普通高等院校规划教材

初等数论

CHU DENG SHU LUN

张文鹏　主编

陕西师范大学出版社

普通高等院校规划教材

初等数论

主编 张文鹏

编者 李海龙　郭金保　刘国栋　易　媛
陈宝安　乔希民　张天平　张小蹦
王　阳

陕西师范大学出版社

图书代号:JC7N0062

图书在版编目(CIP)数据

初等数论/张文鹏主编. —西安:陕西师范大学出版社,2007.4
ISBN 978-7-5613-3764-6

Ⅰ. 初… Ⅱ. 张… Ⅲ. 数论-高等学校-教材 Ⅳ. 0156

中国版本图书馆 CIP 数据核字(2007)第 019978 号

初等数论

张文鹏 主编

责任编辑 梁潇蕾
责任校对 刘锋利
视觉设计 吉人设计
出版发行 陕西师范大学出版社
社　　址 西安市陕西师大 120 信箱(邮政编码:710062)
网　　址 http://www.snuph.com
经　　销 新华书店
印　　刷 陕西师范大学印刷厂
开　　本 787mm×960mm 1/16
印　　张 15.25
字　　数 239 千
版　　次 2007 年 6 月第 1 版
印　　次 2007 年 6 月第 1 次
书　　号 ISBN 978-7-5613-3764-6
定　　价 22.00 元

读者购书、书店添货或发现印刷装订问题,请与本社教材中心联系、调换。
电　话:(029)85307826　85303622(传真)
E-mail:jcc@snnup.net

前　言

数论，这门古老而又常新的学科既是典型的纯粹数学，又是日益得到广泛应用的新“应用数学”.

在数论中，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.

本书共八章内容. 全面介绍了初等数论中整数的整除性理论、不定方程、同余理论、二次剩余和二次反转定理、原根、数论函数及其均值、哥德巴赫猜想等基本内容. 最后一章中，结合各章内容精选了一些专题进行探讨，并提出了初等数论中有待解决的一些问题. 这样的内容设计和编排顺序，为读者提供了宽松的选择余地和创新探究的平台.

每章附有“习题”和富有启发的“问题与探究”，书后给出了较为详尽的参考答案与提示.

在编写过程中，征求了许多兄弟院校从事初等数论教学和研究的一线教师的意见和建议，吸收了许多兄弟院校的有关成果和经验，借此表示衷心的感谢.

编　者

2007 年 5 月

目　录

第一章　算术基本定理

整除性理论是数论中最重要的基本内容．本章首先简要介绍最小数原理与数学归纳法，着重讨论整除的概念与带余除法定理，并以此为工具，探讨最大公约数与最小公倍数的性质，进一步研究素数的基本性质和算术基本定理，最后探讨了高斯函数在数论中的应用．

§1－1　数、数列、和

一、数

数是最基本的数学概念之一，通常包括自然数、整数、有理数、实数、复数以及在它们的基础上形成的其他概念，例如代数数、超越数等等．我们用 $\mathbf{Z}$ 表示整数集$\{\cdots,-2,-1,0,1,2,\cdots\}$，用 $\mathbf{Z}^+$ 表示正整数集$\{1,2,3,\cdots\}$，用 $\mathbf{N}$ 表示自然数集$\{0,1,2,3,\cdots\}$，用 $\mathbf{Q},\mathbf{R},\mathbf{C}$ 分别表示有理数集、实数集和复数集．

二、数列

数列是一组按一定顺序排列的数，记为$\{a_n\}$ $(n\geqslant 1)$，即 $a_1,a_2,a_3,\cdots$．我们称 a_1 为数列的“第一项”，称 a_2 为数列的“第二项”等等．数列中数的总数为数列的“项数”，项数有限的数列称为“有限数列”，项数无限的数列称为“无限数列”．数列可以看成是一种定义在正整数集或其子集上的函数．

数列 $a_1,a_2,a_3,\cdots$ 是等差数列，如果存在常数 d，满足

$$a_2-a_1=a_3-a_2=\cdots=d,$$

则数 d 称为公差，数列的第 n 项为

$$a_n=a_1+(n-1)d.$$

数列 $a_1,a_2,a_3,\cdots$ 是等比数列，如果存在常数 q，使得对 $k=1,2,3,\cdots$ 有

$$a_{k+1}=qa_k,$$

则数 q 称为公比,数列的第 n 项为

$$a_n=a_1q^{n-1}.$$

数列 $F_1,F_2,F_3,\cdots$ 定义为 $F_1=1,F_2=1,\cdots,F_n=F_{n-1}+F_{n-2}(n\geqslant 3)$,此数列称为 Fibonacci 数列. 数列 $L_1,L_2,L_3,\cdots$ 定义为 $L_1=1,L_2=3,\cdots,L_n=L_{n-1}+L_{n-2}(n\geqslant 3)$,此数列称为 Lucas 数列.

三、和

定义 1-1 设 m,n 是整数,且 $m\leqslant n$,我们定义和式 $\sum_{k=m}^{n}a_k$ 为

$$\sum_{k=m}^{n}a_k=a_m+a_{m+1}+\cdots+a_n.$$

例题 1-1
$$\sum_{k=1}^{6}k=1+2+3+4+5+6=21.$$

$$\sum_{k=2}^{6}k^2=4+9+16+25+36=90.$$

$$\sum_{k=-2}^{6}k^2=4+1+0+1+4+9+16+25+36=96.$$

由和式的定义,我们容易得到如下性质(读者自己证明):

性质 1-1 $\sum_{k=m}^{n}ca_k=c\sum_{k=m}^{n}a_k.$

性质 1-2 $\sum_{k=m}^{n}(a_k+b_k)=\sum_{k=m}^{n}a_k+\sum_{k=m}^{n}b_k.$

性质 1-3 $\sum_{i=m}^{n}\sum_{j=k}^{p}a_ib_j=\left(\sum_{i=m}^{n}a_i\right)\left(\sum_{j=k}^{p}b_j\right).$

性质 1-4 $\sum_{k=m}^{n}\sum_{i=m}^{k}a_{ki}=\sum_{i=m}^{n}\sum_{k=i}^{n}a_{ki}.$

定义 1-2 设 $x>0$ 是实数,我们定义和式 $\sum_{n\leqslant x}a_n$ 为

$$\sum_{n\leqslant x}a_n=a_1+a_2+\cdots+a_{[x]},$$

这里 $[x]$ 表示不大于 x 的最大整数.

例题 1-2 $\sum_{n\leqslant 7.5}\log n=\log 1+\log 2+\log 3+\log 4+\log 5+\log 6+\log 7.$

定义 1-3 设 m,n 是整数,且 $m\leqslant n$,我们定义求积式 $\prod_{k=m}^{n}a_k$ 为

$$\prod_{k=m}^{n} a_k = a_m a_{m+1} \cdots a_n.$$

由求积式的定义,我们容易得到如下性质(读者自己证明):

性质 1-5　$\prod_{k=m}^{n} ca_k = c^{n-m+1} \prod_{k=m}^{n} a_k.$

性质 1-6　$\prod_{k=m}^{n} ka_k = m(m+1) \cdot \cdots \cdot n \prod_{k=m}^{n} a_k.$

性质 1-7　$\prod_{k=m}^{n} a_k^s = \left(\prod_{k=m}^{n} a_k \right)^s.$

定义 1-4　设 n 是正整数,定义 $n!$ 为

$$n! = \prod_{k=1}^{n} k = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n.$$

特别地,我们约定 $0! = 1$.

定义 1-5　数 α 称为代数数,如果存在整系数多项式 $a_0 + a_1 x + \cdots + a_n x^n$ 满足 $a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0$. α 若不是代数数,则称为超越数.

例题 1-3　设 a 是整数,则 $\sqrt{a}$ 是代数数,因为它是整系数多项式 $x^2 - a$ 的根.

注 1-1　所有的有理数都是代数数.

§1-2　最小数原理与数学归纳法

一、最小数原理

定理 1-1　正整数集的任何非空子集都必含有最小数.

证明　设 S 是正整数集 $\mathbf{Z}^+$ 的一个非空子集,在 S 中任取一个数 s,则 S 中不大于 s 的数最多有 s 个,所以这些数中一定有一个最小数,记为 m,显然,m 就是 S 中的最小数.

注 1-2　最小数原理只对正整数的集合适用,其他数集中不一定成立. 例如:正分数集中就没有最小数.

二、数学归纳法

定理 1-2(第一数学归纳法)　设 $P(n)$ 是关于正整数 n 的命题,若

(i)当 $n=1$ 时,命题 $P(1)$ 成立;

(ii)在 $P(k)$(k 为任意正整数)成立的假设下可以推出 $P(k+1)$ 成立,则

$P(n)$对一切正整数 n 都成立.

证明 假设命题 $P(n)$不是对一切正整数 n 都成立,则使命题 $P(n)$不成立的正整数组成的集合 S 是 $\mathbf{Z}^+$ 的非空子集. 由最小数原理,S 中有最小数 m,故 $m-1\notin S$,即 $P(m-1)$是正确的,由(ii)知 $P(m)$正确,这就与假设产生了矛盾. 所以命题 $P(n)$对一切正整数 n 都成立.

例题 1-4 若 $x_1=3$,且 $x_{n+1}=x_n(x_n+2)$,$n\geqslant 1$. 求此数列的通项公式.

解答 易知 $x_1=3=2^2-1$,$x_2=15=2^4-1$,$x_3=255=2^8-1$,因此可猜测:对任意正整数 n,有

$$x_n=2^{2^n}-1.$$

上面已经验证 $n=1$ 成立,现假设结论对正整数 $n=k$ 时也成立,对 $n=k+1$,有

$$x_{k+1}=x_k(x_k+2)=(2^{2^k}-1)(2^{2^k}-1+2)=2^{2^{k+1}}-1.$$

所以我们猜测的公式正确.

定理 1-3(第二数学归纳法) 设 $P(n)$是关于正整数 n 的命题,若

(i)当 $n=1$ 时,命题 $P(1)$成立;

(ii)假设对一切 $k<m$,命题 $P(k)$是成立的,可以推出 $P(m)$成立,则 $P(n)$对一切正整数 n 都成立.

证明 假设命题 $P(n)$不是对一切正整数 n 都成立,则使命题 $P(n)$不成立的正整数组成的集合 S 是 $\mathbf{Z}^+$ 的非空子集. 由最小数原理,S 中有最小数 m,故对一切 $k<m$,命题 $P(k)$是成立的. 由(ii)知 $P(m)$正确,这就与假设产生了矛盾. 所以命题 $P(n)$对一切正整数 n 都成立.

注 1-3 数学归纳法是一种非常有效的证明与正整数有关的命题的数学方法. 它绕开了证明过程中的很多障碍,因此显得简洁有力. 所以,如何用好数学归纳法是解题的关键.

例题 1-5 证明:Fibonacci 数列 F_n 满足公式

$$F_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}(n\geqslant 1),\ \text{这里}\ \alpha=\frac{1+\sqrt{5}}{2},\ \beta=\frac{1-\sqrt{5}}{2}.$$

证明 用数学归纳法证明此公式. 当 $n=1$ 时,由于 $F_1=1$,所以公式显然成立.

现在令 $n\geqslant 2$,假设公式对不大于 n 的正整数成立,证明用 $n+1$ 代替 n 时,公式也成立. 因为

$$F_{n+1}=F_n+F_{n-1}=\frac{\alpha^n-\beta^n}{\alpha-\beta}+\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}=\frac{\alpha^{n-1}(\alpha+1)-\beta^{n-1}(\beta+1)}{\alpha-\beta}$$

$$=\frac{\alpha^{n-1}\cdot\alpha^2-\beta^{n-1}\cdot\beta^2}{\alpha-\beta}=\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}.$$

所以,由数学归纳法证得公式成立.

§1-3　整除的概念与带余除法

一、整除的概念

定义 1-6　设 a,b 是两个整数且 $a\neq0$,如果存在整数 q,使得等式

$$b=aq \tag{1-1}$$

成立,则称 a 整除 b 或 b 被 a 整除,记作 $a\mid b$,此时我们把 a 叫做 b 的约数(因数或除数),把 b 叫做 a 的倍数.

如果(1-1)式中的整数 q 不存在,我们就说 a 不能整除 b 或 b 不能被 a 整除,记作 $a\nmid b$.

例题 1-6　$11\nmid189$, $-6\mid42$, $25\mid0$, $5\nmid56$, $-7\nmid68$.

例题 1-7　6 的所有约数是 ±1, ±2, ±3 和 ±6. 11 的所有约数是 ±1 和 ±11.

例题 1-8　设 $d_1<d_2<\cdots<d_k$ 是 n 的所有正约数,则 $\frac{n}{d_1}>\frac{n}{d_2}>\cdots>\frac{n}{d_k}$ 也是 n 的所有正约数. 从而有 $d_1d_2\cdots d_k=\frac{n}{d_1}\cdot\frac{n}{d_2}\cdot\cdots\cdot\frac{n}{d_k}$,故 $d_1d_2\cdots d_k=n^{\frac{k}{2}}$.

例题 1-9　若 a,b 是整数,n 是正整数,则

(i)当 $a\neq b$ 时,$(a-b)\mid(a^n-b^n)$;

(ii)当 $a+b\neq0$ 时,$(a+b)\mid(a^{2n+1}+b^{2n+1})$;

(iii)$8\mid(a^2-1)$,这里 a 是奇数.

注 1-4　两个平方数之和 a^2+b^2 在 $2ab$ 是平方数时可分解,例如:

$a^4+4b^4=(a^2+2b^2)^2-(2ab)^2=(a^2+2b^2+2ab)(a^2+2b^2-2ab)$.

二、整除的基本性质

由整除的定义,我们容易得到下列性质(读者自己给出证明):

性质 1-8　设 a,b,c 是整数,且 $a\mid b,b\mid c$,则 $a\mid c$.

性质 1-9　设 a,b,m,n 是整数,如果 $c\mid a,c\mid b$,则 $c\mid(am+bn)$.

性质 1-10　设 a,b,c 是整数,且 $c\neq0$,则 $a\mid b\Leftrightarrow ac\mid bc$.

性质 1-11　设 a,b 是正整数,且 $a\mid b$,则 $a\leqslant b$.

性质 1-12　设 a,b 是整数,且 $a\mid b,b\mid a$,则 $a=\pm b$.

三、带余除法

定理 1－4(带余除法定理) 设 a,b 是整数,且 $b>0$,则存在两个整数 q 及 r,使得

$$a=bq+r,0\leqslant r<b \tag{1-2}$$

成立,且 q 和 r 是唯一的.(q 和 r 分别称为 a 除以 b 所得的商和余数.)

证明 存在性 (通过对数轴的划分)作整数序列

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

则 a 必在上述序列的某两项之间,即存在一个整数 q 使得

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

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

唯一性(反证法) 设 q_1,r_1 是满足(1－2)式的两个整数,则

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

因而 $$bq_1+r_1=bq+r.$$

于是 $$b(q-q_1)=r_1-r.$$

故 $$b|q-q_1|=|r_1-r|.$$

由于 r 及 r_1 都是小于 b 的整数,所以上式右边是小于 b 的. 如果 $q\neq q_1$,则上式左边 $\geqslant b$,这是不可能的. 因此 $q=q_1$,进而 $r=r_1$.

例题 1－10 设 $n,d(d\neq0)$ 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 $d\mid f(n)\Leftrightarrow d\mid f(r)$.

证明 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 $d\mid f(n)\Leftrightarrow d\mid f(r)$.

§1－4 最大公约数与最小公倍数

一、最大公约数

定义 1－7 整数 a,b 的公共约数称为 a,b 的公约数. 不全为零的整数 a,b 的公约数中最大的一个称为 a,b 的最大公约数,记作(a,b).

注 1－5 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 1－8 如果整数 a,b 的最大公约数$(a,b)=1$,则称 a,b 是互素的(或

互质的).

定理 1-5　如果整数 a,b 的最大公约数 $(a,b)=d$,则 $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

证明　设 $\left(\frac{a}{d},\frac{b}{d}\right)=e$,则 $e\left|\frac{a}{d},e\right|\frac{b}{d}$,即 $ed\mid a,ed\mid b$. 也就是说 ed 是 a,b 的一个公约数,从而 $ed\leqslant d$,所以 $e=1$.

定理 1-6　如果整数 a,b 的最大公约数 $(a,b)=d$,则对任意整数 c,有 $(a+cb,b)=d$,即 $(a+cb,b)=(a,b)$.

证明　设 $(a+cb,b)=e$,则 $e\mid(a+cb),e\mid b$,所以 $e\mid[(a+cb)-cb]$,即 $e\mid a$. 也就是说 e 是 a,b 的一个公约数,从而 $e\leqslant d$. 另一方面,由 $(a,b)=d$,得 $d\mid a,d\mid b$,所以 $d\mid(a+cb)$. 也就是说 d 是 $a+cb,b$ 的一个公约数,从而 $d\leqslant e$,所以 $d=e$.

例题 1-11　证明 $\frac{21n+4}{14n+3}$ 为既约分数,即证明:$(21n+4,14n+3)=1$.

证明　由定理 1-6 得,$(21n+4,14n+3)=(7n+1,14n+3)=(7n+1,1)=1$.

定理 1-7　如果整数 a,b(不全为零)的最大公约数 $(a,b)=d$,则存在整数 m,n,使得 $d=am+bn$.

证明　令 $S=\{ax+by>0\mid x,y\in\mathbf{Z}\}$,由整数 a,b 不全为零,知 S 非空,所以由最小数原理,S 中存在最小的正整数,设为 e. 令

$$e=am+bn,$$

这里 m,n 是整数. 下面我们证明 $e=d$.

一方面,由带余除法定理,有

$$a=qe+r,0\leqslant r<e,$$

所以 $r=a-qe=a-q(ma+nb)=(1-qm)a-qnb$. 若 $r\neq0$,则 $r\in S$,则由 e 的假设知 e 为 S 中的最小正整数,这和 $r<e$ 矛盾. 故 $r=0$,从而 $e\mid a$,同理 $e\mid b$,即 e 是 a,b 的一个公约数,所以 $e\leqslant d$.

另一方面,由 $(a,b)=d$,知 $d\mid a,d\mid b$,则 $d\mid(ma+nb)$,即 $d\mid e$,因此 $d\leqslant e$. 所以 $e=d$.

注 1-6　由定理 1-7,我们知道 a,b 的任一公约数都能整除它们的最大公约数 (a,b).

定理 1-8　整数 a,b 不全为零,如果 d 是 a,b 的一个正公约数,且存在整数 m,n,使得 $d=am+bn$,则 $(a,b)=d$.

证明　设 $(a,b)=e$,则 $e\mid a,e\mid b$,由 $d=am+bn$,得 $e\mid d$,所以 $e\leqslant d$. 另一方面,由 d 是 a,b 的一个正公约数,知 $d\leqslant e$. 故 $d=e$.

定理 1-9 设 a,b 是两个不全为零的整数,若 m 是任一正整数,则

$$(am,bm)=(a,b)m.$$

证明 因为存在整数 u,v 使得 $au+bv=(a,b)$,所以 $amu+bmv=(a,b)m$,又 $(a,b)m$ 是 am,bm 的一个正公约数,所以由定理 1-9 得,

$$(am,bm)=(a,b)m.$$

定理 1-10 $(a,b)=1$ 的充要条件是存在整数 u,v 使得 $au+bv=1$.

证明 由定理 1-7 和定理 1-8 即得.

定理 1-11 设 a,b,c 都为整数,则

(i)若 $(a,c)=1$,且 $c\mid ab$,则 $c\mid b$;

(ii)若 $b\mid a,c\mid a$,且 $(b,c)=1$,则 $bc\mid a$;

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

证明 (i)因为 $(a,c)=1$,由定理 1-10 知,存在整数 u,v 使得 $au+cv=1$,所以 $abu+bcv=b$. 又 $c\mid ab$,所以 $c\mid (abu+bcv)$,即 $c\mid b$.

(ii)因为 $(b,c)=1$,由定理 1-10 知,存在整数 u,v 使得 $bu+cv=1$,所以 $abu+acv=a$. 又 $b\mid a,c\mid a$,所以 $bc\mid ab,bc\mid ac$,从而 $bc\mid (abu+acv)$,即 $bc\mid a$.

(iii)因为 $(a,c)=1,(b,c)=1$,由定理 1-10 知,存在整数 u_1,v_1 及 u_2,v_2 使得 $au_1+cv_1=1,bu_2+cv_2=1$,所以 $abu_1u_2+c(au_1v_2+bu_2v_1+cv_1v_2)=1$,即 $(ab,c)=1$.

定理 1-12 设 $a_1,a_2,\cdots,a_n$ 及 $b_1,b_2,\cdots,b_m$ 是任意两组整数,若前一组中任一整数与后一组中任一整数互质,则 $(a_1a_2\cdots a_n,b_1b_2\cdots b_m)=1$. 特别地,当 $(a,b)=1$ 时,有 $(a^n,b^m)=1$,其中 m,n 是正整数.

证明 由定理 1-11(iii)即得.

定义 1-9 不全为零的整数 $a_1,a_2,\cdots,a_n(n\geqslant 2)$ 的公约数中最大的一个称为 $a_1,a_2,\cdots,a_n$ 的最大公约数,记作 $(a_1,a_2,\cdots,a_n)$.

定理 1-13 整数 $a_1,a_2,\cdots,a_n(n\geqslant 2)$ 不全为零,则

$$(a_1,a_2,\cdots,a_{n-1},a_n)=(a_1,a_2,\cdots,(a_{n-1},a_n)).$$

证明 记 $(a_1,a_2,\cdots,(a_{n-1},a_n))=d$,则 $d\mid a_1,d\mid a_2,\cdots,d\mid a_{n-2},d\mid (a_{n-1},a_n)$,从而 $d\mid a_1,d\mid a_2,\cdots,d\mid a_{n-2},d\mid a_{n-1},d\mid a_n$,即 d 是 $a_1,a_2,\cdots,a_n$ 的一个公约数. 又设 h 是 $a_1,a_2,\cdots,a_n$ 的任一公约数,则由 $h\mid a_{n-1},h\mid a_n$,得 $h\mid (a_{n-1},a_n)$. 所以 $h\mid a_1,h\mid a_2,\cdots,h\mid a_{n-2},h\mid (a_{n-1},a_n)$,即 h 是 $a_1,a_2,\cdots,(a_{n-1},a_n)$ 的一个公约数. 故 $h\leqslant d$. 所以 $(a_1,a_2,\cdots,a_{n-1},a_n)=d$.

定理 1-14 若 $a_1,a_2,\cdots,a_n$ 是任意 n 个不全为零的整数,则存在 n 个整数 $t_1,t_2,\cdots,t_n$,使得

$$a_1t_1+a_2t_2+\cdots+a_nt_n=(a_1,a_2,\cdots,a_n).$$

证明　利用定理1-7,定理1-13及数学归纳法即可证得.

注1-7　设h是不全为零的整数$a_1,a_2,\cdots,a_n$的任一公约数,由定理1-14有$h\mid(a_1,a_2,\cdots,a_n)$,即$a_1,a_2,\cdots,a_n$的公因数与$(a_1,a_2,\cdots,a_n)$的因数相同.

定义1-10　如果整数$a_1,a_2,\cdots,a_n$的最大公约数$(a_1,a_2,\cdots,a_n)=1$,则称$a_1,a_2,\cdots,a_n$是互素的(或互质的).如果整数$a_1,a_2,\cdots,a_n$中的任意两个整数都互素,则称整数$a_1,a_2,\cdots,a_n$两两互素.

注1-8　整数$a_1,a_2,\cdots,a_n$两两互素可以推出整数$a_1,a_2,\cdots,a_n$互素,反之不成立.例如,15,21,35互素,但不是两两互素.

定理1-15　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

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

证明　由定理1-14可得.

二、最大公约数的求法:辗转相除法(Euclid算法)

由最大公约数的定义可知,任意一个整数与它的相反数都有相同的约数,即$(a,b)=(|a|,|b|)$,这一性质告诉我们要讨论最大公约数不妨仅就非负整数讨论,又因为$(a,0)=|a|$,所以我们只需讨论正整数的最大公约数的求法.下面我们介绍辗转相除法,辗转相除法不仅可用以求出两个正整数的最大公约数,而且可借此推出最大公约数的重要性质.

设$r_0=a,r_1=b$是任意两个正整数,且$a\geqslant b$,由带余除法,我们有下列等式:

$$\begin{aligned}
&r_0=r_1q_1+r_2,\ 0<r_2<r_1,\\
&r_1=r_2q_2+r_3,\ 0<r_3<r_2,\\
&\cdots\\
&r_{n-2}=r_{n-1}q_{n-1}+r_n,\ 0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_n.
\end{aligned}\tag{1-3}$$

因为每进行一次带余除法,余数就至少减一,而b是有限的,所以我们最多进行b次(事实上不到b次)带余除法,就可以得到一个余数是零的等式,即$r_{n+1}=0$.(1-3)式所指出的计算方法,叫做辗转相除法.

由(1-3)式和定理1-6,有$r_n=(0,r_n)=(r_{n+1},r_n)=(r_n,r_{n-1})=\cdots=(r_1,r_2)=(r_0,r_1)=(a,b)$,并且

$$r_k=s_ka+t_kb\ (k=0,1,\cdots,n),$$

其中$s_0=1,s_1=0,s_j=s_{j-2}-q_{j-1}s_{j-1},t_0=0,t_1=1,t_j=t_{j-2}-q_{j-1}t_{j-1}(2\leqslant j\leqslant n)$.

例题1-12　设$a=169,b=121$,求一组整数s,t使得$as+bt=(a,b)$.

解答　$169=1\times121+48$,

$121=2\times48+25$,

$48=1\times25+23$,

$25=1\times23+2$,

$23=11\times2+1$,

$2=2\times1$.

所以 $r_6=1=(169,121)$.

因为 $q_1=1,q_2=2,q_3=1,q_4=1,q_5=11$,所以

$s_0=1$,　　$t_0=0$,

$s_1=0$,　　$t_1=1$

$s_2=s_0-s_1q_1=1-0\times1=1$,　　$t_2=t_0-t_1q_1=0-1\times1=-1$,

$s_3=s_1-s_2q_2=0-1\times2=-2$,　　$t_3=t_1-t_2q_2=1-(-1)\times2=3$,

$s_4=s_2-s_3q_3=1-(-2)\times1=3$,　　$t_4=t_2-t_3q_3=-1-3\times1=-4$,

$s_5=s_3-s_4q_4=-2-3\times1=-5$,　　$t_5=t_3-t_4q_4=3-(-4)\times1=7$,

$s_6=s_4-s_5q_5=3-(-5)\times11=58$,　　$t_6=t_4-t_5q_5=-4-7\times11=-81$,

从而,由 $r_6=s_6a+t_6b$,有

$$169\times58+121\times(-81)=1.$$

三、最小公倍数

定义 1-11　设 $a_1,a_2,\cdots,a_n$ 是 $n(n\geqslant2)$ 个整数. 如果正整数 M 满足

(i) M 是 $a_1,a_2,\cdots,a_n$ 的公倍数,即 $a_1\mid M,a_2\mid M,\cdots,a_n\mid M$;

(ii) 对 $a_1,a_2,\cdots,a_n$ 的任意一个正公倍数 H,有 $H\geqslant M$,则称 M 是 $a_1,a_2,\cdots,a_n$ 的最小公倍数,记作 $[a_1,a_2,\cdots,a_n]$.

由于任意一个整数与它的相反数都有相同的倍数,所以 $[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]$,这一性质告诉我们要讨论最小公倍数不妨仅就非负整数讨论.

定理 1-16　设 a,b 是任意两个正整数,H 是 a,b 的任一公倍数,则 H 是 $[a,b]$ 的倍数,即 $[a,b]\mid H$.

证明　由带余除法,设 $H=[a,b]q+r$,这里 $0\leqslant r<[a,b]$. 由 $a\mid H,b\mid H$ 知 $a\mid r,b\mid r$,即 r 是 a,b 的公倍数,若 $0<r<[a,b]$,则与 $[a,b]$ 的定义相矛盾,所以 $r=0$,即 $[a,b]\mid H$.

定理 1-17　设 a,b 是任意两个正整数,则 $[a,b](a,b)=ab$. 特别地,若 $(a,b)=1$,有 $[a,b]=ab$.

证明　问题相当于证明 $(a,b)=\dfrac{ab}{[a,b]}$,下面我们按最大公约数的定义来