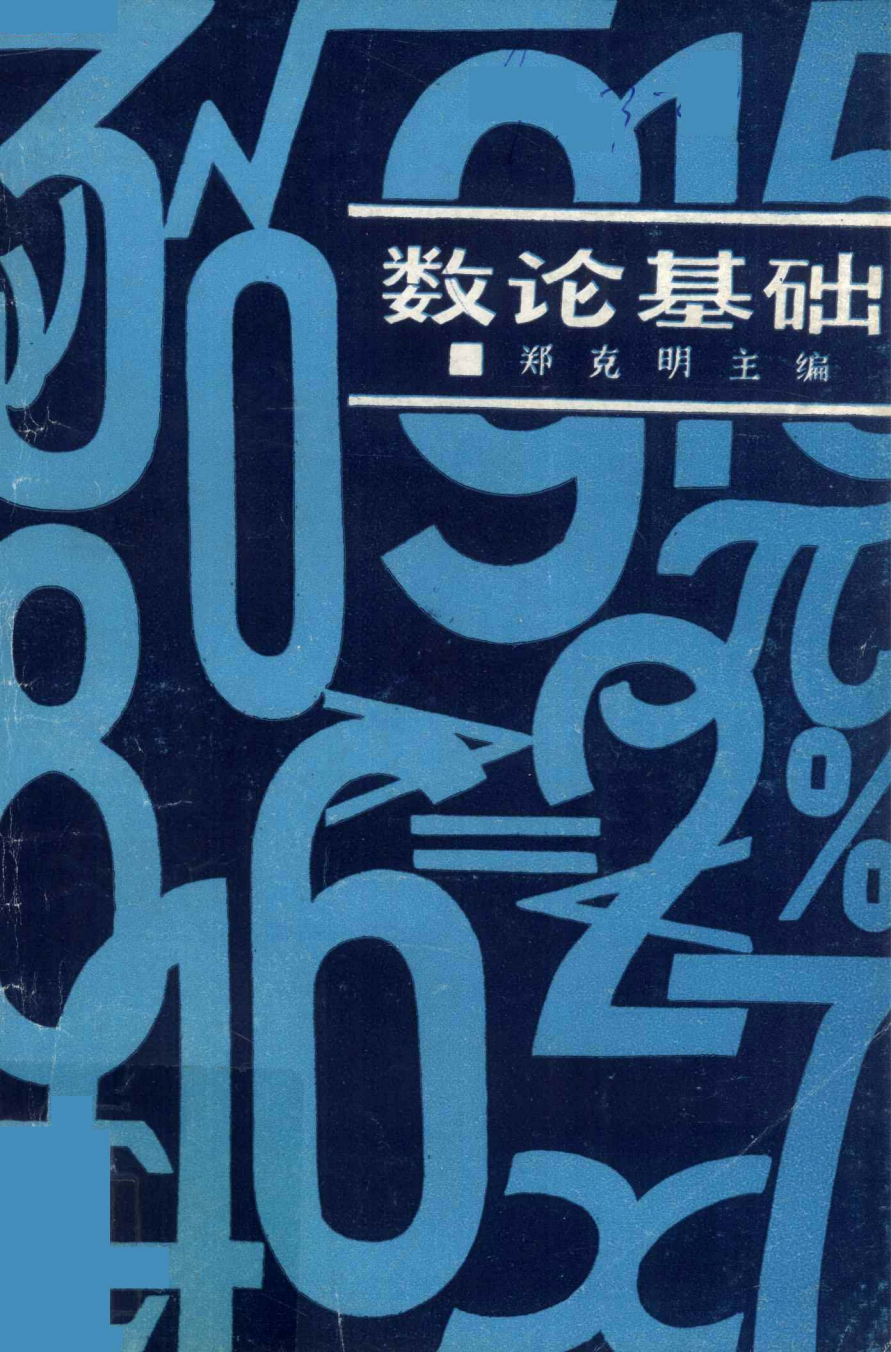
数论基础

郑克明主编



数论基础

郑克明主编　陈重穆主审

西南师范大学出版社

责任编辑：赵宏量　施明全
封面设计：傅孝修

数论基础
郑克明　主编

西南师范大学出版社出版
（重庆　北碚）
新华书店重庆发行所经销
内江新华印刷厂印刷
开本：787×1092 1/32 印张：6.625字数：144千
1991年1月第1版　　1991年1月第1次印刷
印数：1—6,000
*
ISBN 7—5621—0510—3/G·345

定价：1.30 元

序　言

数论是研究数的性质的一门学科，按研究中使用数学方法的不同而分为初等数论、解析数论、代数数论和几何数论．数论基础主要用初等数学方法研究整数的性质，它与中学数学教育有着密切的联系，并给现代数学提供理论基础．在计算技术、组合数学等领域中有着广泛的应用．数论中的一些问题，貌似简单，实则不易，解决起来，灵活而富有技巧，是培养数学思维能力的重要内容，是中学数学竞赛题的丰富源泉之一，是数学教育工作者必备的基础知识．

高等师范院校开设数论基础课的主要目的在于使学生熟悉和掌握数论的基础知识、基本理论和基本的解题技能技巧，培养学生的逻辑思维能力，为从事中学数学教学、指导数学课外小组活动和进一步学习其它数学学科打下坚实的基础，为此，必须加强教材建设，1988年4月西南五省区高师院校数学系系主任于贵州师范大学举行首届联席会议，在与会代表的倡议下，决定群策群力，加强协作，积极着手编写数论教材．经过一年多的努力，完成了教材初稿．1989年9月，西南五省区第二届高师院校数学系系主任联席会议在广西师范大学举行，会上检查了教材协作编写的情况．与此同时，举行了数论基础教材审稿会，参加编写或审稿的院校有西南师范大学、云南师范大学、广西师范大学、贵州师范大学、四川师范学院、重庆师范学院、海南师范学院和西南民

族学院．四川师范大学对编写本书也给予了支持．参加编写的有七位副教授：第一章陈良群，第二章王骅，第三章严家森，第四章彭光济，第五章陈应枢，第六章郑克明，有关数论函数部分则由刘先年编写．最后由郑克明汇集审稿意见统一修改完成．

在本书的编写中，我们注意系统而科学地讲清数论的基础知识、基本理论和基本方法，贯彻理论联系实际和少而精的原则，紧密结合中学实际、国际奥林匹克数学竞赛试题和在生产实践中的应用．联系所学内容介绍国内外数论方面的新成就和尚未解决的问题，以开拓视野，激发学习热情．尤其注意介绍各类问题的解题思路与方法，并通过大量的例题具体加以剖析，适宜作为高师院校数学系本、专科和函授数学专业本、专科以及同类专业的数论课教材，也可供中学数学教师和其它数学工作者参考．授完本教材约需 50 学时左右．

在本书编写过程中，得到西南师范大学严栋开教授、陈重穆教授的大力支持和热情指导．本书由陈重穆教授主审，他对书稿进行了认真而详尽的审阅，提出了许多宝贵意见，作者对严、陈二位教授表示衷心的感谢．编写中还参阅了有关书籍和期刊，谨向原编著者致谢．对西南师范大学出版社的全力支持，作者深表谢意．

由于时间仓促，水平有限，疏漏之处在所难免，欢迎指正．

编者

1990．3．于成都

目　录

第一章　整除理论

本章以整除和带余除法为先导，以辗转相除法、最大公因数、最小公倍数和算术基本定理为主干，阐述整除理论中最基本的性质．对这些性质的论证，力求理论体系的连贯性和逻辑推理的严密性．

§1.1　整　　除

我们知道，整数的相加、相减、相乘，其和、差、积仍为整数；相除则不然，从而有必要引入整除的概念．

定义1　对于整数a和非零整数b，如果存在整数q，使得$a=bq$，则称b能**整除**a或a能被b整除，记为$b|a$．此时，又称a是b的倍数，b是a的因数或约数．如果这样的q不存在，则称b不能整除a或a不能被b整除，记为$b\nmid a$．

由定义易知$1|a$，$b|0$，$b|b$（$b\neq 0$）．以后，如无特殊声明，拉丁字母a，b，c，…均表整数．

整除不是整数集中的代数运算，因二整数的商不一定是整数．整除具有下列基本性质：

性质1　整数a及非零整数b，如果$b|a$，则有$b|(-a)$，$(-b)|a$，$(-b)|(-a)$．

事实上，由$b|a$，存在整数q，使$a=bq$，从而有

$-a=b(-q)$，$a=(-b)(-q)$，$-a=(-b)q$．

性质1表明，整除性与整数之正负无关．

性质2 若$c|b$, $b|a$, ($b\neq0$, $c\neq0$)则$c|a$.

证 由$c|b$, $b|a$的定义知有整数q_1, q_2使

$$b=cq_1,\quad a=bq_2$$

于是$a=c(q_1q_2)$, 且$c\neq0$, q_1q_2为整数, 故$c|a$.

性质3 (i) 若$b|a$,则$a=0$或$|b|\leqslant|a|$;

(ii) 若$b|a$,$a|b$, 则$a=\pm b$;

(iii) 若$b|a$,则$b|ma$,(m为整数).

(证明留给读者)

性质4 若$b|a_1$, $b|a_2$($b\neq0$), 则

$$b|m_1a_1+m_2a_2,\ (m_1,\ m_2\text{为整数}).$$

证 由性质3(iii)知$b|m_1a_1$, $b|m_2a_2$, 于是存在整数q_1, q_2使$m_1a_1=bq_1$, $m_2a_2=bq_2$, 而有

$$m_1a_1+m_2a_2=b(q_1+q_2),$$

其中q_1+q_2为整数, 故得$b|m_1a_1+m_2a_2$.

由此易得

推论 (i) 若$b|a_i$($i=1,\ 2,\ \cdots,\ n,\ n\geqslant2$), 则$b|\sum_{i=1}^{n}m_ia_i$, ($m_i$为整数, $i=1,\ 2,\ \cdots,\ n$);

(ii)设$a=\sum_{i=1}^{n}a_i$,而$b|a_l$,$l=1,2,\cdots,k-1,k+1,\cdots,n$则$b|a$的充要条件是$b|a_k$.

例1 $9|\overline{a_na_{n-1}\cdots a_1a_0}$的充要条件是$9|\sum_{i=0}^{n}a_i$. (其中$a_0$, a_1, $\cdots$, a_n是十进数码, $\overline{a_na_{n-1}\cdots a_1a_0}$表示$n+1$位数码组成的数.)

证 $\overline{a_na_{n-1}\cdots a_1a_0}=a_n\cdot10^n+a_{n-1}\cdot10^{n-1}+\cdots+a_1\cdot10+a_0=a_n(10^n-1)+a_{n-1}(10^{n-1}-1)+\cdots+a_1(10-1)+$

$\sum_{i=1}^{n} a_i$由$10^k-1=(10-1)(10^{k-1}+\cdots+10+1)$知 $9\mid 10^k-1$，有$9\mid a_k(10^k-1)$，　$k=1, 2, \cdots, n$，用推论(ii)即得：

$9\mid \overline{a_n a_{n-1}\cdots a_1 a_0}$的充要条件是$9\mid \sum_{i=1}^{n} a_i$.

于是显然有

$3\mid \overline{a_n a_{n-1}\cdots a_1 a_0}$的充要条件是$3\mid \sum_{i=1}^{n} a_i$.

例2　设m是非负整数，证明$57\mid 7^{m+2}+8^{2m+1}$.

证　当m＝0时，$7^{m+2}+8^{2m+1}=7^2+8=57$，有$57\mid 57$.

当m为正整数时，则　$7^{m+2}+8^{2m+1}=49\cdot 7^m+8\cdot 64^m=57\cdot 7^m+8(64^m-7^m)=57\cdot 7^m+8(64-7)(64^{m-1}+\cdots+7^{m-1})=57[7^m+8(64^{m-1}+\cdots+7^{m-1}]$. 仍有

$$57\mid 7^{m+2}+8^{2m+1},$$

2的倍数叫做**偶数**，可表为2n；不是2的倍数的整数叫做**奇数**，可表为2m＋1，其中n、m为整数. 易知

偶数±偶数＝偶数；　　奇数±奇数＝偶数；

偶数±奇数＝奇数；　　偶数×整数＝偶数；

奇数×奇数＝奇数.

这些基本的整数性质，固属显然. 可是利用它能较易地解决一些不太显然的问题.

例3　是否存在十个正奇数的倒数之和等于1？

证　不存在. 用反证法，若有10个正奇数$a_1, a_2, \cdots, a_{10}$　使$\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_{10}}=1$ 成立，两端乘以$a_1a_2\cdots a_{10}$得　$a_2a_3\cdots a_{10}+a_1a_3\cdots a_{10}+\cdots+a_1a_2\cdots a_9=a_1a_2\cdots a_{10}$ 右端是奇数之积为奇数，而左端是10个奇数之和应为一偶数.

故等式不成立.

例4 不用直接计算，证明行列式

$$\begin{vmatrix} 1 & 3 & 5 & 7 & 9 \\ 3 & 5 & 7 & 9 & 2 \\ 5 & 7 & 9 & 2 & 4 \\ 7 & 9 & 2 & 4 & 6 \\ 9 & 2 & 4 & 6 & 8 \end{vmatrix} \neq 0.$$

证 根据行列式的定义，这个五阶行列式共有$5!=120$项，每项的绝对值是取自不同行不同列的五个数的乘积．副对角线上的五个数之积$9\cdot9\cdot9\cdot9\cdot9$这一项为奇数；易知其余119项均为偶数，其代数和应为偶数．因此，这个行列式之值可化为一个奇数与一个偶数的代数和，应为一奇数．故不可能为0．（0为偶数）

（注：以上两例均可推广．）

定理1.1（带余除法） 对于任一整数a和正整数b，有且仅有一整数对q、r，使

$$a=bq+r,\quad 0\leqslant r<b.$$

证 因为任一给定的整数a，必落在整数序列$\cdots,-3b,-2b,-b,0,b,2b,3b,\cdots(b>0)$某相邻二整数之间，即必存在整数q，使$qb\leqslant a<(q+1)b$成立，于是$0\leqslant a-qb<b$，令$a-bq=r$，即得$a=bq+r$，$0\leqslant r<b$.

这样的q、r是唯一的．如果有整数q'、r'使$a=bq'+r'$，$0\leqslant r'<b$，则

$$r-r'=b(q'-q),$$

即$b\mid r-r'$．而$|r-r'|<b$，故必有$r-r'=0$，于是$r'=r$．随之$q'=q$．■

定理中的q称为b除a的整数商，r称为b除a的余数．读者不难证明

推论1 任意整数a及非零整数b，存在唯一整数对q、r，使$a=bq+r$，$0\leqslant r<|b|$．

推论2 $b|a$的充要条件是$r=0$．

例5 三个连续整数之积必为3的倍数．

证 设三个连续整数为$n-2$，$n-1$，n由带余除法，对于这个n，存在整数q，r，使$n=3q+r$或$n-r=3q$，$0\leqslant r<3$．当$r=0$时，有$3|n$；$r=1$时有$3|n-1$；$r=2$时有$3|n-2$，故总有，$3|n(n-1)(n-2)$．

例6 任意一百个整数中，必有两个整数之差能被99整除．

证 设a_1，a_2，…，a_{100}为任意给定的一百个整数．于是应存在一百个整数对q_i，r_i使

$$a_i=99q_i+r_i,\quad 0\leqslant r_i<99,\quad i=1,2,\cdots,100.$$

这100个r_i的每一个只能为0至98这99个整数中的某一个，于是至少有两个余数r_i，r_j相同，从而有$a_j-a_i=99(q_j-q_i)$，且q_j-q_i是整数，所以

$$99|a_j-a_i.$$

§1.2 最大公因数

定义1 设整数$d\neq 0$，如果d分别是整数a_1，a_2，…，a_n（$n\geqslant 2$）的因数，则称d是a_1，a_2，…，a_n的**公因数**或**公约数**．

显然，(i) 如果a_1，a_2，…，a_n全为零，则任何非零

整数都是它们的公因数.

(ii) 公因数与数组的顺序和 数的正负性无关.

定义2 若d是整数a_1, a_2, …, a_n ($n\geqslant 2$) 的公因数中的最大者, 则称d是它们的**最大公因数**或**最大公 约 数**, 记为 $d=(a_1, a_2, \cdots, a_n)$.

如果$(a_1, a_2, \cdots, a_n)=1$, 则称$a_1$, a_2, …, a_n 互 素或互质. 如果a_1, a_2, …, a_n中任意两个数的最大公因数都是 1 , 则称它们两两互素.

两两互素必互素, 但互素不一定两两互 素, 例 如 (2, 4, 5)=1, 但2, 4, 5非两两互素, 因(2, 4)=2≠1.

全为零的数组, 任一整数都是它们的公因数, 规定(0, 0,…,0)=0.不全为零的整数组的最大公因 数 显 然 是 存 在的.

由定义不难得到

性质5 (i) (a, 1) = 1 , 故 任 一 整 数 与 1 互 素; (ii) (b, 0)=|b|; (iii) $(a_1, a_2, \cdots, a_n)=(|a_1|, |a_2|, \cdots, |a_n|)$.

于是讨论最大公因数常就正整数进行.

定理1.2 若a=bq+c, 则 (i) a, b与b, c有相同的公因数; (ii) (a, b)=(b, c)或(a, b)=(b, a−bq).

证 设d是a、b的任一公因数, d|a,d|b ∴d|a−bq, 即d|c, 可见d是b, c的公因数, 同理可证b, c的 任一公 因数也是a, b的公因数, 故(i)成立. 随之(ii)成立. ∎

如何求两个数的最大公因数呢? 我 们 介 绍 辗 转 相 除法.

设a, b均为正整数, 反复引用带余除法可得:

$$
\begin{aligned}
a&=bq_1+r_1, \quad 0<r_1<b\\
b&=r_1q_2+r_2, \quad 0<r_2<r_1\\
&\cdots\cdots \qquad \cdots\cdots\\
r_{k-2}&=r_{k-1}q_k+r_k, \quad 0<r_k<r_{k-1} \qquad (1)\\
&\cdots\cdots \qquad \cdots\cdots\\
r_{n-2}&=r_{n-1}q_n+r_n, \quad 0<r_n<r_{n-1}\\
r_{n-1}&=r_nq_{n+1}+r_{n+1}, \quad r_{n+1}=0.
\end{aligned}
$$

由于b是已给定的正整数，显然存在n，使$r_{n+1}=0$.

式(1)中所指的计算方法，通常称为**辗转相除法**或**辗转算法**. 辗转相除法为我国古代筹算家之一卓越成就；西方则因欧几里得有此法则而称欧几里得(Euclid)除法.

定理1.3 正整数a，b的最大公因数$(a, b)=r_n$.

证 由性质5(ii)，定理1.2及式(1)知

$(a, b)=(b, r_1)=(r_1, r_2)=\cdots=(r_n, r_{n-1})=(r_n, 0)=r_n$. ∎

推论 设d是a，b的任一公因数，则$d|(a, b)$.

(证明留给读者)

例1 求$(-2346, 1081)$.

解 $(-2346, 1081)=(2346, 1081)$

	2346	1081	$2=q_1$
	2162	920	
$q_2=5$	184	161	$1=q_3$
	161	161	
$q_4=7$	23	0	

$(2346, 1081)=23$, $\therefore (-2346, 1081)=23$.

由定理1、2(ii)，$(a, b)=(b, a-bq)$还可得一求两数最大公因数的辗转相减法(实质上还是辗转相除法，只是形

式不同而已）不必写出演算竖式，只要多次用上式即得. 例如，$(1859, 1573)=(1573, 286)=(143, 286)$
$$=(143, 0)=143.$$

定理1.4 设$a_1, a_2, \cdots, a_n$ $(n\geqslant 2)$ n个整数中a_1, a_2不全为零，令$(a_1, a_2)=d_2$, $(d_2, a_3)=d_3$, $\cdots$, $(d_{n-1}, a_n)=d_n$, 则$(a_1, a_2, \cdots, a_n)=d_n$.

证 令$(a_1, a_2, \cdots, a_n)=d$, 则因$d|a_1$, $d|a_2$, 有$p|d_2$, 而$d|a_3$, 又有$d|d_3$, 仿此类推，得$d|d_n$, 故$d\leqslant d_n$.

另一方面，由$d_n|a_n$, $d_n|d_{n-1}$, 故$d_n|a_{n-1}$, 仿此可得$d_n|a_{n-2}$, $\cdots$, $d_n|a_2$, $d_n|a_1$, d_n是$a_1, a_2, \cdots, a_n$的公因数，从而$d_n\leqslant d$, 故$d=d_n$, 即
$$(a_1, a_2, \cdots, a_n)=d_n. \blacksquare$$

推论1 设d是$a_1, a_2, \cdots, a_n$的公因数，则
$$d|(a_1, a_2, \cdots, a_n).$$

推论2 (i) $(ma_1, ma_2, \cdots, ma_n)=|m|(a_1, a_2, \cdots, a_n)$;

(ii) $\left(\frac{a_1}{b}, \frac{a_2}{b}, \cdots, \frac{a_n}{b}\right)=\frac{(a_1, a_2, \cdots, a_n)}{|b|}$.

其中m为整数，整数$b\neq 0$，且$b|a_i$ $(i=1, 2, \cdots, n)$.

它们的证明由辗转相除法及定理1.4易得.

定理1.5 设a, b均为正整数，由式(1)可得
$$a[(-1)^{k-1}Q_k]+b[(-1)^kP_k]=r_k,$$
$$k=1, 2, \cdots, n \qquad (2)$$
其中$P_0=1$, $P_1=q_1$, $P_k=q_kP_{k-1}+P_{k-2}$,
$$Q_0=0, \ Q_1=1, \ Q_k=q_kQ_{k-1}+Q_{k-2},$$
$$(k=2, 3, \cdots, n) \qquad (3)$$

证 对k用数学归纳法.

当k=1时，式(2)显然成立。

当k=2时，由式(3)，$P_2=q_2P_1+P_0=q_1q_2+1$，$Q_2=q_2Q_1+Q_0=q_2$，于是 $a[(-1)^{2-1}Q_2]+b[(-1)^2P_2]=a(-q_2)+b(q_1q_2+1)=b-(a-bq_1)q_2=b-r_1q_2=r_2$，此时(2)成立.

假定式(2)在条件(3)下对小于k(≥3)成立，今对k用归纳假设及式(1)、(3)得

$$\begin{aligned}
&a[(-1)^{k-1}Q_k]+b[(-1)^kP_k]\\
&=(-1)^{k-1}a(q_kQ_{k-1}+Q_{k-2})\\
&\quad+(-1)^kb(q_kP_{k-1}+P_{k-2})\\
&=[(-1)^{k-1}aQ_{k-2}+(-1)^kbP_{k-2}]\\
&\quad+[(-1)^{k-1}aQ_{k-1}+(-1)^kbP_{k-1}]q_k\\
&=\{a[(-1)^{k-3}Q_{k-2}]+b[(-1)^{k-2}P_{k-2}]\}\\
&\quad-\{a[(-)^{k-2}Q_{k-1}]+b[(-1)^{k-1}P_{k-1}]\}q_k\\
&=r_{k-2}-r_{k-1}q_k=r_k.
\end{aligned}$$

即式(2)对k成立. ∎

下面介绍两种求P_k，Q_k的方法：

(一)列表法： 由a,b用辗转相除法求出$q_1,q_2,\cdots,q_n$，然后列表如下，按箭头所指方向进行运算，即得P_k，Q_k：

$$\begin{array}{ccccccccccc}
P_0=1 & \overset{+}{\leftarrow} & P_1=q_1 & & P_2\cdots P_{k-2} & \overset{+}{\leftarrow} & P_{k-1} & & P_k\cdots P_n\\
 & \nwarrow^{\times} & & \nearrow & & \nwarrow^{\times} & & \nearrow & \\
 & & q_1 & & q_2\cdots q_{k-2} & & q_{k-1} & & q_k\cdots q_n\\
 & \swarrow & & \searrow^{\times} & & \swarrow & & \searrow^{\times} & \\
Q_0=0 & \overset{+}{\leftarrow} & Q_1=1 & & Q_2\cdots Q_{k-2} & \overset{+}{\leftarrow} & Q_{k-1} & & Q_k\cdots Q_n
\end{array}$$

(二)矩阵法：利用二阶矩阵的乘法求P_k，Q_k：对a,

b用辗转相除法求得q_1，q_2，…，q_n，则

$$\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \quad k\geqslant 2.$$

此法不难由定理1.5用数学归纳法证明.

推论 (i) 对于不全为0的整数a，b，必存在整数s，t使as+bt=(a，b)。 (ii) (a，b)=1的充要条件是存在整数s，t使 as+bt=1.

证 (i) 不妨设a，b均为正整数，由定理1.5取$s=(-1)^{n-1}Q_n$，$t=(-1)^nP_n$及定理1.3即得.

(ii) 如 (a，b)=1，由(i)知，存在整数s，t使as+bt=1. 反之，若有整数s，t使as+bt=1，则由(a,b)|a,(a,b)|b,而有(a，b)|1,于是(a，b)=1。故(ii)得证.

例2 已知(−2346，1081)=23，求s，t使−2346s+1081t=23.

解 先求s′，t使2346s′+1081t=23. 由例1知n=3，$q_1=2$，$q_2=5$，$q_3=1$.

P_k: 1 ← 2 ← 11 ← 13

q_k: 2 5 1

Q_k: 0 ← 1 ← 5 ← 6

∴ $P_n=P_3=13$，$Q_n=Q_3=6$.

从而 $s'=(-1)^{1-3}Q_3=6$，$t=(-1)^3P_3=-13$;

∴ 2346·6+1081(−13)=23，

所以 −2346(−6)+1081(−13)=23.