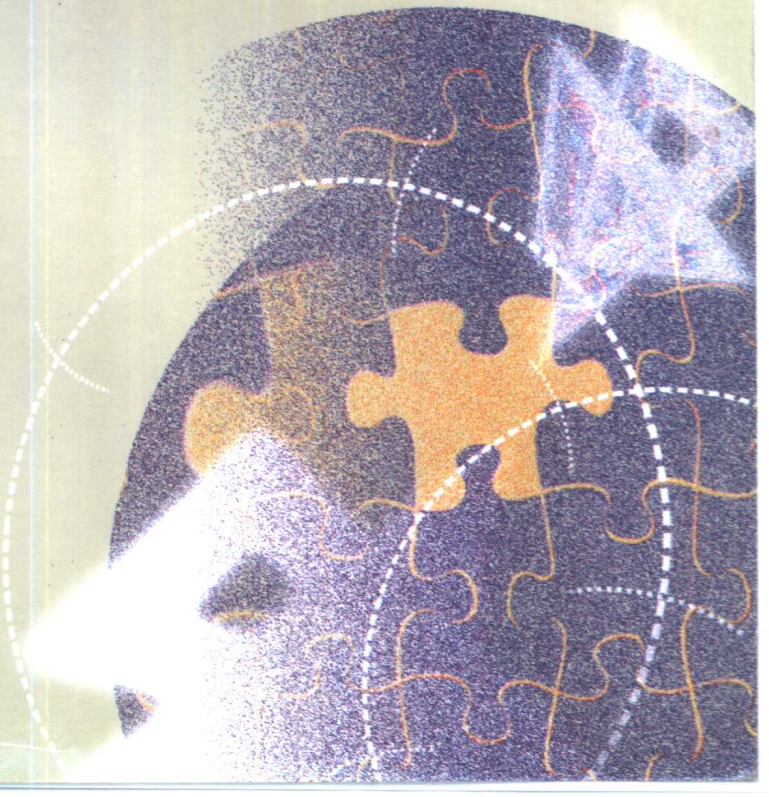
研究生教材

Graduate Student

代数学基础

李 超 谢端强 等编著



防科技大学出版社

内 容 简 介

本书主要介绍数论、多项式、群、环、域、模和格的基本理论与方法，内容精炼，深入浅出，每节后配有习题，可作为高等院校工科类研究生数学基础教材。

图书在版编目(CIP)数据

代数学基础/李超等编著.—长沙：国防科技大学出版社，2000.10

ISBN 7-81024-698-4

Ⅰ.代… Ⅱ.李… Ⅲ.代数 Ⅳ.O15

中国版本图书馆 CIP 数据核字(2000)第 56445 号

国防科技大学出版社出版发行

电话：(0731)4572640 邮政编码：410073

E-mail：gfkdcbs@ox.hn.cn

责任编辑：谷建湘 责任校对：石少平

新华书店总店北京发行所经销

国防科技大学印刷厂印装

开本：850×1168 1/32 印张：9.875 字数：248 千

2000 年 11 月第 1 版第 1 次印刷 印数：1—3000 册

定价：15.00 元

前　言

代数学的理论与方法无论是对整个数学的发展与完善，还是对学生数学综合素质的培养与提高，都具有不可替代的作用.随着科学技术的进步，特别是计算机技术的迅速发展与普及，代数学在通信、系统工程和计算机科学等许多领域都有非常广泛的应用.

本书是在国防科技大学工科博士研究生公共课讲义《代数学基础》的基础上形成的，主要介绍抽象代数的基本概念、基本方法和主要结论，使学生在此基础上通过自学进一步提高数学素质，并能在其他课程的学习和应用领域的研究中发挥作用.

本书前五章约需 50 教学课时，主要介绍数论、多项式、群、环和域的基本理论与方法.我们力图做到内容精炼准确，叙述深入浅出，文字简洁生动.第六章和第七章为选学内容，分别介绍模论和格论的基本理论与方法，教学过程中可根据教学的需要取舍.

第一、二、三章由李超编写，第四、五章由谢端强编写，第六、七章分别由冯良贵和戴清平编写.

本书集我校代数组全体同仁多年教学经验之大成，虽经十分努力，仍恐难免有误，皆因编者学识水平有限.书中不当之处，望各位专家不吝赐教.

作者

2000 年 10 月

目　录

第一章　数论的基本知识

初等数论研究整数环中整数的最基本性质，是一门十分重要的数学基础课．整除理论、同余理论和不定方程的求解是初等数论的基本内容．整除理论是初等数论的基础，其中心问题是算术基本定理与最大公因数理论．同余理论是初等数论的核心，它是数论所特有的思想与方法，这一理论是德国大数学家 C. F. Gauss 于 1801 年在他的《算术探讨》一书中首先提出并加以研究，它标志着数论从此成为一门独立的学科．求解不定方程是推动数论发展的最主要课题．

本章主要介绍整除理论与同余理论，在此基础上介绍一类最基本的不定方程的求解方法．值得注意的是，数论中除了以上的三部分内容，还有许多在理论研究与工程应用中有意义的内容，比如连分数与 Pell 方程、素数分布、数论函数、二次剩余、三角和与特征等等．有兴趣的读者可以参见文献[1]～[3]．

§1.1　整除性

本书中我们总是以 $\boldsymbol{N}$、$\boldsymbol{Z}$、$\boldsymbol{Q}$、$\boldsymbol{R}$ 和 $\boldsymbol{C}$ 分别表示自然数集、整数集、有理数集、实数集与复数集．整除理论主要探讨整数集 $\boldsymbol{Z}$ 中整数的算术运算性质．

在整数集 $\boldsymbol{Z}$ 中可以作加法、减法和乘法三种运算，并且整数关于加法运算满足如下基本性质：

(1) 封闭律 $\forall a,b \in \boldsymbol{Z}$， $a+b \in \boldsymbol{Z}$；

(2) 结合律 $\forall a,b,c \in \boldsymbol{Z}$， $(a+b)+c=a+(b+c)$；

(3) 有单位元 存在 $0 \in \boldsymbol{Z}$，$\forall a \in \boldsymbol{Z}$，均有

$$a+0=0+a=a;$$

(4) 有逆元 $\forall a \in \boldsymbol{Z}$，存在 $b \in \boldsymbol{Z}$，使得

$$a+b=b+a=0;$$

(5) 交换律 $\forall a,b \in \boldsymbol{Z}$， $a+b=b+a$.

一个非空集合，关于某种运算如果满足性质(1)～(2)，我们称它具有**半群**结构；如果满足性质(1)～(4)，我们称它具有**群**结构；进一步，如果满足性质(1)～(5)，我们称它具有 **Abel 群**结构. 由此可知整数集关于加法是一个 Abel 群. 我们称 Abel 群中单位元为**零元**，每个元素的逆元为**负元**，并且对任意 $a,b \in \boldsymbol{Z}$，$a-b=a+(-b)$，故减法为加法的逆运算.

下面我们考虑整数集 $\boldsymbol{Z}$ 关于乘法运算的性质：

(1) 封闭律 $\forall a,b \in \boldsymbol{Z}$， $ab \in \boldsymbol{Z}$；

(2) 结合律 $\forall a,b,c \in \boldsymbol{Z}$， $(ab)c=a(bc)$；

(3) 有单位元 存在 $1 \in \boldsymbol{Z}$，$\forall a \in \boldsymbol{Z}$， $a1=1a=a$；

(4) 交换律 $\forall a,b \in \boldsymbol{Z}$， $ab=ba$.

由此可知整数集关于乘法构成一个有单位元的交换半群，但它不构成群. 这是因为，并不是对每一个 $m \in \boldsymbol{Z}$，均存在 $n \in \boldsymbol{Z}$，使得 $mn=1$. 事实上，在整数集 $\boldsymbol{Z}$ 中只有 ± 1 具有乘法逆元.

整数集 $\boldsymbol{Z}$ 关于加法构成 Abel 群，关于乘法构成半群，而且乘

法对加法如下分配律成立:对任意 $a,b,c \in \boldsymbol{Z}$,

$$a(b+c) = ab + ac,$$

$$(a+b)c = ac + bc.$$

于是我们称 $(\boldsymbol{Z}, +, \cdot)$ 为一个**环**.又由于整数环 $\boldsymbol{Z}$ 关于乘法还满足乘法性质(3)和(4),我们称 $\boldsymbol{Z}$ 为**有单位元的交换环**.同样分析可知,全体有理数集合 $\boldsymbol{Q}$ 关于有理数的加法与乘法构成一个环,并且也是有单位元的交换环.但是与整数环 $\boldsymbol{Z}$ 不同的是,在有理数环 $\boldsymbol{Q}$ 中,对每个有理数 $a \neq 0$ 而言,一定存在另一个有理数 b,使得 $ab = 1$(这里 1 为乘法单位元),我们称 b 为 a 的**乘法逆元**.也就是说,有理数环 $\boldsymbol{Q}$ 的代数结构比整数环 $\boldsymbol{Z}$ 的代数结构更整齐.事实上,正如我们在第四章中所讲的,$(\boldsymbol{Q}, +, \cdot)$ 具有**域**结构,我们称 $\boldsymbol{Q}$ 为**有理数域**.

由于整数环 $\boldsymbol{Z}$ 中乘法不满足有逆元性质,从而除法不能作为乘法的逆运算,为此需要研究整数环中整数的整除性.

定义 1.1 设 $a,b \in \boldsymbol{Z}$, $b \neq 0$, 如果存在 $c \in \boldsymbol{Z}$, 使得 $a = bc$, 则称 b **整除** a, 记作 $b \mid a$, 否则称 b **不整除** a, 记作 $b \nmid a$.

如果 $b \mid a$, 我们称 b 为 a 的**因数**,称 a 为 b 的**倍数**.显然 1 和 -1 是任何整数的因数,所有的非零整数都是 0 的因数.进一步,由整除的定义,易推出如下性质:

(1) 如果 $c \mid b, b \mid a$,则 $c \mid a$;

(2) 如果 $c \mid a, c \mid b$, 则 $\forall m, n \in \boldsymbol{Z}, c \mid (ma + nb)$;

(3) 如果 $b \mid a$ 且 $a \neq 0$,则 $|b| \leqslant |a|$;

(4) 如果 $a \mid b, b \mid a$,则 $a = \pm b$.

例 1.1 证明:对任意 $n \in \boldsymbol{N}$, $6 \mid n(n+1)(2n+1)$.

证明 对 n 用第一数学归纳法证明.

(1)当 $n = 1$ 时, $n(n+1)(2n+1) = 1 \times 2 \times 3 = 6$,它是6的倍数,结论成立.

(2)假设当 $n = k$ 时,结论成立.即

$$6 \mid k(k+1)(2k+1).$$

则当 $n = k+1$ 时,

$$\begin{aligned} n(n+1)(2n+1) &= (k+1)(k+2)(2k+3) \\ &= k(k+1)(2k+1) + 6(k+1)^2. \end{aligned}$$

由归纳假设, $6 \mid k(k+1)(2k+1)$,并且 $6 \mid 6(k+1)^2$. 从而

$$6 \mid (k+1)(k+2)(2k+3)$$

由归纳法原理, $6 \mid n(n+1)(2n+1)$ 对任意 $n \in \boldsymbol{N}$ 成立. □

例 1.2 如果 $m, n, p, q \in \boldsymbol{Z}$,并且 $(m-p) \mid (mn+pq)$,证明 $(m-p) \mid (mq+np)$.

证明 由于

$$\begin{aligned} mq + np &= mq - pq + pq + mn - mn + np \\ &= q(m-p) + (mn+pq) - n(m-p). \end{aligned}$$

右边的三项都是 $(m-p)$ 的倍数,从而

$$(m-p) \mid (mq+np).$$ □

定理 1.1(带余除法) 设 $a, b \in \boldsymbol{Z}, b \neq 0$,则存在唯一的 q, $r \in \boldsymbol{Z}$,使得 $a = bq + r$,这里 $0 \leqslant r < |b|$.

证明 不妨设 $b > 0$. 考虑如下整数序列:

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

则对任意 $a \in \boldsymbol{Z}$,必存在 $q \in \boldsymbol{Z}$,使得

$$qb \leqslant a < (q+1)b.$$

令 $r = a - qb$,则 $0 \leqslant r < b$,并且 $a = bq + r$.

下面讨论 q, r 的唯一性.

如果 $a = q_1 b + r_1 = q_2 b + r_2$,这里 $0 \leqslant r_1, r_2 < b$,则

$$(q_1 - q_2)b = r_1 - r_2.$$

如果 $q_1 \neq q_2$,则 $|r_1 - r_2| \geqslant b$,但由条件 $|r_1 - r_2| < b$,矛盾!故 $q_1 = q_2$,从而 $r_1 = r_2$. 唯一性成立. □

定义 1.2 设 $a, b \in \mathbf{Z}, b \neq 0$,如果 $a = bq + r, 0 \leqslant r < |b|$,则称 q 为 b 除 a 所得的**商**,r 为 b 除 a 所得的**余数**.

显然,$b \mid a$ 当且仅当 b 除 a 所得余数为 0.

习题 1.1

1. 从 176 到 545 的所有整数中,13 的倍数有多少个?

2. 已知 $p \mid (10a - b), p \mid (10c - d)$,证明 $p \mid (ad - bc)$.

3. 已知 n 为自然数,并且 $3 \mid n, 7 \mid n$,证明 $21 \mid n$.

4. 已知 $a, b \in \mathbf{Z}$,并且 $a \mid b, b \mid a$,证明 $a = \pm b$.

5. 证明当 n 为奇数时,$16 \mid (n^4 + 4n^2 + 11)$.

6. 证明:对任意 $x, y \in \mathbf{Z}$,$17 \mid (2x + 3y)$ 当且仅当 $17 \mid (9x + 5y)$.

§1.2 最大公因数与最小公倍数

定义 1.3 设 $d, a_1, a_2, \cdots, a_n \in \mathbf{Z}$,并且 $a_1, a_2, \cdots, a_n$ 不全为 0,如果对每个 a_i,$d \mid a_i$,则称 d 为 $a_1, a_2, \cdots, a_n$ 的一个**公因**

数. $a_1, a_2, \cdots, a_n$ 的所有公因数中最大的正因数称为 $a_1, a_2, \cdots, a_n$ 的**最大公因数**,记作 $(a_1, a_2, \cdots, a_n)$.

对于任意一组不全为零的整数 $a_1, a_2, \cdots, a_n$, 最大公因数 $(a_1, a_2, \cdots, a_n)$ 是否存在? 如果存在,怎样求最大公因数呢?

关于最大公因数的存在性问题,需要用到有关自然数的一个原理——**最大自然数原理**:

设 A 是自然数集 $\boldsymbol{N}$ 的一个非空子集,如果 A 有上界,则 A 中必存在最大自然数.

如果记 $A = \{d \mid d \in \boldsymbol{N}, \text{并且 } d \mid a_i (i = 1, 2, \cdots, n)\}$, 则易知 $1 \in A$, 并且 A 中每个数均小于等于 $\min\{\mid a_i \mid \mid a_i \neq 0, 1 \leqslant i \leqslant n\}$, 从而 A 有上界,由最大自然数原理, A 中存在最大自然数,它就是 $a_1, a_2, \cdots, a_n$ 的最大公因数.

下面考虑最大公因数的求法.

定理 1.2 设 $a, b, c \in \boldsymbol{Z}$,并且 $b \neq 0$, 如果 $a = bq + c$, 则

$$(a, b) = (b, c).$$

证明 设 $(a, b) = d_1, (b, c) = d_2$.

由于 $(a, b) = d_1$, 故 $d_1 \mid a, d_1 \mid b$, 又 $c = a - bq$, 从而 $d_1 \mid c$, 即 d_1 为 b 和 c 的一个公因数,于是 $d_1 \leqslant d_2$. 同样由于 $(b, c) = d_2$, 故 $d_2 \mid b, d_2 \mid c$, 又 $a = bq + c$, 从而 $d_2 \mid a$, 即 d_2 为 a 和 b 的一个公因数,于是 $d_2 \leqslant d_1$, 由此可知, $d_1 = d_2$. □

由定理 1.2 我们可以求两个不全为 0 的整数的最大公因数.

设 $a, b \in \boldsymbol{Z}$, 并且 a, b 不全为 0,不妨设 $b \neq 0$. 由带余除法,必存在自然数 n, 满足:

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

$$
\begin{aligned}
b &= r_1 q_2 + r_2, & 0 < r_2 < |r_1|,\\
&\vdots & \vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < |r_{n-1}|,\\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, & r_{n+1} = 0.
\end{aligned}
$$

从而根据定理 1.2,我们得到:

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

上面求两个整数的最大公因数的方法称为**辗转相除法**,由辗转相除法的推导过程反推回去,我们得到(读者自证):

定理 1.3 设 $a,b \in \boldsymbol{Z}$,a,b 不全为 0,则存在 $m,n \in \boldsymbol{Z}$,使得下式成立

$$(a,b) = ma + nb.$$

一般而言,定理 1.3 中 m,n 不一定唯一,比如:

$$2 = (4,6) = (-1)\times 4 + 1\times 6 = 5\times 4 + (-3)\times 6.$$

由定理 1.3 易知,a 和 b 的任意公因数都是最大公因数的因数. 反过来,最大公因数的每个因数也是 a 和 b 的公因数. 这说明两个不全为零整数的公因数与它们最大公因数的因数是一致的.

例 1.3 设 $a = 288, b = 158$,计算 (a,b),并将 (a,b) 表示为 a 和 b 的组合.

解 利用辗转和除法

$$288 = 158\cdot 1 + 130,\quad 158 = 130\cdot 1 + 28,\quad 130 = 28\cdot 4 + 18,$$

$$28 = 18\cdot 1 + 10,\quad 18 = 10\cdot 1 + 8,\quad 10 = 8\cdot 1 + 2,$$

$$8 = 2\cdot 4 + 0.$$

因此$(288,158) = 2$,并且

$$2 = 10 - 8\cdot 1 = 10 - (18 - 10\cdot 1)\cdot 1$$

$$=2\cdot 10-1\cdot 18=2\cdot(28-18\cdot 1)-1\cdot 18=2\cdot 28-3\cdot 18$$
$$=2\cdot 28-3(130-4\cdot 28)=(-3)\cdot 130+14\cdot 28$$
$$=(-3)130+14(158-130\cdot 1)=(-17)\cdot 130+14\cdot 158$$
$$=(-17)\cdot(288-158\cdot 1)+14\cdot 158$$
$$=(-17)\cdot 288+31\cdot 158,$$

即 $(288,158)=(-17)\cdot 288+31\cdot 158$.

用辗转相除法可以求两个整数的最大公因数,而多个整数的最大公因数的求法可以转化为两个整数的最大公因数的求法,即我们有如下结论:

定理 1.4 设 $a_1,a_2,\cdots,a_n$ 是一组全不为 0 的整数,并且 $(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{n-1},a_n)=d_n$,则 $(a_1,a_2,\cdots,a_n)=d_n$.

证明 由条件 $d_n\mid a_n,d_n\mid d_{n-1}$,但 $d_{n-1}\mid a_{n-1},d_{n-1}\mid d_{n-2}$,故 $d_n\mid a_{n-1},d_n\mid d_{n-2}$.由此类推,最后得到 $d_n\mid a_n,d_n\mid a_{n-1},\cdots,d_n\mid a_1$,即 d_n 为 $a_1,a_2,\cdots,a_n$ 的一个公因数.又设 d 为 $a_1,a_2,\cdots,a_n$ 的任一公因数,则 $d\mid a_1,d\mid a_2$,从而 $d\mid d_2$.又 $d\mid a_3$,故 $d\mid d_3$.由此类推,最后得到 $d\mid d_n$.于是 $d\leqslant d_n$,故 d_n 是 $a_1,a_2,\cdots,a_n$ 的最大公因数. □

对于一组给定的不全为 0 的整数 $a_1,a_2,\cdots,a_n$,在求其最大公因数时,考虑到数 0 是任何非零整数的倍数,不失一般性,我们只需求那些不为 0 的整数的最大公因数,并利用定理 1.4 由辗转相除法求得.

定义 1.4 设 a,b 是两个不为 0 的整数,如果 $(a,b)=1$,则称 a 与 b **互素**.

互素具有下列基本性质：

(1) 设 $a,b \in \mathbf{Z}$，则 $(a,b)=1$ 当且仅当存在 $m,n \in \mathbf{Z}$，使得 $ma+nb=1$；

(2) 如果 $(a,b)=1,(a,c)=1$，则 $(a,bc)=1$；

(3) 如果 $a \mid bc$，并且 $(a,b)=1$，则 $a \mid c$；

(4) 如果 $a \mid c, b \mid c$，并且 $(a,b)=1$，则 $ab \mid c$.

下面只证性质(1)，性质(2)～(4)可由性质(1)推出.

如果 $(a,b)=1$，由定理 1.3 可知存在 $m,n \in \mathbf{Z}$，使得

$$ma+nb=1.$$

反过来，如果 $ma+nb=1$，则对 a 和 b 的任意公因子 d 而言，$d \mid a, d \mid b$，从而 $d \mid 1$，于是 $d \leqslant |d| \leqslant 1$，又 1 显然为 a 和 b 的公因子，从而 $(a,b)=1$.

下面我们来研究整数的公倍数与最小公倍数.

定义 1.5 设 $a_1,a_2,\cdots,a_n,m \in \mathbf{Z}$，如果对每个 a_i，均有 $a_i \mid m$，则称 m 为 $a_1,a_2,\cdots,a_n$ 的**公倍数**，$a_1,a_2,\cdots,a_n$ 的一切公倍数中最小的正整数，叫做 $a_1,a_2,\cdots,a_n$ 的**最小公倍数**，记作 $[a_1,a_2,\cdots,a_n]$.

同最大公因数一样，最小公倍数是否存在？如果存在，怎样求最小公倍数呢？

首先由于任何正整数都不是 0 的倍数，故在讨论最小公倍数时，假定这些整数都不是零. 其次由于最小公倍数只涉及到整数的整除性，而整数的整除性与数的正负号无关. 从而不妨设所有 a_i 为正整数.

关于最小公倍数的存在性问题，需要用到有关自然数的另一

个原理——**最小自然数原理**：

设 A 为自然数集 N 的一个非空子集，则 A 中必存在最小自然数.

如果记 $A=\{m \mid m \in N$，并且 $a_i \mid m(i=1,2,\cdots,n)\}$，则易知 $a_1a_2\cdots a_n \in A$，从而 A 为自然数集 N 的一个非空子集，由最小自然数原理知，A 中必有最小正整数，它就是 $a_1,a_2,\cdots,a_n$ 的最小公倍数.

两个正整数的最小公倍数的求法可通过如下定理给出.

定理 1.5 设 a,b 为两个正整数，则下列结论成立：

(1) a,b 的所有公倍数就是 $[a,b]$ 的所有倍数；

(2) $[a,b]=\dfrac{ab}{(a,b)}$.

证明 设 m 是 a,b 的任一公倍数，不妨设 $m>0$，则存在 k，$k' \in N$，使得 $m=ak=bk'$.

令 $a=a_1(a,b)$，$b=b_1(a,b)$，则 $(a_1,b_1)=1$，并且

$$a_1(a,b)k=b_1(a,b)k',$$

于是 $a_1k=b_1k'$. 又由于 $(a_1,b_1)=1$，故 $b_1 \mid k$，设 $k=b_1t$.

因此 $m=ak=ab_1t=\dfrac{ab}{(a,b)}t$，即 a,b 的公倍数都是 $\dfrac{ab}{(a,b)}$ 的倍数.

另一方面，$\dfrac{ab}{(a,b)}=a\cdot\dfrac{b}{(a,b)}=\dfrac{a}{(a,b)}\cdot b$ 是 a,b 的公倍数，从而是最小公倍数，即(2)成立.

由前面的证明可知(1)亦成立. □

多个整数的最小公倍数，可以通过两个整数的最小公倍数求

得。事实上,我们有:

定理 1.6 设 $a_1,a_2,\cdots,a_n(n\geqslant 2)$ 为正整数,并且$[a_1,a_2]=m_2,[m_2,a_3]=m_3,\cdots,[m_{n-1},a_n]=m_n$,则

$$[a_1,a_2,\cdots,a_n]=m_n.$$

证明 由定理1.5,$m_i\mid m_{i+1},(2\leqslant i\leqslant n-1)$,并且 $a_1\mid m_2$,$a_i\mid m_i(2\leqslant i\leqslant n)$,故 m_n 是$a_1,a_2,\cdots,a_n$的一个公倍数.又设 m 为 $a_1,a_2,\cdots,a_n$ 的任意公倍数,则 $a_1\mid m,a_2\mid m$,于是 $m_2\mid m$.又 $a_3\mid m$,故 $m_3\mid m$,依此类推,最后得 $m_n\mid m$,于是 $m_n\leqslant|m|$.从而

$$m_n=[a_1,a_2,\cdots,a_n].$$ □

例 1.4 求同时满足 $(a,b)=10,[a,b]=100$ 的全部正整数 a,b.

解 由于 $(a,b)=10$,则$\left(\frac{a}{10},\frac{b}{10}\right)=1$.

又 $[a,b]=100$,则$\left[\frac{a}{10},\frac{b}{10}\right]=10$.

令 $x=\frac{a}{10},y=\frac{b}{10}$,则满足$(x,y)=1$并且$[x,y]=10$的 x 和 y 的值为:

x	1	10	2	5
y	10	1	5	2

于是相应 a 和b 的取值为

a	10	100	20	50
b	100	10	50	20

习题 1.2

1. 求下列数组的最大公因数与最小公倍数.

1) $a = 72, b = -60$;

2) $a = -120, b = 28$;

3) $a = 168, b = -180, c = 495$.

2. 设 $a = 158, b = 342$,计算(a,b),并将(a,b)表示为 a 和 b 的组合.

3. 设 a,b 为正整数,如果$[a,b] = (a,b)$,证明 $a = b$.

4. 证明对任意正整数 n,$(21n + 4, 14n + 3) = 1$.

5. 设$(a,b) = 1$,证明$(a + b, a^2 + ab + b^2) = 1$.

6. 求满足$(a,b,c) = 10, [a,b,c] = 100$ 的全部正整数 a, b, c

7. 设 a,b,c 都是非零整数,并且$(a,b) = 1, (a,c) = 1$,证明 $(a, bc) = 1$.

8. 给定 x 和 y,如果 $m = ax + by, n = cx + dy$,这里 $ad - bc = \pm 1$.证明:$(m,n) = (x,y)$.

§1.3 算术基本定理

在正整数中,1 的正因数只有它本身,任何大于 1 的整数都至少有两个正因数,即 1 和它本身.