初等数论

张廷海　黄福生　主编

科学出版社

初等数论

张廷海　黄福生　主编

科学出版社

北京

内 容 简 介

本书是作者结合多年初等数论的教学实践，根据高校初等数论课程的教学大纲，并充分考虑专业理论知识与学生未来就业的实际需要相结合的需求编写而成的. 其主要内容包括整除理论、不定方程、同余、数的表示、一元同余方程、平方剩余与二次同余方程、原根与指标. 书中例题和习题大部分选自中小学各类数学竞赛试题，且每节节后几乎都附有数学家小故事.

本书可作为综合性大学、师范院校数学系、计算机系及其相关专业的教材，也可作为教师进修学院的教师、学生及报考公务员考生的参考书.

图书在版编目(CIP)数据

初等数论/张廷海，黄福生主编. —北京：科学出版社，2017.12

ISBN 978-7-03-055886-2

Ⅰ.①初… Ⅱ. ①张… ②黄… Ⅲ.①初等数论 Ⅳ.①O156.1

中国版本图书馆 CIP 数据核字(2017) 第 305532 号

责任编辑：胡海霞 / 责任校对：张凤琴

责任印制：吴兆东 / 封面设计：迷底书装

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

北京中石油彩色印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2017 年 12 月第 一 版 开本：720 × 1000 1/16

2017 年 12 月第一次印刷 印张:14 1/2

字数：292 000

定价：45.00 元

(如有印装质量问题，我社负责调换)

前　言

初等数论是研究整数性质和方程 (组) 整数解的一门学科, 也是一个古老的数学分支. 作为大学数学专业的基础课程, 它不仅在师范院校普遍开设, 也是综合性大学数学专业及计算机科学等许多相关专业所需的课程. 近几十年来, 随着数论理论和方法在计算机科学、代数编码和信息安全等许多领域的广泛应用, 数论已日益成为除数学工作者之外的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, 因而, 许多高等学校在更多专业开设数论课程, 以满足人才培养的需要.

本书是作者结合多年初等数论的教学实践, 根据高校初等数论课程的教学大纲, 并充分考虑专业理论知识与学生未来就业的实际需要而编写的. 其主要内容包括整除理论、不定方程、同余、数的表示、一元同余方程、平方剩余与二次同余方程、原根与指标. 本书区别于以往的初等数论教材具有以下显著特点.

(1) 实用性. 初等数论的许多概念在中小学数学教材中都介绍过, 因此, 一直以来, 在中小学的各类数学竞赛中, 有关初等数论的知识占有很大的比重. 本书根据这一现状, 在介绍数论理论和方法的同时, 选取了历年数学竞赛中的相关原题作为例题和习题, 以利于准备成为中小学数学教师的师范生更好地适应将来的工作. 此外, 近年来, 报考公务员是大学生就业的主流选择之一, 而公务员招考科目之一的《行政职业能力测验》中的 "数量关系" 部分就有大量的有关初等数论的知识, 因此, 本书中也选取了历年各级公务员考试中的原题, 以帮助有志于报考公务员的学生更好地熟悉公务员招考的内容.

(2) 教育性. 初等数论是数学的一个源远流长的分支, 古今中外, 该学科涌现了一大批数学家, 而且也是我国数学家做出享有世界声誉贡献的领域之一. 因此, 本书在讲解数论理论的同时, 也介绍了相关数学家的生平事迹. 这既可以让学生更全面地了解该学科的发展历史, 尤其了解我国数学家所做的贡献, 以激发学生的爱国热情, 同时也增加课程的趣味性.

(3) 习题多样性. 初等数论的问题看起来似乎很简单, 但真正学好它并不容易, 尤其是习题很不好做. 以往的许多数论教材中的例题和习题几乎都是侧重于理论性的证明题, 这就使得学生更觉得初等数论课程枯燥. 本书精心编写了包括选择题、填空题在内的多种不同难易程度的题型, 不仅每小节后附有习题, 而且每一章结束后又有总复习题, 这可以让学生通过习题的练习更好地理解和掌握数论理论、方法与技巧, 弥补了以往教材题量少而难的不足.

本书选材精炼、重点突出、例题丰富, 每章均配有大量习题, 且书后附有习题解答, 可作为综合性大学师范院校数学系、计算机系及其相关专业师生, 教师进修学院师生及广大报考公务员考生的用书. 其中, 较难部分章节加 “*” 号, 读者可根据自身需要选用这些内容.

本书的出版得到了江西师范大学数学与信息科学学院的领导和老师们的帮助, 在此表示诚挚的感谢. 由于作者水平有限, 其中不当之处在所难免, 望广大读者批评指正.

张廷海

2017 年 1 月

目　录

第1章 整除理论

数论是研究整数性质的一个数学分支, 其中整数的整除理论是初等数论的基础, 其他内容都与之有着直接或间接的联系. 它是对在小学就学过的整数的算术运算作抽象的、系统的总结, 看起来似乎简单, 但是它的内涵却十分深刻. 它也是中小学数学竞赛和公务员考试中所考查的有关初等数论知识的主要部分. 本章主要内容包括整除的概念和基本性质、带余除法、最大公因数与最小公倍数、辗转相除法、素数与合数、算术基本定理、数的奇偶性与平方数以及高斯函数 $[x]$ 及其应用, 其中最大公因数和算术基本定理是整除理论的核心内容, 带余除法和辗转相除法是整除理论的重要工具.

1.1 整除的概念和基本性质

我们知道, 两个整数的和、差、积仍然是整数, 但是用不为零的整数去除另一个整数所得的商却不一定是整数, 为此, 我们引入整数的整除的概念, 并由此给出其性质及应用.

定义 1.1.1 设 $a,b\in\mathbb{Z}$($\mathbb{Z}$ 表示整数集合), 且 $b\neq 0$, 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 $b\,|a$, 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 **不能被** b **整除**或 b **不整除** a, 记为 $b\nmid a$.

显然每个非零整数 a 至少有因数 ± 1, $\pm a$, 称它们为 a 的**平凡因数**; a 的其他因数, 称为 a 的**非平凡因数**.

由整除的定义和乘法运算性质立即可以推出整除的以下性质.

定理 1.1.1 设 $a,b,c\in\mathbb{Z}$, 则下面的结论成立.

(i) 若 $b\,|a$, 则 $\pm b|\pm a$;

(ii) 若 $c|b$, 且 $b\,|a$, 则 $c\,|a$ (整除的传递性);

(iii) 若 $c\,|a$, 且 $c\,|b$, 则对任意整数 m,n, 有 $c|(ma+nb)$, 一般地, 若 $b\,|a_i$ $(i=1,2,\cdots,n)$, 则对任意整数 $m_i(i=1,2,\cdots,n)$, 有 $b\,|(a_1m_1+a_2m_2+\cdots+a_nm_n)$ (整除的线性性);

(iv) 若 $b\,|a$, 且 $c\neq 0$, 则 $bc\,|ac$, 反之也成立;

(v) 若 $b\,|a$, 且 $a\neq 0$, 则 $|b|\leqslant|a|$, 若 $b\,|a$, 且 $|b|>|a|$, 则 $a=0$, 若 $b|a$, 且 $a|b$, 则 $a=\pm b$.

请读者自证.

注意　由整除的定义可知, 为了证明 $b|a$, 设法将 a 分解为 b 与另一个因数的乘积是其中的基本方法之一, 因此一些常见的代数式的分解公式对证明整数的整除具有一定的帮助. 如

(Ⅰ) 设 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) 设 n 是正奇数, 则在上式中以 $-b$ 代换 b 得

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

(Ⅲ) 设 n 是正偶数, 则

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

例 1　证明: $\underbrace{9\cdots9}_{59个9}$ 能被 1001 整除.

证明　由分解公式 (Ⅲ), 有

$$\underbrace{9\cdots9}_{59个9}=1\underbrace{0\cdots0}_{60个0}-1=10^{60}-1=(10^3)^{20}-1=(10^3+1)[(10^3)^{19}-(10^3)^{18}+\cdots+10^3-1],$$

所以, $1001=10^3+1$ 整除 $\underbrace{9\cdots9}_{59个9}$.

例 2　证明: 若 $5|n$, 且 $7|n$, 则 $35|n$.

证明　由 $5|n$, 有 $n=5k, k\in\mathbb{Z}$, 由 $7|n$ 可知 $7|5k$. 又由 $7|7k$, 可知 $7|(3\cdot5k-2\cdot7k)$, 即 $7|k$, 因此有 $k=7t, t\in\mathbb{Z}$. 所以 $n=35t, t\in\mathbb{Z}$, 即 $35|n$.

例 3　设 p,q 都是正奇数, 且 $p-1=q+1$, 证明: $(p+q)|(p^p+q^q)$.

证明　由分解公式 (Ⅰ), 有

$$p^p-1=(p-1)(p^{p-1}+p^{p-2}+\cdots+p+1);$$

由分解公式 (Ⅱ), 有

$$q^q+1=(q+1)(q^{q-1}-q^{q-2}+\cdots-q+1).$$

再由有限个奇数的乘积仍是奇数, 奇数个奇数的和、差也是奇数, 因此 $p^{p-1}+p^{p-2}+\cdots+p+1$ 和 $q^{q-1}-q^{q-2}+\cdots-q+1$ 都是奇数, 于是 $p^p-1=(p-1)(2s+1)$, $s\in\mathbb{Z}$; $q^q+1=(q+1)(2t+1)$, $t\in\mathbb{Z}$. 上述两式相加并结合 $p-1=q+1$ 得

$$p^p+q^q=2(p-1)(s+t+1)=(p+q)(s+t+1),$$

所以 $(p+q)\,|(p^p+q^q)$.

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

(i) $3|m \Leftrightarrow 3\left|\sum_{i=0}^{n} a_i\right.$;

(ii) $7|m \Leftrightarrow 7|(\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\overline{a_8a_7a_6}-\cdots)$;

(iii) $11|m \Leftrightarrow 11\left|\sum_{i=0}^{n}(-1)^i a_i\right.$;

(iv) $13|m \Leftrightarrow 13|(\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\overline{a_8a_7a_6}-\cdots)$.

证明 (i) 由 $m=a_n\times 10^n+\cdots+a_1\times 10+a_0$ 及 $\sum_{i=0}^{n} a_i=a_n+a_{n-1}+\cdots+a_1+a_0$, 有

$$m-\sum_{i=0}^{n} a_i=a_n(10^n-1)+\cdots+a_1(10-1),$$

对于所有的 $0\leqslant i\leqslant n$, 有 $3|(10^i-1)$, 从而由整除的线性性可知 3 整除上式右端, 因此 $3\left|\left(m-\sum_{i=0}^{n} a_i\right)\right.$, 由此进一步得到 $3\,|m \Leftrightarrow 3\left|\sum_{i=0}^{n} a_i\right.$.

(ii) 由 $m=\overline{a_2a_1a_0}+\overline{a_5a_4a_3}\times 1000+\overline{a_8a_7a_6}\times 1000^2+\cdots$, 有

$$m-(\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\overline{a_8a_7a_6}-\cdots)=\overline{a_5a_4a_3}\times(1000+1)+\overline{a_8a_7a_6}\times(1000^2-1)+\cdots,$$

再由分解公式 (Ⅱ), (Ⅲ) 可知 $(1000+1)\,|(1000^i+1)$, i 为正奇数; $(1000+1)\,|(1000^j-1)$, j 为正偶数, 于是由整除的线性性有

$$1001\,|(m-(\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\overline{a_8a_7a_6}-\cdots)),$$

再由 $7\,|1001$ 及整除的传递性有

$$7\,|(m-(\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\overline{a_8a_7a_6}-\cdots)),$$

由此进一步推出:

$$7|m \Leftrightarrow 7|(\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\overline{a_8a_7a_6}-\cdots).$$

(iii), (iv) 可分别类似于 (i) , (ii) 证得.

注意　一个十进制整数被另一个正整数整除的条件 (如本节例 4), 称为 "**整除的数字特征**". 此类问题在数学竞赛和公务员考试中经常出现, 现将常见的整除数字特征归纳如表 1.1.1.

表 1.1.1

	除数	整除判定基本法则
被 2, 4, 8 整除	2	如果一个数的是偶数, 则这个数能被 2 整除
	4	如果一个数的末两位能被 4 整除, 则这个数能被 4 整除
	8	如果一个数的末三位能被 8 整除, 则这个数能被 8 整除
被 3, 9 整除	3	如果一个数的数字和能被 3 整除, 则这个数能被 3 整除
	9	如果一个数的数字和能被 9 整除, 则这个数能被 9 整除
被 5, 25, 125 整除	5	如果一个数的个位数字是 0 或 5, 则这个数能被 5 整除
	25	如果一个数的末两位能被 25 整除, 则这个数能被 25 整除
	125	如果一个数的末三位能被 125 整除, 则这个数能被 125 整除
被 11 整除	11	如果一个数奇数位上的数字和与偶数位上的数字和的差能被 11 整除, 则这个数能被 11 整除
被 7, 13 整除	7	如果一个数的末三位与前面部分数字之差能被 7 整除, 则这个数能被 7 整除, 如 223−13=210 能被 7 整除, 所以 13223 能被 7 整除
	13	如果一个数的末三位与前面部分数字之差能被 13 整除, 则这个数能被 13 整除, 如 287−14=273 能被 13 整除, 所以 14287 能被 13 整除

华罗庚小传

华罗庚 (1910~1985), 出生于江苏省金坛县. 数学家, 中国科学院院士, 美国国家科学院外籍院士. 他是中国解析数论、矩阵几何学、典型群、自守函数论与多元复变函数论等多方面研究的创始人和开拓者, 他为中国数学的发展做出了无与伦比的贡献, 被誉为 "中国现代数学之父". 美国著名数学家贝特曼著文称: "华罗庚是中国的爱因斯坦, 足够成为全世界所有著名科学院的院士."

华罗庚少年时期因家境贫困, 初中毕业后无法继续上学, 弃学回家帮助其父经营小店, 他只能利用业余时间自修数学. 这时华罗庚已对数学产生了强烈的兴趣, 而不能全力从事小店工作, 他的父亲对此很反感, 多次要撕掉他的 "天书". 他 18 岁时不幸染上伤寒, 卧床半年, 从此左腿落下残疾. 但是, 华罗庚不悲观, 不气馁, 顽强发奋, 刻苦自学, 20 岁时, 就在《科学》上发表了关于代数方程式解法的文章, 受到当时清华大学数学系主任熊庆来的重视, 被邀请到清华大学工作. 在清华大学, 华罗庚勤奋好学, 只用了一年时间, 就把大学数学系的全部课程学完了, 同时开始了

对数论的研究, 卓有成就.

华罗庚一生热爱祖国. 新中国诞生时, 他正在美国伊利诺伊大学任教, 是终身教授. 出于对祖国的热爱和对民族强烈的责任感, 他致信留美同学: "为了抉择真理, 我们应当回去; 为了国家民族, 我们应当回去; 为了为人民服务, 我们也应当回去 …… 为我们伟大祖国的建设和发展而奋斗!"1950 年, 华罗庚毅然回到祖国, 以极大的热情参与国家的建设和科学事业的复兴. 他领导中国科学院数学研究所, 推动中国近代数学的研究和发展, 培养了许多数学人才, 使中国多个数学领域的研究领先于国际水平. 在长期的科学研究中, 尽管有时身处逆境, 他总是精神振奋, 全然不顾自己身残, 以赤子之心, 忘我工作, "沧海不捐一滴水, 洪炉陶冶砂成金, 四化作尖兵""横刀哪顾头颅白, 跃马紧傍青壮人, 不负党员名", 他诗如其人, 一生都以极大的热情报效国家.

1985 年 6 月 12 日, 他在访问日本期间因突发心脏病不幸逝世. 为了纪念他, 1986 年中国数学学会等单位开展了以 "华罗庚" 名字命名的全国性少年数学竞赛活动, 其中最具影响力的是 "华罗庚金杯" 少年数学邀请赛, 至今已举办了 20 余届, 以弘扬他热爱祖国和献身科学的精神.

习 题 1.1

1. 设 $n \in \mathbb{Z}$, 证明: $6 \mid n(n-1)(2n-1)$.

2. 证明: 若整系数方程 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ 有整数根 $b(\neq 0)$, 则必有 $b \mid a_0$. 并由此判断以下方程有无整数根, 若有整数根, 则求出所有整数根.

(1) $x^2 + x + 2 = 0$; (2) $x^3 - x^2 - 4x + 4 = 0$.

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

4. (第 3 届 "华罗庚金杯" 复赛) $\overline{173A}$ 是一个四位数. 数学老师说:"先后用 3 个数字代替 A, 所得到的 3 个四位数, 依次可以被 9,11,6 整除." 问: 这 3 个数字的和是多少?

5. (第 5 届 "华罗庚金杯" 初赛) 李明 1995 年的年龄是他出生那年的年份的数字之和. 问: 李明 1995 年多少岁?

6. 一个三位数能被 3 整除, 去掉它的末位数后, 所得的两位数是 17 的倍数, 这样的三位数中, 最大的是几?

7. (1992 年小学数学奥林匹克竞赛) 一个整数乘 13 后, 积的最后三位数是 123, 那么这样的整数中最小的是几?

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

9. 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. 证明: 若 $d \mid (b-c)$, 则 $d \mid (f(b) - f(c))$.

10. 证明: $S = 5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$ 能被 19 整除.

1.2　带余除法

1.1 节我们讨论了两个整数之间的整除的性质, 事实上对任意两个整数 $a, b(b \neq 0)$, a 未必能被 b 整除. 为此本节将介绍整数的除法算法——带余除法, 它是初等数论的证明中最重要、最基本、最常用的工具.

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

$$a = bq + r, \quad 0 \leqslant r < |b|, \tag{1.2.1}$$

特别地, $b \mid a$ 当且仅当 $r = 0$.

证明　作整数序列 $\cdots, -3|b|, -2|b|, -|b|, 0, |b|, 2|b|, 3|b|, \cdots$, 则 a 必位于上述序列中的某相邻两项之间, 即存在一个整数 q, 使得 $q|b| \leqslant a < (q+1)|b|$ 成立. 从而有 $0 \leqslant a - q|b| < |b|$, 令 $a - q|b| = r$. 因此, 当 $b > 0$ 时, 有 $a = qb + r$; 当 $b < 0$ 时, 有 $a = (-q)b + r$. 总之, q, r 是存在的.

下面证明 q, r 也是唯一的.

设 q_1, r_1 也满足式 (1.2.1), 即 $a = q_1 b + r_1$, $0 \leqslant r_1 < |b|$, 则有

$$a = qb + r = q_1 b + r_1, \quad 0 \leqslant r, r_1 < |b|. \tag{1.2.2}$$

于是 $b(q - q_1) = r_1 - r$, 由此得到 $b \mid (r_1 - r)$, 但 $0 \leqslant |r_1 - r| < |b|$, 故必有 $r_1 - r = 0$, 即 $r = r_1$.

代入式 (1.2.2) 得 $q = q_1$, 唯一性得证.

定义 1.2.1　称式 (1.2.1) 中的 q 是 a 被 b 除的**不完全商**, r 是 a 被 b 除的**余数**, 也称为**最小非负余数**.

此外, 带余除法还有以下更灵活的形式.

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, r, 使得

$$a = bq + r, \quad d \leqslant r < |b| + d. \tag{1.2.3}$$

证明　对整数 $a - d$ 和 b, 由定理 1.2.1 可知, 存在唯一的一对整数 q, r', 使得

$$a - d = bq + r', \quad 0 \leqslant r' < |b|,$$

从而 $a = bq + r' + d$, 令 $r = r' + d$, 于是 $a = bq + r$, 且 $d \leqslant r < |b| + d$.

由 q, r' 的唯一性可知 q, r 也是唯一的.

注意　由推论 1.2.1 可得到另外两种常见的余数:

(1) 当 $2 \mid b$ 时, 取 $d = -\dfrac{|b|}{2}$; 当 $2 \nmid b$ 时, 取 $d = -\dfrac{|b| - 1}{2}$, 则此时式 (1.2.3) 成为

$a=bq+r$, 其中

$$\begin{cases} -\dfrac{|b|}{2} \leqslant r < \dfrac{|b|}{2}, & 2|b, \\ -\dfrac{|b|-1}{2} \leqslant r < \dfrac{|b|+1}{2}, & 2\nmid b, \end{cases}$$

并称余数 r 为**绝对最小余数**.

(2) 取 $d=1$, 此时式 (1.2.3) 成为

$$a=bq+r, \quad 1 \leqslant r \leqslant |b|,$$

此时称余数 r 为**最小正余数**.

推论 1.2.2 设 b 是正整数, 则任一整数被 b 除后所得的最小非负余数是且仅是 $0, 1, \cdots, b-1$ 这 b 个数中的一个.

注意 这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. 它是常用的整数分类及进位制表示法的基础.

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

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

中的最小正整数, 则对任意 $y \in A$, 有 $y_0 \,|\, y$; 特别地, 有 $y_0 \,|\, a_i$, $1 \leqslant i \leqslant n$.

证明 设 $y_0=a_1x_1'+\cdots+a_nx_n' \in A$, 则对任意的 $y=a_1x_1+\cdots+a_nx_n \in A$, 由定理 1.2.1, 存在 $q, r \in \mathbb{Z}$, 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 $0<r<y_0$, 从而 r 是 A 中比 y_0 还要小的正整数, 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 $y_0 \,|\, a_i$, $1 \leqslant i \leqslant n$.

例 2 设 $b \geqslant 2$ 是给定的正整数, 则任一正整数 n 必可唯一地表示为

$$n=r_kb^k+r_{k-1}b^{k-1}+\cdots+r_1b+r_0, \tag{1.2.4}$$

其中整数 $k \geqslant 0$, $0 \leqslant r_i \leqslant b-1 (i=0,1,\cdots,k)$, 且 $r_k \neq 0$, 这就是正整数的 b**进制表示**.

证明 由 $b \geqslant 2$, 对任一正整数 n, 必有唯一的整数 $k \geqslant 0$, 使 $b^k \leqslant n < b^{k+1}$. 又由带余除法知, 必有唯一的一对整数 q_0, r_0 , 满足 $n=q_0b+r_0, 0 \leqslant r_0 < b$.

现对上述整数 k 进行归纳.

若 $k=0$, 即 $1 \leqslant n < b$, 则必有 $q_0=0$, $1 \leqslant r_0 < b$, 此时 $n=r_0$ 结论成立.

假设结论对 $k=m \geqslant 0$ 成立. 那么, 当 $k=m+1$ 时, 上式中的 q_0 必满足

$$b^m \leqslant q_0 < b^{m+1}.$$

从而由假设知 $q_0 = s_m b^m + \cdots + s_0$, 其中 $0 \leqslant s_i \leqslant b-1 (i = 0, 1, \cdots, m)$, $s_m \neq 0$, 于是有

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

即结论对 $k = m+1$ 成立, 由归纳假设原理知, 式 (1.2.4) 成立.

例 3 (北京市第 7 届 "迎春杯" 小学数学竞赛)　有一个自然数, 用它分别去除 63,90,130 都有余数, 三个余数的和为 25, 则这三个余数中最小的是几?

解　设该自然数为 m, 且它除 63,90,130 的商分别为 q_1, q_2, q_3, 余数分别为 r_1, r_2, r_3, 即有

$$63 = mq_1 + r_1, \quad 90 = mq_2 + r_2, \quad 130 = mq_3 + r_3,$$

由 $r_1 + r_2 + r_3 = 25$ 知, 其中最大的余数必大于 $\dfrac{25}{3}$, 即大于等于 9, 从而除数 $m > 9$. 此外上述三个等式相加有 $283 = m(q_1 + q_2 + q_3) + 25$, 即

$$m(q_1 + q_2 + q_3) = 258 = 2 \times 3 \times 43,$$

因此 m 是 258 的大于 9 的因数, 同时 m 必小于 63, 否则 m 除 63 的余数是 63(大于 25) 或 0, 不合题意, 故 $m = 43$. 所以其中最小的余数是 1.

陈景润小传

陈景润 (1933~1996) 是中国数学家, 1933 年 5 月 22 日生于福建省福州市. 1953 年毕业于厦门大学数学系. 由于他对塔内问题的一个结果作了改进, 受到华罗庚的重视, 1957 年经华罗庚的推荐被调到中国科学院数学研究所工作, 先任实习研究员、助理研究员, 再被聘为研究员及一级研究员, 并当选为中国科学院数学物理学部委员. 陈景润也是世界著名解析数论学家之一.

1966 年居于六平方米小屋的陈景润, 借一盏昏暗的煤油灯, 伏在床板上, 用一支笔, 耗去了几麻袋的草稿纸, 攻克了世界著名数学难题哥德巴赫猜想中的 (1+2), 创造了距摘取这颗数论皇冠上的明珠 (1+1) 只有一步之遥的辉煌. 他证明了 "每个大偶数都是一个素数及一个不超过两个素数的乘积之和", 使他在哥德巴赫猜想的研究上居世界领先地位. 这一结果国际上誉为 "陈氏定理", 受到广泛征引. 他研究 "哥德巴赫猜想" 和其他数论问题的成就, 至今仍然在世界上遥遥领先. 世界级的数学大师、美国学者阿·威尔 (A. Weil) 曾这样称赞他: "陈景润的每一项工作, 都好像是在喜马拉雅山山巅上行走. "

陈景润在工作上常常是废寝忘食甚至忘我的. 有一次, 他一边走路, 一边低头想问题, 突然撞到树, 他脱口而出: "噢, 对不起, 撞了你. " 还有一次, 他去理发店理发, 当时理发店里人很多, 他拿的是 38 号的小牌子. 他想, 轮到我还早, 时间多么宝贵啊, 我可不能白白浪费掉. 于是他走出理发店, 找了个安静的地方坐下来, 从口袋里掏出小本子背起了外文单词. 背了一会儿, 他突然想起上午读外文时有个地方没看懂, 他又跑到图书馆去查一查. 过了好久, 等他在图书馆里把不懂的东西弄懂了, 才高高兴兴地往理发店走去. 可当他路过外文阅览室时, 被其中各式的新书所吸引, 又跑进去看起书来直到太阳下山, 他才想起理发的事, 一摸口袋, 那张 38 号的小牌子还在, 但等他到理发店时, 这个号码早已过时了. 他甚至有一次在图书馆由于看书太专注了被图书管理员误锁在里面, 经多方求救才找来了管理员. 正是他的这种对数学研究的痴迷, 才使得他取得了常人无法达到的成果.

陈景润于 1978 年和 1982 年两次收到国际数学家大会的作 45 分钟报告的邀请. 这是作为一个数学家的自豪和骄傲. 由于他的关于哥德巴赫猜想等问题的杰出研究成果, 他与王元、潘承洞于 1982 年共同荣获国家自然科学奖一等奖. 陈景润共发表学术论文 70 余篇, 出版专著 4 部. 主要著作有《算术级数中的最小素数》《表达偶数为一个素数及一个不超过两个素数的乘积之和》《数学趣味谈》《组合数学》《哥德巴赫猜想》等. 1996 年 3 月 19 日下午 1 点 10 分, 陈景润在北京去世, 终年 63 岁.

习 题 1.2

1. 在大于 1999 的自然数中, 被 66 除后, 商与余数相等的数共有多少个? 这些数总和是多少?

2. 一个正整数, 如果用 7 进制表示, 则为 $\overline{xyz}$. 如果用 5 进制表示, 为 $\overline{zyx}$. 请用 10 进制表示此数.

3. (2006 年 "小学数学 ABC" 竞赛) 设 n 是一个正整数, 求 n 个 n 相乘的积 (即 n^n) 除以 $n+1$ 的余数.

4. 证明: 对任意整数 a, b, $3 \mid (a^2+b^2)$ 当且仅当 $3 \mid a$ 且 $3 \mid b$.

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

6. 设 α 为有理数, b 是使 $b\alpha$ 为整数的最小正整数, 证明: 若 c 和 $c\alpha$ 都是整数, 则 $b \mid c$.

7. (1991 年俄罗斯国际城镇数学竞赛) 找出 10 进制数, 使得这个数的每一位数字, 从第二位开始不比前一位数字小, 最后的数字是 5, 并且这些数字的平方也具有同样的性质.

(1) 找出 4 个这样的数;

(2) 证明有无限多个这样的数.

1.3　最大公因数

定义 1.3.1　设 a_1, a_2 是两个整数. 如果 $d|a_1$ 且 $d|a_2$, 那么, 称 d 是 a_1 和 a_2 的**公因数**(或**公约数**). 一般地, 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数. 如果 $d|a_1$, $d|a_2$, $\cdots$, $d|a_n$, 那么, 称 d 是 $a_1, a_2, \cdots, a_n$ 的**公因数**.

显然, 任意整数 $a_1, a_2, \cdots, a_n$ 都有公因数 (例如, ± 1). 并且, 如果这些整数不全为零, 则它们的公因数的个数有限, 这其中必存在一个最大的公因数. 由此, 可引进以下概念.

定义 1.3.2　设 a_1, a_2 是两个不全为零的整数. 称 a_1 和 a_2 的公因数中的最大者为 a_1 和 a_2 的**最大公因数**, 记作 (a_1, a_2). 一般地, 对不全为零的整数 $a_1, a_2, \cdots, a_n$, 称它们的公因数中的最大者为 $a_1, a_2, \cdots, a_n$ 的**最大公因数**, 记作 $(a_1, a_2, \cdots, a_n)$. 易知, 如果 d 是它们的公因数, 则 $(-d)$ 也是它们的公因数. 因此, 最大公因数一定是正整数.

特别地, 如果 $(a_1, a_2, \cdots, a_n)$=1, 则称 $a_1, a_2, \cdots, a_n$**互素**(或**互质**), 即它们的公因数只有 ± 1. 如果 $(a_i, a_j) = 1$, $1 \leqslant i, j \leqslant n, i \neq j$, 则称 $a_1, a_2, \cdots, a_n$**两两互素**(或**两两互质**).

显然, $a_1, a_2, \cdots, a_n$ 两两互素可以推出 $(a_1, a_2, \cdots, a_n) = 1$, 反之, 则不然.

例如: $(2, 3, 4) = 1$, 但 $(2, 4) = 2$.

定理 1.3.1　设 $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, 记 $A = \left\{ y \middle| y = \sum_{i=1}^{n} a_i x_i, x_i \in \mathbb{Z}, 1 \leqslant i \leqslant n \right\}$. 如果 y_0 是集合 A 中最小的正整数, 则 $y_0 = (a_1, a_2, \cdots, a_n)$.

证明　设 d 是 $a_1, a_2, \cdots, a_n$ 的任意一个公因数, 则由整除的线性性有 $d|y_0$, 于是有 $d \leqslant y_0$. 同时, 由 1.2 节例 1 的结论可知, 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整数, 所以 $y_0 = (a_1, a_2, \cdots, a_n)$.

推论 1.3.1　设不全为零的整数 $a_1, a_2, \cdots, a_n$ 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 $d|(a_1, a_2, \cdots, a_n)$, 进而, 若 $b_i|a_i$ $(1 \leqslant i \leqslant n)$, 则 $(b_1, b_2, \cdots, b_n)|(a_1, a_2, \cdots, a_n)$.

证明　由推论 1.3.1, 存在整数 $x_1', x_2', \cdots, x_n'$ 使得

$$a_1 x_1' + a_2 x_2' + \cdots + a_n x_n' = (a_1, a_2, \cdots, a_n),$$

再由 $d|a_i$ $(1 \leqslant i \leqslant n)$, 有

$$d|(a_1 x_1' + a_2 x_2' + \cdots + a_n x_n'),$$

即 $d|(a_1, a_2, \cdots, a_n)$. 又由