21世纪精品规划教材系列

初等数论

CHU DENG SHU LUN

主编◎韩灵娟 阮佶

吉林大学出版社

21世纪精品规划教材系列

初等数论

主　编　韩灵娟　阮　佶
参　编　巩军胜　郭胜红

吉林大学出版社

图书在版编目(CIP)数据

初等数论 / 韩灵娟，阮佶主编. —— 长春 ：吉林大学出版社，2016.1

ISBN 978-7-5677-5621-2

Ⅰ. ①初… Ⅱ. ①韩… ②阮… Ⅲ. ①初等数论 Ⅳ. ①O156.1

中国版本图书馆 CIP 数据核字(2016)第 016255 号

书　　名：初等数论

作　　者：韩灵娟　阮　佶　主编

责任编辑：李伟华　责任校对：甄志忠　　封面设计：可可工作室

吉林大学出版社出版、发行　　北京楠海印刷厂印刷

开本：787×1092 毫米　1/16　　2016 年 1 月 第 1 版

印张：13.5　字数：260 千字　　2016 年 1 月 第 1 次印刷

ISBN 978-7-5677-5621-2　　定价：29.00 元

社址：长春市明德路 501 号　邮编：130021

发行部电话：0431-89580028/29

网址：http://www.jlup.com.cn

E-mail:jlup@mail.jlu.edu.cn

前　言

初等数论是以整除理论为基础，研究整数性质和方程(组)整数解的一门数学学科，是一门古老的数学分支。它展示着近代数学中最典型、最基本的概念、思想、方法和技巧。同时，它对于一些看似简单却困惑了人类智者许多年的著名难题，如梅森数问题、完全数问题、伪素数问题等的研究，推动着数学的发展。目前，初等数论在计算机科学、代数编码、密码学、组合数学、计算方法等领域内得到了广泛的应用，成为计算机科学等相关专业不可缺少的数学基础。

本书介绍了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、连分数、数论函数以及初等数论的应用等内容。在附录部分简要地介绍了数论各分支的形成和发展的历史，以及在实际问题中的简单应用。这些内容可作为高等院校数学专业和计算机相关专业学生的教材，也可作为高中数学教师的教学参考书。

本书的目的是介绍初等数论的基础知识。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、重点突出、结构严谨、例题典型。每章开始通过引述部分达到各章之间的自然过渡，并对重点内容给出必要的评注；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。本书第一章，第二章和第八章由韩灵娟执笔，第三章，第四章和前言由巩军胜执笔，第五章，第六章，第七章由阮佶执笔，附录由郭胜红执笔，最后由韩灵娟和阮佶统纂定稿。

本教材在编写过程中参考了较多国内现有相关文献资料，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

2015 年 9 月

目 录

第一章 整 除

整除理论是数论中最重要的基本内容.本章首先简要介绍自然数与数学归纳法,然后引进整除的概念,利用带余除法和辗转相除法这两个工具,建立最大公约数与最小公倍数的理论,进一步研究素数的基本性质和极具重要性的算术基本定理,最后探讨了$[x]$,$\{x\}$这两个很有用的记号,并利用$[x]$来说明如何把$n!$表示成素数幂的乘积.这一切都是整个课程中最基本的部分,以后时常要用到.

§1 自然数与整数

自然数,也叫正整数,就是大家所熟悉的

$$1,2,3,\cdots,n,n+1,\cdots$$

自然数集:所有自然数组成的集合称为自然数集,用N表示,即

$$\mathrm{N}=\{1,2,3,\cdots\}$$

整数就是指正整数、负整数及零,即

$$\cdots,-n-1,-n,\cdots,-3,-2,-1,0,1,2,3,\cdots,n,n+1,\cdots.$$

整数集:全体整数组成的集合称为整数集,用Z表示,即

$$\mathrm{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$$

我们熟知的整数基本知识是:

(Ⅰ)整数可以比较大小,用$\leqslant$、$<$、$\geqslant$、$>$、$=$表示.

整数具有下列性质:

(1)自反性:$a\leqslant a,a\in Z$.

(2)反对称性:对任意的$a,b\in Z$,若$a\leqslant b$且$a\geqslant b$,则$a=b$.

(3)传递性:对任意的$a,b,c\in Z$,若$a\leqslant b$且$b\leqslant c$,则$a\leqslant c$,等号仅当$a=b$且$b=c$时成立.

(Ⅱ)在整数集合中可以作加法运算“+”及其逆运算减法运算“-”.加法运算满足以下性质:

(1)结合律 $(a+b)+c=a+(b+c),a,b,c\in \mathrm{Z}$.

(2)交换律 $a+b=b+a,a,b\in \mathrm{Z}$.

(3)消去律 若 $a+b=b+c$,则 $b=c,a,b,c\in \mathrm{Z}$.

(4)$a+0=a,a\in \mathrm{Z}$.

(5)对任意的 $a,b\in \mathrm{Z}$,必有 $c\in \mathrm{Z}$,使得 $a=b+c$.

(Ⅲ)在整数集合中可以进行乘法运算,但不一定能做其逆运算——除法运算.整数的乘法运算具有如下性质:

(1)若 $a,b\in Z$,则 $a\cdot b\in Z$,$a\div b$ 不一定是整数$(b\neq 0)$.

(2)结合律:$(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

(3)交换律:$a\cdot b=b\cdot a$.

(4)消去律:若 $a\neq 0$,且 $a\cdot b=a\cdot c$,则 $b=c$.

(5)分配律:$(a+b)\cdot c=ac+bc,c\cdot(a+b)=c\cdot a+c\cdot b$.

(Ⅳ)在整数集合中还引入了绝对值的概念,即:

$$|a|=\begin{cases}a,a\in \mathrm{N},\\0,a=0,\\-a,-a\in \mathrm{N}.\end{cases}$$

绝对值具有如下性质:

(1)$|ab|=|a|\cdot|b|,a,b\in Z$.

(2)$|a+b|\leqslant|a|+|b|,a,b\in Z$.

自然数源于经验,自然数的本质属性是由归纳原理(或称归纳公理)刻画的,定理的核心用通常的语言可表述如下:

归纳原理 设 S 是 N 的一个子集,满足条件:(ⅰ)$1\in S$,(ⅱ)如果 $n\in S$,则 $n+1\in S$,那么,$S=\mathrm{N}$.

这原理是我们常用的数学归纳法的基础,两者实际上是一回事.

定理 1 (第一数学归纳法)设 $p(n)$ 是关于自然数数 n 的命题,若

(ⅰ)当 $n=1$ 时,命题 $p(1)$ 成立;

(ⅱ)在 $p(k)$(k 为任意自然数)成立的假设下可以推出 $p(k+1)$ 成立,则 $p(n)$ 对一切自然数 n 都成立.

证 设使 $p(n)$ 成立的所有自然数 n 组成的集合是 S. S 是 N 子集.由条件(ⅰ)知 $1\in S$;

由条件(ⅱ)知,若 $k \in S$,则 $k+1 \in S$. 所以由归纳原理知 $S = \mathrm{N}$. 证毕.

由归纳原理还可推出在数学中,特别是初等数论中常用的自然数的重要性质.

定理 2 (最小自然数原理) 自然数集的任何非空子集都必含有最小数.

证 设 T 是自然数集 N 的一个非空子集,则对任意的 $t \in T$,必有 $s \leqslant t$. 令 $S = \{s \mid s \leqslant t, t \in T\}$,显然 $1 \in S$,S 非空. 此外,若 $t_1 \in T$,则 $t_1 + 1 > t_1$,所以 $t_1 + 1 \notin S$. 由以上及归纳原理可得,必存在 $s_0 \in S$,使得 $s_0 + 1 \notin S$. 故 s_0 是 T 中最小的自然数. 证毕.

注 最小自然数原理是我们常用的第二种数学归纳法的基础.

定理 3 (第二种数学归纳法) 设 $P(n)$ 是关于自然数 n 的一种性质或命题. 如果

(ⅰ) 当 $n = 1$ 时,$P(1)$ 成立;

(ⅱ) 设 $n > 1$. 若对所有的自然数 $m < n$,$P(n)$ 成立,则必可推出 $P(n)$ 成立,那么,$P(n)$ 对所有自然数 n 成立.

证 用反证法. 若定理不成立,设 T 是使 $P(n)$ 不成立的所有自然数组成的集合,T 非空. 由定理 2 知集合 T 必有最小自然数 m. 故对一切 $k < m$,命题 $P(k)$ 是成立的. 由(ⅰ)知 $P(m)$ 正确,这就与假设产生了矛盾. 证毕.

在初等数论中还经常用到的一个工具是:

定理 4 (鸽巢原理) 设 n 是一个自然数. 现有 n 个盒子和 $n+1$ 个物体. 无论怎样把这 $n+1$ 个物体放入这 n 个盒子中,一定有一个盒子中被放了两个或两个以上的物体.

证 用反证法. 假设结论不成立,即每个盒子中至多有一个物体,那么,这 n 个盒子中总共有的物体个数 $\leqslant n$. 这和有 $n+1$ 个物体放到了这 n 个盒子中相矛盾. 证毕.

习题 1.1

1. 试证:任何 $\geqslant 8$ 的正整数均能表示为若干个 3 与 5 的和.

2. 试证:对于任何正整数 $n \geqslant 3$,总存在奇数 x, y,使得 $2^n = 7x^2 + y^2$.

3. 有两堆棋子,数目相等,有两人玩耍,每人可以在任意一堆里任意取几颗,但不能同时在两堆里取,规定取得最后一颗者胜. 试证:后取者必胜.

4. 设 k_0 是给定的正整数,$P(n)$ 是关于正整数 n 的一种性质或命题. 如果

(ⅰ) 当 $n = k_0$ 时,$P(k_0)$ 成立;

(ⅱ) 由 $P(n)$ 成立可推出 $P(n+1)$ 成立,

那么,$P(n)$ 对所有正整数 $n \geqslant k_0$ 成立.

5. 设 T 是一个由整数组成的集合. 若 T 中有正整数，则 T 中必有最小正整数.

§2 数的整除性

我们知道，两个整数的和、差、积仍然是整数，但是用一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，从而有必要引入整除的概念.

定义 设 a,b 是两个整数，$b\neq 0$，如果存在整数 q，使得 $a=bq$，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 q，使得 $a=bq$ 成立，则称 a 不被 b 整除或 b 不整除 a，记为 $b\nmid a$.

例 1 $11\nmid 189,-6\mid 42,25\mid 0,5\nmid 56,-7\nmid 68$.

例 2 6 的所有约数是 $\pm 1,\pm 2,\pm 3$ 和 ± 6；11 的所有约数是 ± 1 和 ± 11.

由定义及乘法运算的性质，立即可推出整除关系有下面性质(注意：符号 $a\mid b$ 本身包含了条件 $a\neq 0$).

定理 设 a,b,c 是整数，下面的结论成立：

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

(ⅱ) 若 $a\mid b$，且 $a\mid c$，则对任意整数 $k,1$，有 $a\mid(k\cdot b+1\cdot c)$.

一般地，若 $a\mid b_i,i=1,2,\cdots,n$，则 $a\mid(b_1x_1+b_2x_2+\cdots+b_nx_n)$，其中 $x_i(i=1,2,\cdots,n)$ 是任意整数.

(ⅲ) 若 $a\mid b$，且 $m\neq 0$，则 $am\mid bm$；反之亦然.

(ⅳ) 若 $a\mid b$，则 $-a\mid b,a\mid(-b),\mid a\mid\mid b\mid$；

(ⅴ) 若 $a\mid b$，且 $b\mid a$，则 $b=\pm a$；

证 (ⅰ) 由整除定义及 $a\mid b,b\mid c$ 知，存在两个整数 q_1,q_2，使得 $b=aq_1,c=bq_2$，因此 $c=a(q_1q_2)$，由于 q_1q_2 是整数，故 $a\mid c$.

(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 3 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 $a\mid n$ 且 $b\mid n$，则 $ab\mid n$.

证 由 $n=n(ax+by)=(na)x+(nb)y$，及 $a\mid n,b\mid n$，从而 $ab\mid na,ab\mid nb$ 即得所要结论. 证毕.

例 4 证明：若 $3\mid n$ 且 $7\mid n$，则 $21\mid n$.

证 因为 $7\times1+3\times(-2)=1$，而 $3\mid n,7\mid n$，由例 3 结论可得 $(3\cdot7)\mid n$，即：$21\mid n$. 证毕.

例 5 证明 $\underbrace{10\cdots1}_{50个0}$ 能被 1001 整除.

证 由分解公式(Ⅱ)，有

$$\underbrace{10\cdots1}_{50个0}=10^{51}+1=(10^3)^{17}+1=(10^3+1)[(10^3)^{16}-(10^3)^{15}+\cdots-10^{3+1}],$$

所以，$10^3+1=1001$ 整除 $\underbrace{10\cdots1}_{50个0}$. 证毕.

例 6 若 n 是奇数，证明：$8\mid(n^2-1$.

证 设 $n=2k+1,k\in Z$ 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 7 设 $m>n\geqslant0$，证明：$(2^{2^n}+1)\mid(2^{2^m}-1)$.

证 由于 $m>n\geqslant0$，故 $m-n-1\geqslant0$. 在分解公式(Ⅰ)中，令 $a=2^{2^{n+1}},b=1$，则 $2^{2^m}-1=(2^{2^{n+1}})^{2^{m-n-1}}-1=(2^{2^{n+1}}-1)[(2^{2^{n+1}})^{2^{m-n-1}}+\cdots+2^{2^{n+1}}+1]$.

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 $(2^{2^n}+1)\mid(2^{2^{n+1}}-1)$.

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

注 在例 7 中，形如 $F_n=2^{2^n}+1(n\in N)$ 的数称为费马数. 当 $m>n\geqslant0$ 时，费马数满足 $F_n\mid(F_m-2)$，即存在整数 t，使得 $F_m-2=t\cdot F_n$.

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 $2^{2^{n+1}}-1$，使之满足定理之(ⅰ)的条件，再利用整除的传递性导出所证结论.

例 8 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 由于 $n=a_k\cdot 10^k+\cdots+a_1\cdot 10+a_0$，$S(n)=a_k+a_{k-1}+\cdots+a_1+a_0$，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，由定理之(ⅱ)知，它们的和也被 9 整除，即 $9\mid[n-S(n)]$，从而 $9\mid n$，$9\mid S(n)$. 证毕.

注 一个十进制整数被另一个正整数整除的条件，称为整除的数字特征. 例 8 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 1.2

1. 设 $a=2t-1$. 若 $a\mid 2n$，则 $a\mid n$.

2. 若 $2\mid n$，$3\mid n$，$5\mid n$，则 $30\mid n$.

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. 设 n 是奇数，证明：$16\mid(n^4+4n^2+11)$.

5. 证明：一个整数 a 既不能被 2 也不能被 3 整除，则 a^2+23 必能被 24 整除.

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

7. 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.

8. 设 $n\neq 1$. 证明：$(n-1)^2\mid n^k-1$ 的充要条件是 $(n-1)\mid k$.

§3 带余数除法

为了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.

定理(带余数除法) 设 a,b 是两个给定的整数，$a\neq 0$. 那么，一定存在惟一的一对整数 q 与 r，满足

$$a = bq + r, 0 \leqslant r < |a| \tag{1}$$

此外，$a \mid b$ 的充要条件是 $r = 0$.

证 **存在性** 若 $a \mid b$，则存在 $q \in Z$，使得 $b = aq$，此时取 $r = 0$，即式(1)成立.

若 $a \nmid b$，考虑集合 $A = \{b - ka \mid k = 0, \pm 1, \pm 2, \cdots\}$. 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 $r = b - k_0 a$，则必有结论：

$$0 < r < |a| \tag{2}$$

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

$$r_1 = -|b| = a + k_0 b - |b| > 0.$$

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(2)成立. 取 $q = -k_0$，知式(2)成立. 存在性得证.

惟一性 若还有整数 q_1 与 r_1 满足(1)，则

$$a = bq_1 + r_1, 0 \leqslant r_1 < b.$$

因此

$$bq_1 + r_1 = bq + r,$$

于是

$$b(q - q_1) = r_1 - r \tag{3}$$

由于 $0 \leqslant |r - r_1| < |b|$，故必须使 $|r - r_1| = 0$，即 $r = r_1$，代入(3)得 $q = q_1$. 证毕.

定义 式(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，也称为最小非负余数.

注 对于给定的 $a \geqslant 0$，可以按照被 a 除的余数将整数集分成 a 类，使得在同一类中的整数被 a 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 $0, 1, \cdots, a - 1$. 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.

带余数除法在具体的应用中，常有以下更灵活的形式：

推论 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 $b = aq + r (d \leqslant r < |b| + d)$.

证 考虑整数 $(b - d)$ 及 a，由带余数除法知，存在唯一的整数对 q 和 r_0，使得 $b - d = aq + r_0 (0 \leqslant r_0 < |a|)$，所以 $b = aq + r$，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.

例 1 两个数相除，商为 8，余数为 16，被除数，除数，商与余数之和为 463，求被除

数.

解 设被除数为 a,除数为 b.

$\because a = 8b + 16$,

$a + b + 8 + 16 = 463$,

$\therefore a + b = 463 - 24 = 439$,

$$\therefore \begin{cases} a = 8b + 16 \\ a = 439 - b \end{cases}$$

解此方程组得:

$a = 392, b = 47$.

$\therefore$ 被除数为 392.

例 2 有一个自然数,用它去除 59,95,129 得到三个余数之和为 25,求这个自然数.

解 设这个自然数为 x,用 x 去除 59,95,129 得到的商和余数分别为 q_1, q_2, q_3 和 r_1, r_2, r_3,

则

$$59 = xq_1 + r_1, 0 < r_1 < x,$$

$$95 = xq_2 + r_2, 0 < r_2 < x,$$

$$129 = xq_3 + r_3, 0 < r_3 < x,$$

$\therefore 59 + 95 + 129 = (q_1 + q_2 + q_3) + (r_1 + r_2 + r_3)$,

$283 = x(q_1 + q_2 + q_3) + (r_1 + r_2 + r_3)$,

而三个余数之和为 25,

$\therefore 283 = x(q_1 + q_2 + q_3) + 25$,

$x(q_1 + q_2 + q_3) = 258$,

$258 = 1 \cdot 258 = 2 \cdot 129 = 3 \cdot 86 = 6 \cdot 43$,

又 $\because r_1 < x, r_2 < x, r_3 < x$,

$\therefore r_1 + r_2 + r_3 < 3x$,

$25 < 3x, x > \frac{25}{3}$,

$\therefore x$ 只可能是 258,129,86,43 中的一个.

当 $x = 258$ 时,

$258 \div 258$ 余数是 $0 < \frac{25}{3}$,

$63 \div 258$ 余数是 $63 > 25$,

$91 \div 258$ 余数是 $91 > 25$,

$129 \div 258$ 余数是 $129 > 25$,

$\therefore x \neq 258$,

同理,$x \neq 129$,$x \neq 86$,

$\therefore x = 43$.

例 3 请在 503 后面添 3 个数字,使所得的 6 位数被 7,9,11 整除.

解 要使所得的 6 位数被 7,9,11 整除,则这个 6 位数必须被 $693(=7 \cdot 9 \cdot 11)$ 整除. 做除法 $504000 \div 693$,得 $504000 = 693 \times 727 + 18$,因此

$$504000 - 189 = 503811(= 693 \times 727),$$

$$503811 - 693 = 503118(= 693 \times 726),$$

它们都能被 693 整除.

于是,所添数字是 8,1,1 或 1,1,8.

例 4 设 $n, d(d \neq 0)$ 是整数,如果 $f(n)$ 是关于 n 的整系数多项式,且 n 除以 d 所得的余数为 r,则 $d \mid f(n), d \mid f(r)$

证 设 $n = dq + r$. 因为 $f(n)$ 是关于 n 的整系数多项式,所以存在整数 A,使得

$$f(n) = f(dq + r) = dA + f(r),$$

所以 $d \mid f(n), d \mid f(r)$. 证毕.

例 5 设 t 是正奇数,证明:对任意的正整数 t,有 $(n+2) \nmid (1^t + 2^t + \cdots + n^t)$.

证 当 $n = 1$ 时,结论显然成立. 现设 $n \geqslant 2$,令 $s = 1^t + 2^t + \cdots + n^t$,则

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

因为 t 为奇数,由 §2 节的分解公式(Ⅱ)可得上式右边中除第一项外,每一加项 $i^t + (n+2-i)^t$ 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 5 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.

习题 1.3

1. 请在 763 后面添加 3 个数字,使所得的 6 位数能被 5,7,9 整除.

2. 设对所有的正整数 n，有 $10 \mid (3^{m+4n}+1)$，求正整数 m.

3. 证明：任意给出的五个整数中，必有三个数之和能被 3 整除.

4. 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.

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

6. 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.

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

8. 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 最大公约数与辗转相除法

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，性质及其求法.

定义 1 设 a_1,a_2 是两个整数. 如果 $d \mid a_1$ 且 $d \mid a_2$，那么，d 就称为是 a_1 和 a_2 的公约数. 一般地，设 $a_1,a_2,\cdots,a_n$ 是 n 个整数. 如果 $d \mid a_1,\cdots,d \mid a_n$，那么，$d$ 就称为是 $a_1,a_2,\cdots,a_n$ 的公约数.

例如：$a_1=4,a_2=12$. 它们的公约数是 $\pm 1,\pm 2,\pm 4$.

$a_1=6,a_2=7,a_3=-15$. 它们的公约数是 ± 1.

注 由于任意一个非零整数的约数的个数都是有限的，所以最大公约数是唯一存在的，并且是正整数.

定义 2 设 a_1,a_2 是两个不全为零的整数. 我们把 a_1 和 a_2 的公约数中的最大的称为 a_1 和 a_2 的最大公约数，记作 (a_1,a_2). 一般地，设 $a_1,a_2,\cdots,a_n$ 是 n 个不全为零的整数. 我们把 $a_1,a_2,\cdots,a_n$ 的公约数中的最大的称为 $a_1,a_2,\cdots,a_n$ 的最大公约数，记作 $(a_1,a_2,\cdots,a_n)$.

定义 3 如果整数 a_1,a_2 的最大公约数 $(a_1,a_2)=1$，则称 a,b 是互素的（或互质的）. 一般地，若 $(a_1,a_2,\cdots,a_n)=1$，则称 $a_1,a_2,\cdots,a_n$ 是既约的，或是互素的. 若 $a_1,a_2,\cdots,a_n$ 中每两个整数互质，我们就说它们两两互质.

显然，若整数 $a_1,a_2,\cdots,a_n$ 两两互质，则 $(a_1,a_2,\cdots,a_n)=1$，反过来却不一定成立，如 $(6,10,-15)=1$，但 $(-15,10)=5,(6,-15)=3$. 且若 $a_1,a_2,\cdots,a_n$ 不全为零，则 $(a_1,a_2,\cdots,a_n)$ 是存在的.

下面的定理对判定一组数是否互素是有用的.

定理 1 设 $a_1,a_2,\cdots,a_n$ 是不全为零的整数. 我们有

(ⅰ)$(a_1,a_2,\cdots,a_n)=\min\{y \mid y=a_1x_1+a_2x_2+\cdots+a_nx_n, x_j\in Z, 1\leqslant j\leqslant n, y>0\}$,即$a_1,a_2,\cdots,a_n$的最大公约数等于$a_1,a_2,\cdots,a_n$的所有整系数线性组合组成的集合中的最小正整数.

(ⅱ)一定存在一组整数$x_{1,0},\cdots,x_{n,0}$,使得

$$(a_1,a_2,\cdots,a_n)=a_1x_{1,0}+a_2x_{2,0}+\cdots+a_nx_{n,0}.$$

证 令$A=\{y \mid y=a_1x_1+a_2x_2+\cdots+a_nx_n, x_j\in Z, 1\leqslant j\leqslant n, y>0\}$,

由于$0<a_1^2+\cdots+a_n^2\in A$,所以集合$A$中有正整数,由最小数原理知$A$中必有最小正整数,设$y_0$是集合$A$中最小的正整数,即证$y_0=(a_1,a_2,\cdots,a_n)$.

由于y_0是集合A中最小的正整数,故

$y_0=a_1x_{1,0}+a_2x_{2,0}+\cdots+a_nx_{n,0}(x_{i,0}\in Z, 1\leqslant i\leqslant n)$,

设d是$a_1,a_2,\cdots,a_n$的任意一个公因数,则$d\mid y_0$,所以$\mid d\mid\mid y_0$.另一方面,对任一a_j由带余数除法知$a_j=q_jy_0+r_j, 0\leqslant r_j<y_0$.显见$r_j\in A$.若$r_j>0$,则和$y_0$的最小性矛盾,所以,$r_j=0$,即$y_0\mid a_j$,$(1\leqslant j\leqslant n)$.

所以,y_0是$(a_1,a_2,\cdots,a_n)$的最大公约数.即$(a_1,a_2,\cdots,a_n)=a_1x_{1,0}+a_2x_{2,0}+\cdots+a_nx_{n,0}$.证毕.

定理2 整数$a_1,a_2,\cdots,a_n$互素的充要条件是存在整数$t_1,t_2,\cdots,t_n$,使得

$$a_1t_1+a_2t_2+\cdots+a_nt_n=1.$$

证 **充分性** 令d是$a_1,a_2,\cdots,a_n$的任一公约数,则$d\mid 1$,必有$d=1$,即$(a_1,a_2,\cdots,a_n)=1$.

必要性 有定理1可知必要性成立.证毕.

最大公约数有以下基本性质:

定理3 若$a_1,a_2,\cdots,a_n$是任意n个不全为零的整数,则$(a_1,a_2,\cdots,a_n)$与$(\mid a_1\mid,\mid a_2\mid,\cdots,\mid a_n\mid)$的公因数相同,且$(a_1,a_2,\cdots,a_n)=(\mid a_1\mid,\mid a_2\mid,\cdots,\mid a_n\mid)$.

证 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$d\mid\mid a_i\mid(1\leqslant i\leqslant n)$,即$d$是$\mid a_i\mid(1\leqslant i\leqslant n)$的公因数;反之亦然.由此可知,$\mid a_i\mid(1\leqslant i\leqslant n)$与$a_i(1\leqslant i\leqslant n)$的全体公因数集合相同.故$(a_1,a_2,\cdots,a_n)=(\mid a_1\mid,\mid a_2\mid,\cdots,\mid a_n\mid)$.证毕.

定理4 若b是任一非零正数,则

(ⅰ)0与b的公因数就是b因数,反之亦然.

(ⅱ)$(0,b)=\mid b\mid$.

证 由最大公因数定义可直接得出结论.

定理5 设a,b,c是任意三个不全为0的整数,且$a=bq+c$,其中q是非零整数,