普通高等教育“十二五”规划教材

数论基础及其应用

沈忠华　编著

科学出版社

普通高等教育“十二五”规划教材

数论基础及其应用

沈忠华　编著

科学出版社

北京

内 容 简 介

本书主要介绍初等数论的基础理论，以及它们在密码学、信息安全等领域中的应用. 全书共分 11 章，包括整除理论、同余、简单密码、剩余系、不定方程、同余方程、公钥密码、二次剩余、原根、实数的表示、平方和等内容. 每章末附有习题.

本书适合作为普通高等院校数学类、计算机科学类、信息安全或电子与通信工程类高年级本科生和研究生的教材，也可作为相关领域研究人员的参考书.

图书在版编目(CIP)数据

数论基础及其应用/沈忠华编著. —北京：科学出版社, 2015.7

普通高等教育“十二五”规划教材

ISBN 978-7-03-044295-6

Ⅰ. 数… Ⅱ. ①沈… Ⅲ. ①数论-高等学校-教材 Ⅳ. ①O156

中国版本图书馆 CIP 数据核字(2015) 第 100378 号

责任编辑：姚莉丽 / 责任校对：蒋 萍

责任印制：霍 兵 / 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

文林印务有限公司印刷

科学出版社发行 各地新华书店经销

*

2015 年 7 月第 一 版 开本：720 × 1000 1/16

2015 年 7 月第一次印刷 印张：11 3/4

字数：236 000

定价：32.00 元

(如有印装质量问题，我社负责调换)

前　言

数论是数学的一个历史悠久的分支, 主要研究整数的性质和规律. 在很长的一个历史时期内, 数论被认为是一门没有应用价值的 "纯" 理论学科. 20 世纪中期以来, 数论的理论和方法在许多理论学科和应用学科领域中都得到了广泛而深入的应用, 尤其是在密码学中的应用, 不仅推动了密码学和信息安全技术的发展, 也有力地促进了数论与密码学、信息安全相关课题的研究, 使之增添了新的活力.

本书是在我们讲授数学专业 "初等数论" 和 "数论及其应用" 课程使用的讲义的基础上形成的, 曾在数学专业和应用数学专业本科生和研究生教学中使用, 目的是使学生在了解和掌握初等数论的基本理论和方法的同时, 较多地了解数论在密码学中的应用, 拓宽知识视野, 促进跨学科研究能力的养成. 在编写本书的时候, 也考虑到了其他专业的学生和科技人员对数论知识的需要.

逻辑推导是数学研究的一个特点, 数论研究尤是如此. 培养学生利用逻辑推理, 由浅入深, 由此及彼, 不断发现新的数学真理的能力, 是非常重要的. 基于这一认识, 在内容安排上, 本书力图让读者从已有的事实出发, 去发现新的数学结论. 因此, 在内容安排上, 我们改变了 "结论叙述 — 证明结论" 的模式, 尽量采用 "已有结论 — 逻辑推理 — 新的结论" 的模式, 使新的数学真理自然地显现出来, 让读者自己推导和发现新的知识. 我们的教学实践表明, 这有助于培养学生的逻辑推理能力, 也提高了他们的学习兴趣.

本书的编写得到了国家 "十二五" 密码研究规划课题、浙江省自然科学基金项目、浙江省基础数学重点学科建设项目、浙江省重点建设教材项目和杭州市应用密码学重点学科建设项目的支持. 杭州师范大学理学院对本书的编写提供了有力支持. 杭州师范大学于秀源教授对本书稿提出了许多建设性的建议. 借本书出版之际, 在此一并表示衷心的感谢.

限于作者水平有限, 本书谬误和不妥在所难免, 恳切地希望读者和同行批评指正.

沈忠华

2014 年 11 月

目　录

第1章　整除理论

1.1　带余数除法

在本书中, 以 $\mathbf{Z}$ 表示全体整数的集合, $\mathbf{N}$ 表示全体正整数的集合, 除特别声明外, 字母 $a, b, c, \cdots$ 等均表示整数.

设 b 是一个正整数. 那么, 互不相交的区间 $[bq, b(q+1))(q = 0, \pm 1, \pm 2, \cdots)$ 的和集是实轴, 因此, 任何整数 a 必落在唯一的一个区间 $[bq, b(q+1))$ 中, 即存在唯一的整数 q, $bq \leqslant a < b(q+1)$, 于是 $a = qb + r$, 其中 $r = a - bq$ 是唯一的, 并且 $0 \leqslant r < b$. 因此, 我们有如下结论.

定理 1.1.1 (带余数除法)　设 $a, b \in \mathbf{Z}, b > 0$, 则存在唯一的一对整数 q, r, 使得

$$a = qb + r, \quad 0 \leqslant r < b. \qquad \square$$

注 1　在定理 1.1.1 中, 称 q 是 b 除 a 的商, r 是 b 除 a 的余数.

定义 1.1.1　设 $a, b \in \mathbf{Z}, b \neq 0$, 若 $|b|$ 除 a 的余数是 0, 则称 b 整除 a(记作 $b \mid a$), 称 b 是 a 的约数 (因数, 或因子), a 是 b 的倍数; 否则, 称 a 不被 b 整除 (记为 $b \nmid a$); 若 $b \mid a$, $1 < |b| < |a|$, 则称 b 是 a 的真约数.

由定义 1.1.1 可知, a 与 $-a$ 有相同的约数, ± 1 与 $\pm a$ 显然是它们的约数.

下面的定理是显然的.

定理 1.1.2　下面的结论成立:

(1) 若 $b \mid a$, 则 b 除 a 的商是唯一的;

(2) $b(\neq 0)$ 的所有倍数是 $0, \pm b, \pm 2b, \cdots$;

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

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

(5) $b \mid a$, 且 $|a| < |b| \Rightarrow a = 0$;

(6) $b \mid a_1, b \mid a_2, m_1, m_2 \in \mathbf{Z} \Rightarrow b \mid a_1 m_1 + a_2 m_2$. $\square$

定义 1.1.2　一个大于 1 的整数, 若除了数 1 和它自身外, 没有另外的约数, 则称为素数. 除了 1 和它自身外, 还有其他约数的数称为合数.

由这个定义我们知道, 一个大于 1 的整数, 要么是素数, 要么是合数.

如果整数 $a(a \neq 0, \pm 1)$ 是合数, 那么, a 的正约数只有有限个, 故必有最小的, 设为 d. 若 d 不是素数, 则有真约数 $d_1, d_1 > 1, d_1 \mid d, d > d_1$, 而且 $d_1 \mid a$. 这与 d 的

最小性矛盾, 故 d 必是素数. 因此, 存在整数 q, 使得 $a = dq$, 于是 $|a| \geqslant d^2$, 即 $d \leqslant \sqrt{|a|}$. 因此, 有如下结论.

定理 1.1.3　任一整数 $a(a \neq 0, \pm 1)$ 的大于 1 的最小约数 d 是素数; 若 $d \neq a$, 则 $d \leqslant \sqrt{|a|}$. □

定理 1.1.3 告诉我们一个判定整数素性的方法: 如果一个整数 a 不被不超过 $\sqrt{|a|}$ 的素数整除, 它一定是素数.

例 1.1.1　判定 97 是否是素数.

解　由于不超过 $\sqrt{97}$ 的素数 2, 3, 5, 7 都不能整除 97, 所以 97 是素数.

利用定理 1.1.2 还可以逐个列出素数. 这就是 Eratosthenes 筛法. 下面是一个具体的例子.

例 1.1.2　写出不超过 100 的所有的素数.

解　将不超过 100 的正整数排列如下:

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

按以下步骤进行:

(i) 删去 1, 剩下的后面的第一个数是 2, 2 是素数;

(ii) 删去 2 后面的被 2 整除的数, 剩下的 2 后面的第一个数是 3, 3 是素数;

(iii) 再删去 3 后面的被 3 整除的数, 剩下的 3 后面的第一个数是 5, 5 是素数;

(iv) 再删去 5 后面的被 5 整除的数, 剩下的 5 后面的第一个数是 7, 7 是素数;

.....

照以上步骤可以依次得到不超过 100 的所有的素数 2, 3, 5, 7, 11, $\cdots$, 97.

要指出的是, Eratosthenes 筛法在理论上是可行的; 但在实际应用中, 由于需要大量的计算, 是不可取的.

定理 1.1.1 虽然简单, 却是数论的基础. 下面我们给出它的一个应用.

设 $b > 1$ 是整数. 那么, 对于任何正整数 a, 由定理 1.1.1, 有整数 k, 使得

$$a = q_1 b + a_0, \quad 0 \leqslant a_0 \leqslant b - 1, \quad q_1 \geqslant b,$$

$$q_1 = q_2 b + a_1, \quad 0 \leqslant a_1 \leqslant b-1, \quad q_2 \geqslant b,$$

$$\cdots\cdots$$

$$q_{k-1} = q_k b + a_{k-1}, 0 \leqslant a_{k-1} \leqslant b-1, 0 < q_k \leqslant b-1,$$

其中诸 a_i 与 q_i 都是唯一确定的. 记 $q_k = a_k$, 则 $0< a_k \leqslant b-1$, 并且

$$\begin{aligned} a = q_1 b + a_0 &= (q_2 b + a_1)b + a_0 = q_2 b^2 + a_1 b + a_0 \\ &= (q_3 b + a_2)b^2 + a_1 b + a_0 = q_3 b^3 + a_2 b^2 + a_1 b + a_0 \\ &= \cdots \\ &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0. \end{aligned}$$

因此, 有如下结论.

定理 1.1.4 设 b 是大于 1 的整数, 则任何正整数 a 都可以写成

$$a = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

的形式, 其中 $a_k \neq 0$, $a_i (0 \leqslant i \leqslant k)$ 是在 0 与 $b-1$ 之间唯一确定的整数. □

定义 1.1.3 设 b 是正整数, n 是正整数, 并且

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

其中 $a_k \neq 0, 0 \leqslant a_i \leqslant b-1 (0 \leqslant i \leqslant k)$, 则称 $(a_k, a_{k-1}, \cdots, a_1, a_0)_b$ 是 n 的 b 进制表示, 称 n 是 $k+1$ 位 b 进制数, $k+1$ 是 n 的 b 进制位数, $a_i (0 \leqslant i \leqslant k)$ 是 n 的 b 进制表示的第 $i+1$ 个位数码 (或第 $i+1$ 位数).

为了叙述方便, 今后, 对于十进制表示的数, 将仍使用常规的写法.

注 2 以 $[x]$ 表示不超过 x 的最大整数. 若 $n = (a_k, a_{k-1}, \cdots, a_1, a_0)_b, a_k \neq 0$, 则

$$b^k \leqslant n < b^{k+1}, \quad k \leqslant \log_b n < (k+1),$$

即 $k = [\log_b n]$.

例 1.1.3 若 n 是整数, 则 n^2 被 8 除的余数只可能是 0, 1, 或 4.

解 整数 n 只可能是 $n = 8q + r$ 的形式, 其中 r=0, 1, 2, $\cdots$, 或 7. 直接计算即可得到结论.

习 题 1.1

1. 证明定理 1.1.2 的结论 (5).
2. 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.

3. 设 b 是大于 1 的整数, α 是小于 1 的正实数. 证明下面的结论:

(1) 对于任意的正整数 k, 存在唯一的整数 a_i, $0 \leqslant a_i \leqslant b-1 (0 \leqslant i \leqslant k)$ 及实数 $\alpha_k, 0 \leqslant \alpha_k < 1$, 使得

$$\alpha = \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots + \frac{a_k}{b^k} + \frac{\alpha_k}{b^k};$$

(2) 如果总是 $\alpha_k \neq 0 (k \geqslant 1)$, 则无穷级数 $\sum\limits_{i=1}^{\infty} \frac{a_i}{b^i}$ 收敛于 α;

(3) 如果对于任意的正整数 m, 都有某个 $n > m$, 使得 $a_n \neq b-1$, 则结论 (2) 中的 α 的级数表示是唯一的.

如果级数 $\sum\limits_{i=1}^{\infty} \frac{a_i}{b^i}$ 是有限项, 那么结论 (3) 还成立吗?

4. 设 a 与 b 是正整数, 证明在 $1, 2, \cdots, a$ 中能被 b 整除的整数恰有 $\left[\frac{a}{b}\right]$ 个.

1.2　辗转相除法

定义 1.2.1　整数 $a_1, a_2, \cdots, a_k$ 的公共约数称为 $a_1, a_2, \cdots, a_k$ 的公约数. 不全为零的整数 $a_1, a_2, \cdots, a_k$ 的公约数中最大的一个称为 $a_1, a_2, \cdots, a_k$ 的最大公约数 (或最大公因数), 记为 $(a_1, a_2, \cdots, a_k)$.

由于每个非零整数的约数的个数是有限的, 所以最大公约数是存在的, 并且是正整数.

定义 1.2.2　如果 $(a_1, a_2, \cdots, a_k) = 1$, 则称 $a_1, a_2, \cdots, a_k$ 是互素的 (或互质的); 如果

$$(a_i, a_j) = 1, \quad 1 \leqslant i, j \leqslant k, \ i \neq j,$$

则称 $a_1, a_2, \cdots, a_k$ 是两两互素的 (或两两互质的).

显然, $a_1, a_2, \cdots, a_k$ 两两互素可以推出 $(a_1, a_2, \cdots, a_k) = 1$; 反之则不然, 例如 $(3, 6, 4) = 1$, $(6, 4) = 2$.

设 a, q, r 和 b 是整数, $a = bq + r$, 那么, 由定理 1.1.2, 如果 $d|a$, $d|b$, 则有 $d|r = a - bq$, 反之, 若 $d|b$, $d|r$, 则 $d|a = bq + r$. 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, 这两个集合中的最大正数当然相等, 即 $(a, b) = (b, r)$. 由此得到下面定理 1.2.1 的结论 (v), 这个定理的其他结论是显然的.

定理 1.2.1　下面的结论成立:

(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 $a=bq+r$, 则 $(a, b) = (b, r)$.　□

注 1 由定理 1.2.1 可知, 在讨论 $(a_1, a_2, \cdots, a_n)$ 时, 不妨假设 $a_1, a_2, \cdots, a_n$ 是正整数, 以后我们就维持这一假设.

设 a 和 b 是整数, $b \neq 0$, 由定理 1.2.1 可知, 如果

$$a = bq_1 + r_1, \quad 0 < r_1 < |b|,$$

则 $(a,b)=(b, r_1)$. 若又有

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1,$$

则 $(b, r_1) = (r_1, r_2)$, 等等. 这样, 如果不断地把带余数除法做下去, 我们得到下面的一组除法:

$$\begin{aligned}
&a = bq_1 + r_1, && 0 < r_1 < |b|,\\
&b = r_1 q_2 + r_2, && 0 < r_2 < r_1,\\
&r_1 = r_2 q_3 + r_3, && 0 < r_3 < r_2,\\
&\quad \cdots\cdots &&\\
&r_{k-1} = r_k q_{k+1} + r_{k+1}, && 0 < r_{k+1} < r_k,\\
&\quad \cdots\cdots &&\\
&r_{n-2} = r_{n-1} q_n + r_n, && 0 < r_n < r_{n-1},\\
&r_{n-1} = r_n q_{n+1}. &&
\end{aligned} \tag{1.2.1}$$

根据上面的分析, 我们知道

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n.$$

这是一个计算最大公约数的有效方法. 上面的这一组算式称为辗转相除法, 或辗转相除算法 (算式).

由 (1.2.1) 中的式子, 我们看到,

$$\begin{aligned}
r_1 &= a - bq_1 = a \cdot 1 - bq_1,\\
-r_2 &= r_1 q_2 - b = (a - bq_1)q_2 - b = aq_2 - b(q_1 q_2 + 1).
\end{aligned}$$

记

$$P_n = q_n P_{n-1} + P_{n-2}, \quad Q_n = q_n Q_{n-1} + Q_{n-2}.$$

假设对于 $k < m (1 \leqslant m \leqslant n)$ 有 $aQ_k - bP_k = (-1)^{k-1} r_k$, 那么, 由 (1.2.1) 就得到

$$r_n = r_{n-2} - r_{n-1} q_n = (-1)^{n-3}(aQ_{n-2} - bP_{n-2}) - (-1)^{n-2}(aQ_{n-1} - bP_{n-1})q_n$$

$$= (-1)^{n-1}(a(Q_{n-2} + Q_{n-1}q_n) - b(P_{n-2} + P_{n-1}q_n)) = (-1)^{n-1}(aQ_n - bP_n).$$

这样, 由归纳法得到如下结论.

定理 1.2.2　使用式 (1.2.1) 中的记号, 记

$$P_0 = 1, \quad P_1 = q_1, \quad P_k = q_k P_{k-1} + P_{k-2}, \quad k \geqslant 2,$$

$$Q_0 = 0, \quad Q_1 = 1, \quad Q_k = q_k Q_{k-1} + Q_{k-2}, \quad k \geqslant 2,$$

则

$$aQ_k - bP_k = (-1)^{k-1} r_k, \quad k = 1, 2 \cdots, n. \tag{1.2.2}$$

□

我们已经知道 $r_n = (a, b)$, 所以又有如下结论.

定理 1.2.3　存在整数 x 和 y, 使得 $(a, b) = ax + by$. □

下面, 我们要对 (1.2.1) 中所包含的等式的个数, 即要做的带余数除法的次数进行估计.

设 $a, b \in \mathbf{N}, a > b$. 在组式 (1.2.1) 中, 我们见到

$$r_{k-1} = r_k q_{k+1} + r_{k+1}, \quad 1 \leqslant k \leqslant n-1,$$

其中 $r_n \geqslant 1, q_{n+1} \geqslant 2, q_i \geqslant 1 (1 \leqslant i \leqslant n)$.

现在, 用下面的方式定义 Fibonacci 数列 $\{F_n\}$:

$$F_1 = F_2 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad n \geqslant 3, \tag{1.2.3}$$

那么, 由组式 (1.2.1), 见到

$$\begin{aligned} & r_n \geqslant 1 = F_2, \\ & r_{n-1} \geqslant 2 r_n \geqslant 2 = F_3, \\ & r_{n-2} \geqslant r_{n-1} + r_n \geqslant F_3 + F_2 = F_4, \\ & \qquad \cdots\cdots \\ & b \geqslant r_1 + r_2 \geqslant F_{n+1} + F_n = F_{n+2}. \end{aligned} \tag{1.2.4}$$

另一方面, 我们知道,

$$F_n \geqslant \left(\frac{\sqrt{5}+1}{2} \right)^{n-2}. \tag{1.2.5}$$

由式 (1.2.3) 和 (1.2.5) 得到

$$b \geqslant \left(\frac{1+\sqrt{5}}{2} \right)^{n},$$

即

$$\log_{10} b \geqslant n \log_{10} \frac{1+\sqrt{5}}{2} > \frac{1}{5} n. \tag{1.2.6}$$

由式 (1.2.6) 得到了如下结论.

定理 1.2.4(Lame) 设 $a,b\in\mathbf{N},a>b$, 使用在式 (1.2.1) 中的记号, 则 $n<5\log_{10}b$. □

例 1.2.1 设 a 和 b 是正整数, 那么只使用被 2 除的除法运算和减法运算就可以计算出 $(a,\ b)$.

解 下面的四个基本事实给出了证明:

(i) 若 $a|b$, 则 $(a,\ b)=a$;

(ii) 若 $a=2^{\alpha}a_1,2\nmid a_1,b=2^{\beta}b_1,2\nmid b_1,\alpha\geqslant\beta\geqslant 1$, 则

$$(a,b)=2^{\beta}(2^{\alpha-\beta}a_1,b_1);$$

(iii) 若 $2\nmid a,b=2^{\beta}b_1,2\nmid b_1$, 则 $(a,b)=(a,b_1)$;

(iv) 若 $2\nmid a,2\nmid b$, 则 $(a,b)=\left(\left|\dfrac{a-b}{2}\right|,b\right)$.

例 1.2.2 用辗转相除法求 $(125,\ 17)$, 以及 $x,\ y$, 使得

$$125x+17y=(125,17).$$

解 做辗转相除法:

$$\begin{aligned}
&125=7\cdot 17+6, && q_1=7, && r_1=6,\\
&17=2\cdot 6+5, && q_2=2, && r_2=5,\\
&6=1\cdot 5+1, && q_3=1, && r_3=1,\\
&5=5\cdot 1, && q_4=5.
\end{aligned}$$

由定理 1.2.1, $(125,\ 17)=r_3=1$.

计算

$$\begin{aligned}
&P_0=1, && P_1=7, && P_2=2\cdot 7+1=15, && P_3=1\cdot 15+7=22,\\
&Q_0=0, && Q_1=1, && Q_2=2\cdot 1+0=2, && Q_3=1\cdot 2+1=3,
\end{aligned}$$

在定理 1.2.2 中, 取 $x=(-1)^{3-1}Q_3=3,\ y=(-1)^3P_3=-22$, 则

$$125\cdot 3+17\cdot(-22)=(125,17)=1.$$

例 1.2.3 求 $(12345,\ 678)$.

解
$$\begin{aligned}
(12345,678)&=(12345,339)=(12006,\ 339)=(6003,\ 339)\\
&=(5664,\ 339)=(177,\ 339)=(177,\ 162)=(177,\ 81)\\
&=(96,\ 81)=(3,\ 81)=3.
\end{aligned}$$

习　题　1.2

1. 用辗转相除法求整数 x, y, 使得 $1387x - 162y = (1387, 162)$.
2. Fibonacci 数列的相邻两项能否有大于 1 的最大公约数?
3. 证明: 若 $(a, 4) = (b, 4) = 2$, 则 $(a + b, 4) = 4$.

1.3　最大公约数的性质

对于给定的整数 $a_1, a_2, \cdots, a_k$, 用 $y_0 = a_1x_1' + \cdots + a_nx_n'$ 表示集合

$$A = \left\{ y; y = \sum_{i=1}^{k} a_i x_i, x_i \in \mathbf{Z}, 1 \leqslant i \leqslant k \right\}$$

中最小的正整数, 那么, 由带余数除法可知, 对于集合 A 中的任一整数 y, 存在 q, $r_0 \in \mathbf{Z}$, 使得

$$y = qy_0 + r_0, \quad 0 \leqslant r_0 < y_0,$$

因此

$$r_0 = y - qy_0 = a_1(x_1 - qx_1') + \cdots + a_n(x_n - qx_n') \in A.$$

如果 $r_0 \neq 0$, 那么, 因为 $0 < r_0 < y_0$, 所以 r_0 是 A 中比 y_0 还小的正整数, 这与 y_0 的定义矛盾. 所以 $r_0 = 0$, 即 $y_0 | y$. 这样, y_0 就整除 $a_1, a_2, \cdots, a_k$, 是它们的一个公约数. 但是, 它显然被 $a_1, a_2, \cdots, a_k$ 的每个公约数整除, 所以它是 $a_1, a_2, \cdots, a_k$ 的最大公约数. 因此, 有如下结论.

定理 1.3.1　设 $a_1, a_2, \cdots, a_k \in \mathbf{Z}$, 记

$$A = \left\{ y; y = \sum_{i=1}^{k} a_i x_i, x_i \in \mathbf{Z}, 1 \leqslant i \leqslant k \right\}.$$

如果 y_0 是集合 A 中最小的正数, 则 $y_0 = (a_1, a_2, \cdots, a_k)$. □

根据此定理, 我们可以得到如下几个推论.

推论 1.3.1　设 d 是 $a_1, a_2, \cdots, a_k$ 的一个公约数, 则 $d | (a_1, a_2, \cdots, a_k)$. □

这个推论对最大公约数的性质做了更深的刻画: 最大公约数不但是公约数中的最大的, 而且是所有公约数的倍数.

推论 1.3.2　$(ma_1, ma_2, \cdots, ma_k) = |m|(a_1, a_2, \cdots, a_k)$. □

推论 1.3.3　记 $\delta = (a_1, a_2, \cdots, a_k)$, 则

$$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \cdots, \frac{a_k}{\delta} \right) = 1.$$ □

特别地, $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$.

推论 1.3.4 $(a_1, a_2, \cdots, a_k) = 1$ 的充要条件是存在整数 $x_1, x_2, \cdots, x_k$, 使得

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1. \tag{1.3.1}$$

□

由定理 1.2.3, 如果 $(a, b) = 1$, 则存在整数 x 与 y, 使得 $ax + by = 1$. 因此, 对于任意的整数 c, 就有

$$acx + bcy = c. \tag{1.3.2}$$

由此可见,

(i) 如果 $b|ac$, 则由式 (1.3.2) 得到必有 $b|c$;

(ii) 如果 $b|c$ 且 $a|c$, 则 $ab|ac, ab|bc$, 由式 (1.3.2) 得到 $ab|c$;

(iii) 如果 d 是 a 与 bc 的一个公约数, 由式 (1.3.2) 得到, $d|c$, 即 d 是 a 与 c 的公约数. 当然, a 与 c 的公约数也是 a 与 bc 的公约数. 因此, a 与 c 的公约数的集合, 就是 a 与 bc 的公约数的集合, 所以, $(a, bc) = (a, c)$.

根据上面的分析, 我们可以得到如下结论.

定理 1.3.2 对于任意的整数 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 $ab|c$;

(iii) 若 $(a, b) = 1$, 则 $(a, bc) = (a, c)$. □

推论 1.3.5 若 p 是素数, 则下述结论成立:

(i) $p|ab \Rightarrow p|a$ 或 $p|b$;

(ii) $p|a^2 \Rightarrow p|a$. □

推论 1.3.6 若 $(a, b_i) = 1, 1 \leqslant i \leqslant n$, 则 $(a, b_1b_2 \cdots b_n) = 1$. □

我们知道, 用辗转相除法可以求出两个数的最大公约数. 现在, 我们考虑如何求出三个以上的数的最大公约数.

假设对于任意的 n 个整数 $a_1, a_2, \cdots, a_{n-1}$, 我们可以求出 $d_{n-1} = (a_1, a_2, \cdots, a_{n-1})$.

对于整数 a_n, 记 $d_n = (d_{n-1}, a_n)$.

首先, 我们有 $d_{n-1}|a_i (1 \leqslant i \leqslant n-1)$, 因此, $d_n|a_i (1 \leqslant i \leqslant n)$, 即它是 $a_1, a_2, \cdots, a_{n-1}, a_n$ 的一个公约数. 另一方面, 由推论 1.3.1, 若 d 是 $a_1, a_2, \cdots, a_{n-1}, a_n$ 的一个公约数, 那么, $d|d_{n-1}$, 从而, d 是 d_{n-1} 和 a_n 的一个公约数, 因此, $d|(d_{n-1}, a_n) = d_n$.

这样, 我们得到如下结论.

定理 1.3.3 对于任意的 n 个整数 $a_1, a_2, \cdots, a_n$, 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

$$d_n = (a_1, a_2, \cdots, a_n).$$ □

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

解　由定理 1.3.1 得到

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

注 1　一般地, 若 $(x, y) = 1$, 那么, 对于任意的整数 a, b, 有

$$(x, y) = (x - ay, y) = (x - ay, y - b(x - ay)) = (x - ay, (ab+1)y - bx),$$

因此, $\dfrac{x - ay}{(ab+1)y - bx}$ 是既约分数.

例 1.3.2　证明：$121 \nmid n^2 + 2n + 12$, $n \in \mathbf{Z}$.

解　由于 $121 = 11^2$, $n^2 + 2n + 12 = (n+1)^2 + 11$, 所以, 若

$$11^2 | (n+1)^2 + 11, \tag{1.3.3}$$

则 $11 | (n+1)^2$, 因此, 由推论 1.3.5 得到

$$11 | n+1, \quad 11^2 | (n+1)^2.$$

再由式 (1.3.3) 得到

$$11^2 | 11,$$

这是不可能的. 所以式 (1.3.3) 不能成立.

注 2　这个例题的一般形式是：

设 p 是素数, a, b 是整数, 则

$$p^k \nmid (an + b)^k + p^{k-1}c,$$

其中 c 是不被 p 整除的任意整数, k 是任意的大于 1 的整数.

例 1.3.3　设 a 和 b 是正整数, $b > 2$, 则 $2^b - 1 \nmid 2^a + 1$.

解　(i) 若 $a < b$, 且

$$2^b - 1 | 2^a + 1. \tag{1.3.4}$$

成立, 则

$$2^b - 1 \leqslant 2^a + 1 \Rightarrow 2^b - 2^a \leqslant 2 \Rightarrow 2^a(2^{b-a} - 1) \leqslant 2,$$

于是 $a = 1$, $b - a = 1$, 即 $b = 2$, 这是不可能的, 所以式 (1.3.4) 不成立.

(ii) 若 $a=b$, 且式 (1.3.4) 成立, 则由式 (1.3.4) 得到

$$2^a-1|(2^a-1)+2 \Rightarrow 2^a-1|2 \Rightarrow 2^a-1 \leqslant 2 \Rightarrow 2^a \leqslant 3,$$

于是 $b=a=1$, 这是不可能的, 所以式 (1.3.4) 不成立.

(iii) 若 $a>b$, 记 $a=kb+r$, $0 \leqslant r<b$, 此时

$$2^{kb}-1=(2^b-1)(2^{(k-1)b}+2^{(k-2)b}+\cdots+1)=(2^b-1)\dot{Q},$$

其中 Q 是整数. 所以

$$\begin{aligned}2^a+1&=2^{kb+r}+1=2^r(2^{kb}-1+1)+1\\&=2^r((2^b-1)Q+1)+1=(2^b-1)Q'+(2^r+1),\end{aligned}$$

其中 Q' 是整数. 因此

$$2^b-1|2^a+1 \Rightarrow 2^b-1|2^r+1,$$

在 (i) 中已经证明这是不可能的, 所以式 (1.3.4) 不能成立.

综上证得 $2^b-1 \nmid 2^a+1$.

习 题 1.3

1. 证明推论 1.3.1$\sim$ 推论 1.3.6.
2. 设 $x, y \in \mathbf{Z}$, $17|2x+3y$, 证明: $17|9x+5y$.
3. 设 $a, b, c \in \mathbf{N}$, c 无平方因子, $a^2|b^2c$, 证明: $a|b$.
4. 设 n 是正整数, 求 $\mathrm{C}_{2n}^1, \mathrm{C}_{2n}^3, \cdots, \mathrm{C}_{2n}^{2n-1}$ 的最大公约数.

1.4 最小公倍数

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

根据这个定义, 容易得到如下结论.

定理 1.4.1 下面的等式成立:

(i) $[a, 1]=|a|$, $[a, a]=|a|$;

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

(iii) $[a_1, a_2, \cdots, a_k]=[|a_1|, |a_2|\cdots, |a_k|]$;

(iv) 若 $a|b$, 则 $[a, b]=|b|$. □