别声明外,当涉及带余数除法时总假定除数是正整数.

定理 1.2.1(带余数除法)　设 a 与 b 是两个整数,$b\neq 0$,则存在唯一的一对整数 q 和 r,使得

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

此外,$b\mid a$ 的充分必要条件是 $r=0$.

证明　**存在性**　若 $b\mid a$,则存在 $q\in\mathbf{Z}$,使得 $a=bq$,此时取 $r=0$,即式(1.1)成立.

若 $b\nmid a$,考虑集合 $A=\{a+kb\mid k\in\mathbf{Z}\}$. 在集合 A 中有无限多个正整数,由自然数的最小数原理知,A 中必有最小的正整数. 设这个最小的正整数为 $r=a+k_0b$,则必有结论:

$$0<r<|b|\tag{1.2}$$

事实上,若不然,就有 $r\geqslant|b|$. 因为 $b\nmid a$,所以 $r\neq|b|$,从而 $r>|b|$,故

$$r_1=r-|b|=a+k_0b-|b|>0$$

这样就有 $r_1\in A$ 且 $0<r_1<r$,这与 r 的最小性矛盾. 所以,式(1.2)成立. 取 $q=-k_0$,知式(1.1)成立. 存在性得证.

唯一性　假设存在两对整数 q',r'与 q'',r''都使得式(1.1)成立,即

$$a = q''b + r'' = q'b + r' \quad (0 \leqslant r', r'' < |b|)$$

于是

$$(q'' - q')b = r' - r'' \tag{1.3}$$

由此推出 $b|(r'-r'')$. 但 $0 \leqslant |r'-r''| < |b|$，故必须使 $r'-r''=0$，即 $r'=r''$，代入式(1.3)得 $q'=q''$. 唯一性得证.

当 $a=bq+r$ 时，$b|a \Leftrightarrow b|r$；而当 $0 \leqslant r < |b|$ 时，$b|r \Leftrightarrow r=0$. 故 $b|a \Leftrightarrow r=0$. 证毕.

注 自然数的最小数原理是：任何非空的自然数集合一定存在最小数. (证明略)

定义 式(1.1)中的 q 称为 a 被 b 除的**不完全商**，r 称为 a 被 b 除的**余数**，也称为**最小非负剩余**.

注 对于给定的正整数 b，可以按照被 b 除的余数将整数集分成 b 类，使得在同一类中的整数被 b 除的余数 r 相同. 这就使得关于全体整数的问题可以化归为对有限个整数类的研究. 此时，r 共有 b 种可能的取值，即 $0,1,\cdots,b-1$. 当 $r=0$ 时，即为“a 被 b 整除”的情形. 由此，整除问题往往可以化归为带余数除法问题来解决.

推论 1.2.1 设 a,b,d 是给定的整数，$b \neq 0$，则存在唯一的一对整数 q 和 r，满足 $a=bq+r$ $(d \leqslant r < |b|+d)$.

证明 考虑整数 $(a-d)$ 及 b，由带余数除法知，存在唯一的整数对 q 和 r_0，使得 $a-d=bq+r_0$ $(0 \leqslant r_0 < |b|)$，所以 $a=bq+r$，其中 $r=r_0+d$ $(d \leqslant r < |b|+d)$. 由 q 和 r_0 的唯一性得知 q 和 r 唯一存在. 证毕.

注 推论 1.2.1 也称为带余数除法，它是带余数除法的一种更为灵活的形式.

例如，当 $2|b$ 时，取 $d=-\frac{|b|}{2}$；当 $2 \nmid b$ 时，取 $d=-\frac{|b|-1}{2}$，则

$$a = bq + r, \quad \text{其中} \begin{cases} -\frac{|b|}{2} \leqslant r < \frac{|b|}{2}, & 2 \mid b \\ -\frac{|b|-1}{2} \leqslant r < \frac{|b|+1}{2}, & 2 \nmid b \end{cases}$$

这种带余数除法中的余数 r 叫做**绝对最小余数**. 有时使用这种余数可使计算相对简化.

例 1 设 $a_1,a_2,\cdots,a_n$ 为不全为零的整数，以 y_0 表示集合

$$A = \{y \mid y = a_1x_1 + \cdots + a_nx_n, x_i \in \mathbf{Z}, 1 \leqslant i \leqslant n\}$$

中的最小正数，则对于任何 $y \in A$，有 $y_0|y$；特别地，有 $y_0|a_i$ $(1 \leqslant i \leqslant n)$.

证明 设 $y_0=a_1x_1'+\cdots+a_nx_n' \in A$，对任意的 $y=a_1x_1+\cdots+a_nx_n \in A$，由定理 1.2.1 知，存在 $q,r \in \mathbf{Z}$，使得 $y=qy_0+r$ $(0 \leqslant r < y_0)$. 因此

$$r = y - qy_0 = a_1(x_1 - qx'_1) + \cdots + a_n(x_n - qx'_n) \in A$$

如果 $r \neq 0$，那么，因为 $0 < r < y_0$，所以 r 是 A 中比 y_0 还小的正整数，这与 y_0 的定义矛盾. 所以 $r=0$，即 $y_0|y$.

显然 $a_i \in A$ $(1 \leqslant i \leqslant n)$，所以由上述结论得 $y_0|a_i$ $(1 \leqslant i \leqslant n)$. 证毕.

注　此类题目的证明方法具有一般性，通常是针对所给“最小正数”的概念进行反证法.

例 2　证明：任意给出的五个整数中，必有三个数之和能被 3 整除.

证明　设这五个整数是 a_i，令 $a_i=3q_i+r_i(0\leqslant r_i<3,i=1,2,3,4,5)$.

分别考虑以下两种情形：

（ⅰ）若在 $r_1,r_2,\cdots,r_5$ 中数 0,1,2 都出现，不妨设 $r_1=0,r_2=1,r_3=2$，此时

$$a_1+a_2+a_3=3(q_1+q_2+q_3)+3$$

能被 3 整除；

（ⅱ）若在 $r_1,r_2,\cdots,r_5$ 中数 0,1,2 至少有一个不出现，则根据抽屉原理至少有三个 r_i 要取相同的值，不妨设 $r_1=r_2=r_3=r$（r 是 0,1,2 中的某一个），此时

$$a_1+a_2+a_3=3(q_1+q_2+q_3)+3r$$

能被 3 整除. 综合情形（ⅰ）和（ⅱ）可知，所证结论成立. 证毕.

注　例 2 涉及的抽屉原理也称为 P. G. Dirichlet 原理，即把 $n+1$ 个元素或者更多的元素放入 n 个抽屉中，则在其中一个抽屉里至少要放入 2 个元素. 一般，将 m 个元素放入 $n(m>n)$ 个抽屉中，则在其中一个抽屉里至少含有 $\left[\frac{m-1}{n}\right]+1$（中括号表示不超过 $\frac{(m-1)}{n}$ 的最大整数）个元素. 值得注意的是，利用带余数除法得到的余数进行分类来构造抽屉是数论解（证）题中常用的方法.

例 3　设 r 是正奇数，证明：对任意的正整数 n，有 $(n+2)\mid(1^r+2^r+\cdots+n^r)$.

证明　当 $n=1$ 时，结论显然成立. 现设 $n\geqslant 2$，令 $S=1^r+2^r+\cdots+n^r$，则

$$2S=2+(2^r+n^r)+[3^r+(n-1)^r]+\cdots+(n^r+2^r)\qquad(*)$$

因为 r 为奇数，由 1.1 节的分解公式(Ⅱ)可得上式右边中除第一项外，每一加项 $i^r+(n+2-i)^r$ 都能被 $i+(n+2-i)=n+2(2\leqslant i\leqslant n)$ 整除，因此 $2S=2+(n+2)Q_1$，其中 Q_1 是整数. 显然，$2S$ 被 $n+2$ 除得的余数是 2，由于 $n+2>2$，所以 $(n+2)\nmid 2S$，故 $(n+2)\nmid S$. 证毕.

注　在例 3 的证明过程中，关键在于找出表达式（$*$）中其和能被 $n+2$ 整除的两项，并将其配成一对. 这种“配对”思想方法，就是将整体对象中满足某种特性的对象组合配对，再利用配对后的特性解决原问题. 它是数论解（证）题中常用的一种方法，后续章节中也经常涉及配对思想方法.

例 4　设 m 和 n 为正整数，$m>2$，证明：$(2^m-1)\nmid(2^n+1)$.

证明　对正整数 m 和 n 分以下三种情形讨论：

（ⅰ）当 $n=m$ 时，$2^n+1=(2^n-1)+2$，由于 $n=m,m>2$，所以 $2^n-1>2$，因而

$$(2^n-1)\nmid(2^n+1)$$

（ⅱ）当 $n<m$ 时，有 $n\leqslant m-1$，注意到 $m>2$，有 $2^n+1\leqslant 2^{m-1}+1<2^m-1$，由定理 1.1.1 之（ⅳ）知 $(2^m-1)\nmid(2^n+1)$.

(ⅲ) 当 $n>m$ 时,设 $n=mq+r(0\leqslant r<m, q\in\mathbf{N})$,由于

$$2^n+1=(2^{mq}-1)\cdot 2^r+(2^r+1)$$

由 1.1 节的分解公式(Ⅰ)得 $(2^m-1)\mid(2^{mq}-1)$.

当 $r=0$ 时,

$$2^n+1=(2^{mq}-1)+2=(2^m-1)\cdot M+2\quad(M\in\mathbf{Z})$$

由于 $m>2$,故 $2^m-1>2$,因此 $(2^m-1)\nmid 2$,从而 $(2^m-1)\nmid(2^n+1)$.

当 $0<r<m$ 时,由(ⅱ)知 $(2^m-1)\nmid(2^r+1)$.

综上可知,对一切正整数 m 和 $n(m>2)$,有 $(2^m-1)\nmid(2^n+1)$. 证毕.

注 例 4 对正整数 m 和 n 的各种可能情况进行了分类讨论,分类的思想方法是数论解(证)题中的常用方法.

例 5 证明:若 a 被 9 除的余数是 3,4,5 或 6,则方程 $x^3+y^3=a$ 没有整数解.

证明 对任意整数 x,y,记 $x=3q_1+r_1, y=3q_2+r_2$,其中 $0\leqslant r_1, r_2<3, q_1, q_2\in\mathbf{Z}$. 于是有 $x^3=9Q_1+r_1^3, y^3=9Q_2+r_2^3$,其中 $Q_1, Q_2\in\mathbf{Z}$. 所以 $x^3+y^3=9(Q_1+Q_2)+r_1^3+r_2^3$.

显然,x^3+y^3 被 9 除的余数与 $r_1^3+r_2^3$ 被 9 除的余数相同. 由于 r_1^3, r_2^3 被 9 除的余数为 0,1 或 8,因此,$r_1^3+r_2^3$ 被 9 除的余数只可能是 0,1,2,7 或 8;而已知 a 被 9 除的余数是 3,4,5 或 6,所以,x^3+y^3 不可能等于 a,即方程 $x^3+y^3=a$ 没有整数解. 证毕.

注 若一个整系数方程有整数解,则用任何非零数同时除此方程两边所得的最小非负余数都相同. 基于这个性质可知,若一个方程两边用同一个非零整数去除所得的余数不相同,则此方程必无整数解. 例 5 正是运用了此种基本思想.

习题 1.2

1. 设 $3\mid(a^2+b^2)$,证明:$3\mid a$ 且 $3\mid b$,其中 a,b 是任意整数.

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

3. 设 $a>0$,证明:相邻的 a 个整数有且仅有一个被 a 整除.

4. 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.

5. 证明:对于任意给定的 n 个整数,必可以从中找出若干个数作和,使得该和能被 n 整除.

6. 设整数 $k\geqslant 1$,证明:

(1) 若 $2^k\leqslant n<2^{k+1}, 1\leqslant a\leqslant n, a\neq 2^k$,则 $2^k\nmid a$;

(2) 若 $3^k\leqslant 2n-1<3^{k+1}, 1\leqslant b\leqslant n, 2b-1\neq 3^k$,则 $3^k\nmid(2b-1)$.

1.3 最大公因数

最大公因数是数论中的一个重要概念. 本节讨论最大公因数的概念及其基本性质.

任意整数 $a_1, a_2, \cdots, a_n$ 必然有公因数(例如 ± 1),如果这些整数不全为零,则易见它们的公

因数只有有限多个，所以它们的最大公因数存在并且唯一. 此外，如果 d 是它们的公因数，则 $(-d)$ 也是它们的公因数，从而最大公因数一定是正整数.

定义　整数 $a_1,a_2,\cdots,a_n$ 的公共因数称为 $a_1,a_2,\cdots,a_n$ 的**公因数**. 不全为零的整数 $a_1,a_2,\cdots,a_n$ 的公因数中最大的一个，称为 $a_1,a_2,\cdots,a_n$ 的**最大公因数**(或**最大公约数**)，记为 $(a_1,a_2,\cdots,a_n)$.

如果 $(a_1,a_2,\cdots,a_n)=1$，则称 $a_1,a_2,\cdots,a_n$ 是**互素的**(或**互质的**)；换言之，如果 $a_1,a_2,\cdots,a_n$ 是互素的，则它们的公因数只有 ±1.

如果 $(a_i,a_j)=1(1\leqslant i,j\leqslant n,i\neq j)$，则称 $a_1,a_2,\cdots,a_n$ 是**两两互素的**(或**两两互质的**). 显然，由 $a_1,a_2,\cdots,a_n$ 两两互素可以推出 $(a_1,a_2,\cdots,a_n)=1$；反之，则不然.

例如 $(2,6,15)=1$，而 $(2,6)=2$. 但是，对于两个整数而言，互素与两两互素的概念却是一致的.

最大公因数有如下的基本性质.

定理 1.3.1　(ⅰ) $(a_1,a_2,\cdots,a_n)=(|a_1|,|a_2|,\cdots,|a_n|)$.

(ⅱ) $(a,b)=(b,a)$.

(ⅲ) 若 $a\neq0$，则 $(a,0)=|a|,(a,a)=|a|$.

(ⅳ) 若 $a=bq+r$，则 $(a,b)=(b,r)$ $(q,r\in\mathbf{Z})$.

证明　(ⅰ)设 d 是 $a_i(1\leqslant i\leqslant n)$ 的公因数，由 $d\mid a_i(1\leqslant i\leqslant n)$ 可推出必有 $d\mid|a_i|(1\leqslant i\leqslant n)$，即 d 是 $|a_i|(1\leqslant i\leqslant n)$ 的公因数；反之亦然. 由此可知，$|a_i|(1\leqslant i\leqslant n)$ 与 $a_i(1\leqslant i\leqslant n)$ 的全体公因数集合相同. 故

$$(a_1,a_2,\cdots,a_n)=(|a_1|,|a_2|,\cdots,|a_n|)$$

(ⅱ)和(ⅲ)均可由最大公因数定义直接得出.

(ⅳ) 令 $d=(a,b),d'=(r,b)$，由于 $d\mid a,d\mid b$，则 $d\mid(a-bq)=r$，即 d 是 b 与 r 的公因数，故 $d\leqslant d'$；同理，得 $d'\leqslant d$. 因此 $d=d'$，即 $(a,b)=(b,r)$. 证毕.

注　定理 1.3.1 之(ⅰ)说明，在讨论 $(a_1,a_2,\cdots,a_n)$ 时，不必考虑 $a_i(1\leqslant i\leqslant n)$ 的正负符号. 因此，在求 $a_1,a_2,\cdots,a_n$ 的最大公因数时，可将它们视为非负整数来讨论；定理 1.3.1 之(ⅳ)的证法也是证明两个最大公因数相等的常用方法，同时，性质(ⅳ)还是辗转相除法(见 1.5 节)求最大公因数的理论基础.

定理 1.3.2　设 $a_1,a_2,\cdots,a_n\in\mathbf{Z}$，记 $A=\left\{y\mid y=\sum_{i=1}^{n}a_ix_i,x_i\in\mathbf{Z},1\leqslant i\leqslant n\right\}$. 如果 y_0 是集合 A 中最小的正数，则 $y_0=(a_1,a_2,\cdots,a_n)$.

证明　由于 y_0 是集合 A 中最小的正数，故 $y_0=\sum_{i=1}^{n}a_ix_i^0(x_i^0\in\mathbf{Z},1\leqslant i\leqslant n)$. 设 d 是 $a_1,a_2,\cdots,a_n$ 的任意一个公因数，则 $d\mid y_0=\sum_{i=1}^{n}a_ix_i^0$，所以 $d\leqslant y_0$.

又由 1.2 节例 1 的结论知 $y_0 | a_i (1 \leqslant i \leqslant n)$，故 y_0 也是 $a_1, a_2, \cdots, a_n$ 的公因数. 因此，y_0 是 $a_1, a_2, \cdots, a_n$ 所有公因数中的最大正数，由此即得 $y_0 = (a_1, a_2, \cdots, a_n)$. 证毕.

注 由于 $(a_1, a_2, \cdots, a_n)$ 是集合 $A = \left\{ y \mid y = \sum_{i=1}^{n} a_i x_i, x_i \in \mathbf{Z}, 1 \leqslant i \leqslant n \right\}$ 的最小正数，由定理 1.3.2 的证明过程直接得到如下推论.

推论 1.3.1 设不全为零整数 $a_1, a_2, \cdots, a_n$ 的最大公因数是 $(a_1, a_2, \cdots, a_n)$，则存在整数 $x_1', x_2', \cdots, x_n'$，使得 $a_1 x_1' + a_2 x_2' + \cdots + a_n x_n' = (a_1, a_2, \cdots, a_n)$.

推论 1.3.2 设 d 是 $a_1, a_2, \cdots, a_n$ 的任意一个公因数，则 $d | (a_1, a_2, \cdots, a_n)$.

证明 由推论 1.3.1 知，存在整数 $x_1', \cdots, x_n'$ 使得

$$a_1 x_1' + \cdots + a_n x_n' = (a_1, \cdots, a_n)$$

所以由 $d | a_i (1 \leqslant i \leqslant n)$，有 $d | (a_1 x_1' + \cdots + a_n x_n')$，即 $d | (a_1, a_2, \cdots, a_n)$. 证毕.

注 推论 1.3.2 对最大公因数的本质属性做了非常深刻的刻画：最大公因数不但是公因数中最大的，而且是 $a_1, a_2, \cdots, a_n$ 所有公因数的倍数. 此结论在问题证明过程中常起到桥梁的关键作用.

定理 1.3.3 $(a_1, a_2, \cdots, a_n) = 1$ 的充分必要条件是存在整数 $x_1, x_2, \cdots, x_n$，使得

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 1 \tag{1.4}$$

证明 **必要性** 由推论 1.3.1 即可得到式(1.4).

充分性 若式(1.4)成立，令 $(a_1, a_2, \cdots, a_n) = d$，由 $d | a_i (1 \leqslant i \leqslant n)$ 推出：

$$d \mid (a_1 x_1 + a_2 x_2 + \cdots + a_n x_n) = 1$$

故 $d = 1$，即 $(a_1, a_2, \cdots, a_n) = 1$. 证毕.

定理 1.3.4 设 a, b 是不全为零的整数，则：

(ⅰ) $(ma, mb) = m(a, b)$，其中 $m > 0$；

(ⅱ) 若 $\delta = (a, b)$，则 $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = 1$，即 $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$；

(ⅲ) $(a^n, b^n) = (a, b)^n$，其中 $n \in \mathbf{Z}$.

证明 留作习题.

由定理 1.3.4 的(ⅰ)和(ⅱ)易推广得到如下结论：

(ⅳ) $(ma_1, ma_2, \cdots, ma_n) = |m| (a_1, a_2, \cdots, a_n)$，其中 $m \neq 0$；

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

注 定理 1.3.4 之(ⅱ)给出了一个证明数论问题的常用方法：由两个不全为零且不互素的整数，可自然地产生一对互素的整数. 利用这一结论，数论中不全为零且不互素的整数可以化归为互素的整数，从而达到简化问题证明过程的目的. 由(ⅲ)还可推知 $(a, b) = 1 \Leftrightarrow (a^n, b^n) = 1$.

最大公因数还有以下重要性质.

定理 1.3.5 对于整数 a, b, c，下面的结论成立：

（ⅰ）由 $b|ac$ 及 $(a,b)=1$ 可以推出 $b|c$；

（ⅱ）由 $b|c,a|c$ 及 $(a,b)=1$ 可以推出 $ab|c$.

证明　（ⅰ）若 $(a,b)=1$，由定理 1.3.3 知，存在整数 x 与 y，使得 $ax+by=1$. 因此，

$$acx+bcy=c \tag{1.5}$$

由式(1.5)及 $b|ac$ 得到 $b|c$. 结论（ⅰ）得证.

（ⅱ）因为 $(a,b)=1$，由定理 1.3.3 知，存在整数 x,y 使得式(1.5)成立. 又由 $b|c$ 与 $a|c$，得 $ab|ac,ab|bc$，再由式(1.5)得 $ab|c$. 故结论（ⅱ）得证. 证毕.

推论 1.3.3　若 $(a,b)=1$，则 $(a,bc)=(a,c)$.

证明　由于 $(a,b)=1$，由定理 1.3.3 知，存在整数 x,y 使得式(1.5)成立.

设 $d=(a,bc)$，$d'=(a,c)$，则 $d|a,d|bc$，由式(1.5)得 $d|c$，即 d 是 a 与 c 的公因数，故 $d\leqslant d'$；又 d' 是 a 与 c 的公因数，则它也是 a 与 bc 的公因数. 因此 $d'\leqslant d$，故 $(a,bc)=(a,c)$. 证毕.

注　推论 1.3.3 在求已知两个大数的最大公因数时会经常被用到.

推论 1.3.4　若 $(a_i,b_j)=1(1\leqslant i\leqslant n,1\leqslant j\leqslant m)$，则 $(a_1a_2\cdots a_n,b_1b_2\cdots b_m)=1$.

特别地，若 $(a,b)=1$，则对任意正整数 m 和 n 有 $(a^n,b^m)=1$.

证明　由于 $(a_i,b_j)=1(1\leqslant i\leqslant n,1\leqslant j\leqslant m)$，由推论 1.3.1 得

$$(a_i,b_1b_2\cdots b_m)=(a_i,b_2\cdots b_m)=\cdots=(a_i,b_m)=1 \quad (1\leqslant i\leqslant n)$$

故
$$(a_1a_2\cdots a_n,b_1b_2\cdots b_m)=(a_2\cdots a_n,b_1b_2\cdots b_m)=\cdots=(a_n,b_1b_2\cdots b_m)=1$$

证毕.

定理 1.3.6　对于任意 n 个不全为零的整数 $a_1,a_2,\cdots,a_n$，记

$$(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{n-2},a_{n-1})=d_{n-1},(d_{n-1},a_n)=d_n$$

则
$$d_n=(a_1,a_2,\cdots,a_n)$$

证明　由已知条件及整除的传递性，有

$d_n=(d_{n-1},a_n)\Rightarrow d_n\mid a_n,d_n\mid d_{n-1}$

$d_{n-1}=(d_{n-2},a_{n-1})\Rightarrow d_{n-1}\mid a_{n-1},d_{n-1}\mid d_{n-2}$，　故 $d_n\mid a_n,d_n\mid a_{n-1},d_n\mid d_{n-2}$

$d_{n-2}=(d_{n-3},a_{n-2})\Rightarrow d_{n-2}\mid a_{n-2},d_{n-2}\mid d_{n-3}$，　故 $d_n\mid a_n,d_n\mid a_{n-1},d_n\mid a_{n-2},d_n\mid d_{n-3}$

$\cdots$

$d_2=(a_1,a_2)\Rightarrow d_n\mid a_n,d_n\mid a_{n-1},\cdots,d_n\mid a_2,d_n\mid a_1$

即 d_n 是 $a_1,a_2,\cdots,a_n$ 的一个公因数.

又对于 $a_1,a_2,\cdots,a_n$ 的任何公因数 d，由推论 1.3.2 及 $d_2,\cdots,d_n$ 的定义，依次得出

$$d\mid a_1,d\mid a_2\Rightarrow d\mid d_2$$
$$d\mid d_2,d\mid a_3\Rightarrow d\mid d_3$$
$$\cdots$$
$$d\mid d_{n-1},d\mid a_n\Rightarrow d\mid d_n$$

故 d_n 是 $a_1,a_2,\cdots,a_n$ 公因数中的最大者. 因此，$d_n=(a_1,a_2,\cdots,a_n)$. 证毕.

注 定理 1.3.6 指出了求 $n(n>2)$ 个不全为零整数最大公因数的方法，其实质是先化归为 $n-1$ 个整数的最大公因数问题，最终化归为两个整数的最大公因数问题来解决.

定理 1.3.7 设 a,b,c,n 是正整数，$ab=c^n$，$(a,b)=1$，则存在正整数 u,v，使得

$$a=u^n,\quad b=v^n,\quad c=uv,\quad (u,v)=1$$

证明 因为 $(a,b)=1$，所以 $(b,a^{n-1})=1$，故 $a=a(b,a^{n-1})=(ab,a^n)=(c^n,a^n)=(c,a)^n$；同理得 $b=(c,b)^n$. 令 $u=(a,c)$，$v=(b,c)$，则 $a=u^n$，$b=v^n$，$c=uv$，且

$$(u,v)=((a,c),(b,c))=(a,b,c)=((a,b),c)=(1,c)=1$$

故定理结论成立. 证毕.

注 定理 1.3.7 说明，如果互素的两个正整数之积是一个整数的 n 次幂，则这两个正整数都是整数的 n 次幂. 此结论还可推广为：如果正整数 $a,b,\cdots,c$ 之积是一个整数的 n 次幂，若 $a,b,\cdots,c$ 两两互素，则 $a,b,\cdots,c$ 都是整数的 n 次幂. 这个性质表现了整数互素的重要性，其应用较广泛.

例 1 设 n 是正整数，证明：$(n!+1,(n+1)!+1)=1$.

证明 设 $d=(n!+1,(n+1)!+1)$，由于 $(n!+1)(n+1)-[(n+1)!+1]=n$，于是有 $d\mid n$. 进一步有 $d\mid n!$，结合 $d\mid(n!+1)$ 可知 $d\mid 1$，故 $d=1$. 证毕.

例 2 证明：任意两个费马数 $(F_m,F_n)=1(m\neq n)$.

证明 不妨设 $m>n$. 由 1.1 节例 3 知，当 $m>n\geqslant 0$ 时，费马数满足 $F_n\mid(F_m-2)$，即存在整数 t，使得 $F_m=2+tF_n$. 设 $d=(F_m,F_n)$，则 $d=(2+tF_n,F_n)=(2,F_n)=2$，故 $d=1$ 或 $d=2$. 但 F_n 显然是奇数，故必有 $d=1$，即费马数是两两互素的. 证毕.

例 3 设 $m,n>0$，$mn\mid(m^2+n^2)$，证明：$m=n$.

证明 设 $(m,n)=d$，则 $m=m_1d$，$n=n_1d$，其中 $(m_1,n_1)=1$. 于是，已知条件化为 $m_1n_1\mid(m_1^2+n_1^2)$，由此得 $m_1\mid(m_1^2+n_1^2)$，故 $m_1\mid n_1^2$. 但是 $(m_1,n_1)=1$，结合 $m_1\mid n_1^2$，可知必须 $m_1=1$. 同理 $n_1=1$. 因此 $m=n$. 证毕.

注 由例 3 知，对于给定的两个不全为零的整数，常借助于它们的最大公因数来产生两个互素的整数，以便能利用互素的性质作进一步讨论，这实质上是将原问题化归为互素的特殊情形.

例 4 设 k 为正整数，证明：$1+2+\cdots+n$ 整除 $1^k+2^k+\cdots+n^k$.

证明 因为 $1+2+\cdots+n=\dfrac{n(n+1)}{2}$，且 $(n,n+1)=1$，所以结论等价于证明

$$n\mid 2(1^k+2^k+\cdots+n^k),\quad (n+1)\mid 2(1^k+2^k+\cdots+n^k)$$

事实上，由于 k 是奇数，利用配对法可得

$$2(1^k+2^k+\cdots+n^k)=[1^k+(n-1)^k]+[2^k+(n-2)^k]+\cdots+[(n-1)^k+1^k]+2n^k$$

上式的每个加项显然都是 n 的倍数，故其和也是 n 的倍数. 同理得

$$2(1^k+2^k+\cdots+n^k)=(1^k+n^k)+[2^k+(n-1)^k]+\cdots+(n^k+1^k)$$

上式是 $n+1$ 的倍数，故 $n(n+1)\mid 2(1^k+2^k+\cdots+n^k)$. 证毕.

习题 1.3

1. 证明定理 1.3.4.

2. 设 n 为正整数，证明：$(12n+5,9n+4)=1$.

3. 设 $x,y\in\mathbf{Z}$，$17\mid 2x+3y$，证明：$17\mid(9x+5y)$.

4. 设 $(a,b)=1$，证明：$(a^2+b^2,ab)=1$.

5. 设 a,b 是整数，若 $9\mid(a^2+ab+b^2)$，证明：$3\mid(a,b)$.

6. 设 m,n 都是正整数，m 为奇数，证明：$(2^m-1,2^n+1)=1$.

7. 若一个有理数的 $k(k\geqslant 1)$ 次幂是整数，则这个有理数必是整数. 一般的，证明：一个首项系数为 ± 1 的整系数多项式的有理根必定是一个整数.

1.4　最小公倍数

本节讨论整数的最小公倍数的概念及其性质.

定义　非零整数 $a_1,a_2,\cdots,a_n$ 的公共倍数称为 $a_1,a_2,\cdots,a_n$ 的**公倍数**. $a_1,a_2,\cdots,a_n$ 的正公倍数中最小的一个叫做 $a_1,a_2,\cdots,a_n$ 的**最小公倍数**，记为 $[a_1,a_2,\cdots,a_n]$.

定理 1.4.1　非零整数的最小公倍数的性质是：

(ⅰ) $[a,1]=|a|$，$[a,a]=|a|$，其中 $a\neq 0$.

(ⅱ) $[a,b]=[b,a]$.

(ⅲ) $[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]$.

(ⅳ) 若 $a\mid b$，则 $[a,b]=|b|$.

证明　留作习题.

注　由定理 1.4.1 之 (ⅲ) 可知，在求非零整数 $a_1,a_2,\cdots,a_n$ 的最小公倍数时，可视 $a_1,a_2,\cdots,a_n$ 都是正整数，从而简化问题的证明过程.

最小公倍数和最大公因数之间存在一个很重要的关系，即定理 1.4.2 的结论.

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 和 b 的一个公倍数，则存在整数 k_1,k_2，使得 $m=ak_1$，$m=bk_2$，因此

$$ak_1=bk_2 \tag{1.6}$$

于是

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

由于 $\left(\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right)=1$，所以 $\dfrac{b}{(a,b)}\mid k_1$，即

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

其中 t 是某个整数. 将上式代入式(1.6)得到