21世纪大学数学精品教材

应用数学基础

吴晓平　秦艳琳　编著

科学出版社
www.sciencep.com

·21世纪大学数学精品教材·

应用数学基础

吴晓平　秦艳琳　编著

科学出版社

北京

内 容 简 介

本书包含初等数论、近世代数、椭圆曲线论、图论、计算复杂性与数理逻辑等方面的内容．结构合理，内容系统全面．书中以大量例题深入浅出地阐述各数学分支的基本概念、基本理论与基本方法．注重背景，强调应用，便于读者理解掌握．

本书可作为信息安全、计算机、通信、电子等领域的研究生和大学生相关课程的教科书，也可作为这些领域工程技术人员的参考书．

图书在版编目（CIP）数据

应用数学基础/吴晓平，秦艳琳编著．—北京：科学出版社，2008
21 世纪大学数学精品教材
ISBN 978-7-03-022778-2

Ⅰ．应… Ⅱ．①吴…②秦… Ⅲ．应用数学－高等学校－教材 Ⅳ．O29

中国版本图书馆 CIP 数据核字（2008）第 123944 号

责任编辑：张颖兵／责任校对：梅 莹
责任印制：董艳辉／封面设计：苏 波

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
京山德兴印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2008 年 8 月第 一 版 开本：B5（720×1000）
2008 年 8 月第一次印刷 印张：14 1/4
印数：1—3 000 字数：277 000
定价：23.80 元
（如有印装质量问题，我社负责调换）

前　言

21世纪是信息的时代，人类长期积累起来的知识体系正面临着第三次数学化. 数学思想、数学方法与数学模型随着计算机科学技术的飞速发展，日益渗透到各种行业中去. 除了古典的数学理论，如初等数学、微积分学、概率论等，早已得到广泛应用外，一些比较抽象的现代数学理论，如抽象代数、图论、数理逻辑、运筹学等，也逐渐成为社会生产、科学实验、工程技术及经济管理中不可缺少的工具，应用数学的适用范围正在迅速扩大. 特别是在信息安全、计算机科学、电子、通信等专业的学习和研究中，涉及数论、抽象代数、椭圆曲线论、图论、计算复杂度理论及数理逻辑等应用数学知识，而完整、系统介绍这些应用数学知识的教材较少. 非数学专业的学生在本专业的学习中用到上述的应用数学知识时，不得不花费大量时间和精力去查阅相关的数学专著，而一般的数学专业书籍内容繁多、抽象难懂，非数学专业的学生学起来普遍感到比较吃力. 因此，本书将应用于信息安全、计算机、电子、通信等专业的数学基础知识作了系统全面的介绍，使非数学专业的学生和相关领域的工程技术人员在工作学习中遇到相关的数学基础知识时，可以拥有一本便捷的工具书，在短时间内了解或掌握需要的数学理论.

本书第1～5章介绍了数论中的整数唯一性分解定理、同余式、二次剩余、原根、素性检验等内容，第6～8章介绍了抽象代数中的群、环、域、模与格的基础知识，第9章简单介绍了椭圆曲线理论，第10章介绍了图论的基础知识及应用，第11章和第12章分别介绍了计算复杂性和数理逻辑的基础知识. 由于篇幅所限，本书在编写过程中有选择性地略去了部分定理较为繁杂的证明过程，学有余力的读者可以查阅列于书末的参考文献或其他相关书籍.

本书选材突出数学理论的应用，表述严谨，例题丰富，以通俗易懂的方式着重介绍在现代科学技术等实际领域中应用广泛的数学理论和方法. 本书可作为信息安全、计算机、通信、电子等领域的大学生和研究生相关课程的教科书，也可作为这些领域工程技术人员的参考书.

感谢李卫军老师对本书编写提出的宝贵意见.由于作者水平有限，书中难免会有不妥和疏漏之处，恳请读者批评指正，以使本书能够进一步修改完善.

作　者

2008年4月

目　录

第 1 章　整数的唯一性分解定理

1.1　整除的概念与欧几里得除法

整数的唯一性分解定理，又叫算术基本定理，它是初等数论中最基本的定理之一. 本章将给出这个定理的证明，并介绍与此有关的初等数论中最基本的概念和性质. 在这节里，我们考虑关于整数的一些基本概念和性质——整除和欧几里得除法.

定义 1.1　设 a,b 是任意两个整数，其中 $b\neq 0$. 如果存在一个整数 q 使得等式

$$a=bq \tag{1.1}$$

成立，就称 b 整除 a 或者 a 被 b 整除，记做 $b\mid a$，并把 b 叫做 a 的因数，把 a 叫做 b 的倍数，这时，q 也是 a 的因数，我们常常将 q 写成 a/b 或 $\frac{a}{b}$. 否则，就称 b 不能整除 a 或者 a 不能被 b 整除，记做 $b\nmid a$.

注　(1) 当 b 遍历整数 a 的所有因数时，$-b$ 也遍历整数 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时，a/b 也遍历整数 a 的所有因数.

例 1.1　$30=2\times 15=3\times 10=5\times 6$.

我们有 2,3,5 分别整除 30 或 30 被 2,3,5 分别整除，记做 $2\mid 30,3\mid 30,5\mid 30$. 这时，2,3,5 都是 30 的因数，30 是 2,3,5 的倍数.

30 的所有因数是 $\{\pm 1,\pm 2,\pm 3,\pm 5,\pm 6,\pm 10,\pm 15,\pm 30\}$，或是 $\{\mp 1,\mp 2,\mp 3,\mp 5,\mp 6,\mp 10,\mp 15,\mp 30\}$，或是 $\{\pm 30=30/\pm 1,\pm 15=30/\pm 2,\pm 10=30/\pm 3,\pm 6=30/\pm 5,\pm 5=30/\pm 6,\pm 3=30/\pm 10,\pm 2=30/\pm 15,\pm 1=30/\pm 30\}$.

又例如：$7\mid 84,-7\mid 84,5\mid 20,19\mid 171,3\nmid 8,5\nmid 12,13\mid 0,11\mid 11$.

0 是任何非零整数的倍数，1 是任何整数的因数，任何非零整数 a 是其自身的倍数，也是其自身的因数.

例 1.2　设 a,b 为整数，若 $b\mid a$，则 $b\mid(-a),(-b)\mid a,(-b)\mid(-a)$.

证　设 $b\mid a$，则存在整数 q 使得 $a=bq$，因而，

$$(-a)=b(-q)\qquad a=(-b)(-q)\qquad (-a)=(-b)q$$

因为 $-q,q$ 都是整数，所以根据整除的定义有

$$b\mid(-a)\qquad (-b)\mid a\qquad (-b)\mid(-a)$$

由整除的定义出发，下面一些性质是明显的.

设 a,b,c 是整数，

(1) 如果 $b\mid a,c\mid b$，则 $c\mid a$；

(2) 如果 $b|a$,则 $cb|ca$;

(3) 如果 $c|a,c|b$,则对任意的整数 m,n,有 $c|ma+nb$;

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

(5) 如果 $cb|ca$,则 $b|a$;

(6) 如果 $b|a,a\neq 0$,则 $\frac{a}{b}\Big|a$;

(7) $a|b,b|a$,则 $a=\pm b$.

因为不是任意两个整数之间都有整除关系,所以我们引进欧几里得(Euclid)除法或带余数除法.

定理 1.1(欧几里得除法) 设 a,b 是两个整数,其中 $b>0$,则存在唯一的整数 q,r 使得

$$a=bq+r \quad (0\leqslant r<b) \tag{1.2}$$

证明 (存在性)考虑一个整数序列

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

它们将实数轴分成长度为 b 的左闭右开的一些区间,而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得

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

令 $r=a-bq$,则有

$$a=bq+r \quad (0\leqslant r<b)$$

(唯一性)如果分别有整数 q,r 和 q_1,r_1 满足式(1.2),则

$$a=bq+r \quad (0\leqslant r<b)$$

$$a=bq_1+r_1 \quad (0\leqslant r_1<b)$$

两式相减,得

$$b(q-q_1)=-(r-r_1)$$

当 $q\neq q_1$ 时,左边的绝对值大于等于 b,而右边的绝对值小于 b,这是不可能的,故 $q=q_1,r=r_1$.

定义 1.2 式(1.2)中的 q 叫做 a 被 b 除所得的不完全商,r 叫做 a 被 b 除所得的余数.

推论 1.1 在定理 1.1 的条件下,$b|a$ 的充要条件是 a 被 b 除所得的余数 $r=0$.

注 在式(1.2)中,$0\leqslant r<b$ 可改写为 $0\leqslant r\leqslant b-1,r=0$,则

$$a=bq=b(q-1)+b$$

令 $r=b$,则有

$$a=b(q-1)+r \quad (r=b)$$

若 $1\leqslant r\leqslant b-1,a=bq+r,1\leqslant r\leqslant b-1$,因此,式(1.2)又可改写为

$$a=bq+r \quad (1\leqslant r\leqslant b) \tag{1.3}$$

称式(1.3)中的 r 为最小正余数.

为了更好地描述不完全商和余数,以及今后表述一些数学概念和问题,我们引进一个数学符号.

定义 1.3　设 x 是一个实数,我们称 x 的整数部分为小于或等于 x 的最大整数,记成 $[x]$,则有

$$[x]\leqslant x<[x]+1$$

注　定理 1.1 中的不完全商 q 可写为 $q=\left[\frac{a}{b}\right]$,余数 r 可写为 $r=a-b\left[\frac{a}{b}\right]$.

例 1.3　$[3.14]=3,[-3.14]=-4,[3]=3,[-3]=-3$.

例 1.4　设 $b=15$,当 $a=255$ 时,

$$a=17b+0\quad\left(q=\left[\frac{255}{15}\right]=17,r=0<15\right)$$

当 $a=417$ 时,

$$a=27b+12\quad\left(q=\left[\frac{417}{15}\right]=27,0<r=12<15\right)$$

1.2　最大公因数与辗转相除法

利用上节的定理 1.1,我们来研究整数的最大公因数的存在问题和实际求法.

定义 1.4　设 $a_1,\cdots,a_n$ 是 $n(n\geqslant 2)$ 个整数,若整数 d 是它们中每一个数的因数,那么 d 就叫做 $a_1,\cdots,a_n$ 的一个公因数.

d 是 $a_1,\cdots,a_n$ 的一个公因数的数学表达式为

$$d\mid a_1,\cdots,d\mid a_n$$

如果整数 $a_1,\cdots,a_n$ 不全为零,那么整数 $a_1,\cdots,a_n$ 的所有公因数中最大的一个公因数叫做最大公因数,记做 $(a_1,\cdots,a_n)$,特别地,当 $(a_1,\cdots,a_n)=1$ 时,我们称 $a_1,\cdots,a_n$ 互素或互质.

实际上,$d>0$ 是 $a_1,\cdots,a_n$ 的最大公因数的数学表达式可叙述为

(1) $d\mid a_1,\cdots,d\mid a_n$;

(2) 若 $e\mid a_1,\cdots,e\mid a_n$,则 $e\mid d$.

对于该数学定义我们将在定理 1.7 中给予说明.

例 1.5　两个整数 14 和 21 的公因数为 $\{\pm 1,\pm 7\}$,它们的最大公因数 $(14,21)=7$.

例 1.6　三个整数 14,−15 和 21 的公因数为 $\{\pm 1\}$,它们的最大公因数 $(14,-15,21)=1$,或者说,三个整数 14,−15 和 21 是互素的.

例 1.7　设 p 是一个素数(即 p 是只有 1 与 p 两个正因数的大于 1 的整数),a 为整数,如果 $p\nmid a$,则 p 与 a 互素.

证 设$(p,a)=d$,则有$d|p$及$d|a$.

因为p是素数,所以由$d|p$,我们有$d=1$或$d=p$.

对于$d=p$,由$d|a$,我们有$p|a$,这与假设$p\nmid a$矛盾.

因此,$d=1$,即$(p,a)=1$,结论成立.

定理 1.2 设$a_1,\cdots,a_n$是$n(n\geqslant 2)$个不全为零的整数,则

(1) $a_1,\cdots,a_n$与$|a_1|,\cdots,|a_n|$的公因数相同;

(2) $(a_1,\cdots,a_n)=(|a_1|,\cdots,|a_n|)$.

证明 (1) 设$d|a_i(1\leqslant i\leqslant n)$,由例 1.2,我们有$d\|a_i|$ $(1\leqslant i\leqslant n)$. 故$a_1,\cdots,a_n$的公因数也是$|a_1|,\cdots,|a_n|$的公因数.

反之,设$d\|a_i|$ $(1\leqslant i\leqslant n)$,同样有$d|a_i(1\leqslant i\leqslant n)$. 故$|a_1|,\cdots,|a_n|$的公因数也是$a_1,\cdots,a_n$的公因数.

(2) 由(1)立得(2).

例 1.8 设b是任一非零整数,则$(0,b)=|b|$.

证 因为任何非零整数都是 0 的因数,而整数b的最大因数为$|b|$,所以

$$(0,b)=|b|$$

定理 1.3 设a,b,c是三个不全为零的整数,如果$a=bq+c$,其中q是整数,则$(a,b)=(b,c)$.

证明 因为$(a,b)|a,(a,b)|b$,所以有$(a,b)|c$,因而$(a,b)\leqslant(b,c)$,同理可证$(b,c)\leqslant(a,b)$,于是得到$(a,b)=(b,c)$.

例 1.9 因为$1859=1\times 1573+286$,所以我们有

$$(1859,1573)=(1573,286)$$

怎样才能具体计算出两个整数a,b的最大公因数?直接应用最大公因数的定义,就需要知道整数的因数分解式,这在a,b不是很大数时是可行的,见定理1.20;但当a,b是很大数时,整数分解本身就是很困难的事,又由于

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

且一组不全为零的整数的最大公因数,等于它们当中全体不为零的整数的最大公因数,所以,不防设$a_i>0$ $(i=1,\cdots,n)$. 我们先讨论两个正整数的最大公因数的求法,即辗转相除法,并借此推出最大公因数的若干性质.

辗转相除法:设a,b是任意两个正整数,记$r_0=a,r_1=b$,反复运用欧几里得除法,我们有

$$\begin{aligned}
r_0&=r_1q_1 &&+r_2 && (0\leqslant r_2<r_1)\\
r_1&=r_2q_2 &&+r_3 && (0\leqslant r_3<r_2)\\
&\cdots\cdots && && \qquad (1.4)\\
r_{n-2}&=r_{n-1}q_{n-1} &&+r_n && (0\leqslant r_n<r_{n-1})\\
r_{n-1}&=r_nq_n &&+r_{n-1} && (r_{n-1}=0)
\end{aligned}$$

经过有限步骤,必然存在n使得$r_n+1=0$,这是因为

$$0=r_n+1<r_n<r_{n-1}<\cdots<r_2<r_1=b$$

且 b 是有限正整数.

定理 1.4　设 a,b 是任意两个正整数,则 $(a,b)=r_n$,其中 r_n 是式(1.4)中最后一个非零余数.

证明　根据定理 1.3,有

$$\begin{aligned}(a,b)&=(b,r_2)\\&=(r_2,r_3)\\&\cdots\cdots\\&=(r_{n-1},r_n)\\&=(r_n,0)\end{aligned}$$

再根据例 1.8,有

$$(a,b)=(r_n,0)=r_n$$

因此,定理 1.4 成立.

因为求两个整数的最大公因数在信息安全的实践中起着重要的作用,所以我们将求两个整数的最大公因数之过程详述如下.

首先,根据定理 1.2,将求两个整数的最大公因数转化为求两个非负整数的最大公因数;其次,运用欧几里得除法,并根据定理 1.3,可将求两个正整数的最大公因数转化为求两个较小正整数的最大公因数. 反复运用辗转相除法,来求两个正整数的最大公因数转化为求 0 和一个正整数的最大公因数.

例 1.10　设 $a=-1859,b=1573$,计算 (a,b).

解　由定理 1.2,$(-1859,1573)=(1859,1573)$.

运用辗转相除法,有

$$\begin{aligned}1859&=1\times1573+286\\1573&=5\times286+143\\286&=2\times143\end{aligned}$$

根据定理 1.4,有

$$(-1859,1573)=143$$

例 1.11　设 $a=46480,b=39423$,计算 (a,b).

解　利用辗转相除法

$$\begin{aligned}46480&=1\times39423+7057\\39423&=5\times7057+4138\\7057&=1\times4138+2919\\4138&=1\times2919+1219\\2919&=2\times1219+481\\1219&=2\times481+257\end{aligned}$$

$$
\begin{aligned}
481 &= 1\times 257 + 224\\
257 &= 1\times 224 + 33\\
224 &= 6\times 33 + 26\\
33 &= 1\times 26 + 7\\
26 &= 3\times 7 + 5\\
7 &= 1\times 5 + 2\\
5 &= 2\times 2 + 1\\
2 &= 2\times 1
\end{aligned}
$$

对于式(1.2)中的余数，如果不要求它是正的，那么，对于整数 a 和 $b>0$，则存在整数 s,t，使 $a=bt+s$ 成立，其中 $|s|\leqslant\frac{b}{2}$，这是因为，当式(1.2)中的 $r<\frac{b}{2}$ 时，取 $s=r$；当 $r>\frac{b}{2}$ 时，取 $s=r-b$；当 b 是偶数且 $r=\frac{b}{2}$ 时，则 s 可取 $\frac{b}{2}$ 和 $-\frac{b}{2}$ 两个数中的任意一个，数 s 叫做 a 被 b 除所得到的绝对最小剩余. 如果我们在式(1.4)的计算过程中，都取绝对最小剩余，并设最后一个不为零的余数为 s_m，则由定理 1.3，仍然有 $|s_m|=(a,b)$，仍用前例说明

$$
\begin{aligned}
46480 &= 1\times 39423 + 7057\\
39423 &= 6\times 7057 - 2919\\
7057 &= 2\times 2919 + 1219\\
2919 &= 2\times 1219 + 481\\
1219 &= 3\times 481 - 224\\
481 &= 2\times 224 + 33\\
224 &= 7\times 33 - 7\\
33 &= 5\times 7 - 2\\
7 &= 3\times 2 + 1\\
2 &= 2\times 1
\end{aligned}
$$

所以，$(46480,39423)=1$. 与一般的辗转相除法相比，计算步骤由 14 次减少为 10 次，大大减少了计算量.

从辗转相除法的演示中，我们观察到

$$
\begin{aligned}
(a,b) = r_n &= r_{n-2} - r_{n-1}q_{n-1}\\
r_{n-1} &= r_{n-3} - r_{n-2}q_{n-3}\\
&\cdots\cdots\\
r_3 &= r_1 - r_2q_2\\
r_2 &= r_0 - r_1q_1
\end{aligned}
$$

这样，逐次消去 $r_{n-1},r_{n-2},\cdots,r_3,r_2$，我们可找到整数 s,t 使得

$$sa+tb=(a,b)$$

例 1.12　设 $a=-1859, b=1573$，求整数 s,t，使得

$$sa+tb=(a,b)$$

解　由例 1.10，我们有

$$\begin{aligned}143 &= 1573-5\times 286\\ &= 1573-5\times(1859-1\times 1573)\\ &= 5\times(-1859)+6\times 1573\end{aligned}$$

因此，整数 $s=5, t=6$ 满足 $sa+tb=(a,b)$.

例 1.13　设 $a=46480, b=39423$，求整数 s,t，使得 $sa+tb=(a,b)$.

解　由例 1.11 有

方法一：最小非负余数.

$$\begin{aligned}1 &= 5-2\times 2\\ &= 5-2\times(7-1\times 5)\\ &= (-2)\times 7+3\times(26-3\times 7)\\ &= 3\times 26+(-11)\times(33-1\times 26)\\ &= (-11)\times 33+14\times(224-6\times 33)\\ &= 14\times 224+(-95)\times(257-1\times 224)\\ &= (-95)\times 257+109\times(481-1\times 257)\\ &= 109\times 481+(-204)\times(1219-2\times 481)\\ &= (-204)\times 7+517\times(2919-2\times 1219)\\ &= 517\times 2919+(-1238)\times(4138-1\times 2919)\\ &= (-1238)\times 4138+1755\times(7057-1\times 4138)\\ &= 1755\times 7057+(-2993)\times(39423-5\times 7057)\\ &= (-2993)\times 39423+16720\times(46480-1\times 39423)\\ &= 16720\times 46480+(-19713)\times 39423\\ &= (16720-39423)\times 46480+(46480-19713)\times 39423\\ &= (-22703)\times 46480+26767\times 39423\end{aligned}$$

方法二：绝对值最小余数.

$$\begin{aligned}1 &= 7-3\times 2\\ &= 7-3\times(-33+5\times 7)\\ &= 3\times 33+(-14)\times(-224+7\times 33)\\ &= 14\times 224+(-95)\times(481-2\times 224)\\ &= (-95)\times 481+204\times(-1219+3\times 481)\\ &= (-204)\times 1219+517\times(2919-2\times 1219)\\ &= 517\times 2919+(-1238)\times(7057-2\times 2919)\\ &= (-1238)\times 7057+2993\times(-39423+6\times 7057)\end{aligned}$$

$$=(-2993)\times 39423+16720\times(46480-1\times 39423)$$
$$=16720\times 46480+(-19713)\times 39423$$
$$=(16720-39423)\times 46480+(46480-19713)\times 39423$$
$$=(-22703)\times 46480+26767\times 39423$$

因此，整数 $s=-22703$，$t=26767$ 满足 $sa+tb=(a,b)$.

由式(1.4)我们还可以猜想有以下定理成立.

定理 1.5 设 a,b 是任意两个正整数，则

$$s_k a-t_k b=(-1)^{k-1}r_k \quad (k=1,\cdots,n) \tag{1.5}$$

其中，

$$\begin{cases} t_0=1, t_1=q_1, t_k=q_k t_{k-1}+t_{k-2} \\ s_0=0, s_1=1, \ s_k=q_k s_{k-1}+s_{k-2} \end{cases} \quad (k=2,\cdots,n) \tag{1.6}$$

证明 当 $k=1$ 时，式(1.5)显然成立. 当 $k=2$ 时，

$$r_2=-[aq_2-b(1+q_1q_2)]$$

但 $1+q_1q_2=q_2t_1+t_0$，则 $q_2=q_2\times 1+0=q_2s_1+s_0$. 故

$$s_2a-t_2b=(-1)^{2-1}r_2$$
$$t_2=q_2t_1+t_0$$
$$s_2=q_2s_1+s_0$$

假定式(1.5)，(1.6)对于不超过 $k\geqslant 2$ 的正整数都成立

$$(-1)^k r_{k+1}=(-1)^k(r_{k-1}-q_{k+1}r_k)$$
$$=(s_{k-1}a-t_{k-1}b)+q_{k+1}(s_ka-t_kb)$$
$$=(q_{k+1}s_k+s_{k-1})a-(q_{k+1}t_k+t_{k-1})b$$

故

$$s_{k+1}a-t_{k+1}b=(-1)^k r_{k+1}$$

其中，$t_{k+1}=q_{k+1}t_k+t_{k-1}$，$s_{k+1}=q_{k+1}s_k+s_{k-1}$.

由归纳法，定理 1.5 为真.

由该定理我们可以得到：

推论 1.2 若 a,b 是任意两个不全为零的整数，则存在两个整数 s,t 使得

$$sa+tb=(a,b)$$

该推论证实了逐次消去法求得 s,t 的可行性.

定理 1.6 整数 a,b 互素的充分必要条件是存在整数 s,t 使得 $sa+tb=1$.

证明 由推论 1.2 我们立即得到命题的必要性.

反过来，设 $d=(a,b)$，则有 $d\mid a, d\mid b$. 现在若存在整数 s,t 使得

$$sa+tb=1$$

则有

$$d\mid sa+tb=1$$

因此，$d=1$，即整数 a,b 互素.

例 1.14　设 4 个整数 a,b,c,d 满足关系式

$$ad-bc=1$$

则 $(a,b)=1,(a,c)=1,(d,b)=1,(d,c)=1$.

下面，再说明最大公因数的数学定义.

定理 1.7　设 a,b 是任意两个不全为零的整数，d 是正整数，则 d 是整数 a,b 的最大公因数的充要条件是

(1) $d|a,d|b$；

(2) 若 $e|a,e|b$，则 $e|d$.

证明　若 d 是整数 a,b 的最大公因数，则显然有(1)成立；

再由推论 1.2 存在整数 s,t 使得

$$sa+tb=d$$

因此，当 $e|a,e|b$ 时，有

$$e|sa+tb=d$$

故(2)成立.

反过来，假设(1)和(2)成立，那么

(1) 说明 d 是整数 a,b 的公因数；

(2) 说明 d 是整数 a,b 的公因数中的最大数，因为 $e|d$ 时，有 $|e|\leqslant d$.

因此，d 是整数 a,b 的最大公因数.

下面的定理给出了最大公因数的一些其他性质.

定理 1.8　设 a,b 是任意两个不全为零的整数，

(1) 若 m 是任一正整数，则 $(am,bm)=(a,b)m$.

(2) 若非零整数 d 满足 $d|a,d|b$，则 $\left(\dfrac{a}{d},\dfrac{b}{d}\right)=\dfrac{(a,b)}{|d|}$. 特别地，

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$$

证明　设 $d=(a,b),d'=(am,bm)$. 由推论(1.2)知，存在整数 s,t 使得

$$sa+tb=d$$

两端同乘 m，得到

$$s(am)+t(bm)=dm$$

因此 $d'|dm$. 又显然有 $dm|am,dm|bm$. 根据定理 1.7(2)，有 $dm|d'$. 故 $d'=(am,bm)$，即(1)成立.

再根据(1)，当 $d|a,d|b$ 时，有

$$(a,b)=\left(\frac{a}{|d|}\times|d|,\frac{b}{|d|}\times|d|\right)$$

$$=\left(\frac{a}{|d|},\frac{b}{|d|}\right)|d|$$

$$=\left(\frac{a}{d},\frac{b}{d}\right)|d|$$

因此，$\left(\frac{a}{d},\frac{b}{d}\right)=\frac{(a,b)}{|d|}$，特别地，取 $d=(a,b)$，有

$$\left(\frac{a}{(a,b)},\frac{b}{(b,a)}\right)=1$$

故(2)成立.

例 1.15 设 $a=11\times200306$，$b=23\times200306$，计算(a,b).

解 因为

$$(11,23)=(11,23-11\times2)=(11,1)=1$$

所以

$$(a,b)=(11\times200306,23\times200306)=200306$$

前面讨论了如何具体求两个整数的最大公因数. 对于 n 个整数 $a_1,\cdots,a_n$ 的最大公因数，我们可以用递归的方法，将求它们的最大公因数转化为一系列求两个整数的最大公因数，具体过程如下：

定理 1.9 设 $a_1,\cdots,a_n$ 是 n 个整数，且 $a_1\neq0$，令$(a_1,a_2)=d_2,\cdots,(d_{n-1},a_n)=d_n$，则

$$(a_1,\cdots,a_n)=d_n$$

证明 由 $d_n|a_n,d_n|d_{n-1},d_{n-1}|a_{n-1},d_{n-1}|d_{n-2}$，可得 $d_n|a_{n-1},d_n|d_{n-2}$.

由此类推，最后得到

$$d_n|a_n,d_n|a_{n-1},\cdots,d_n|a_1$$

因此有 $d_n\leqslant(a_1,\cdots,a_n)$，另一方面，设$(a_1,\cdots,a_n)=d$，由 $d|d_2,d|d_3,\cdots,d|d_n$ 得

$$d\leqslant d_n$$

于是可得

$$(a_1,\cdots,a_n)=d_n$$

由定理 1.9 可推出，存在整数$(x_1,\cdots,x_n)$使得

$$(a_1,\cdots,a_n)=a_1x_1+\cdots+a_nx_n$$

例 1.16 计算最大公因数(120,150,210,35).

解 因为

$$(120,150)=(120,30)=30$$

$$(30,210)=30$$

$$(30,35)=(30,5)=5$$

所以最大公因数(120,150,210,35)=5.