经全国中小学教材审定委员会
2005 年初审通过

普通高中课程标准实验教科书

数学

选修 4–6

初等数论初步

人民教育出版社　课程教材研究所
中学数学教材实验研究组　编著

人民教育出版社
B 版

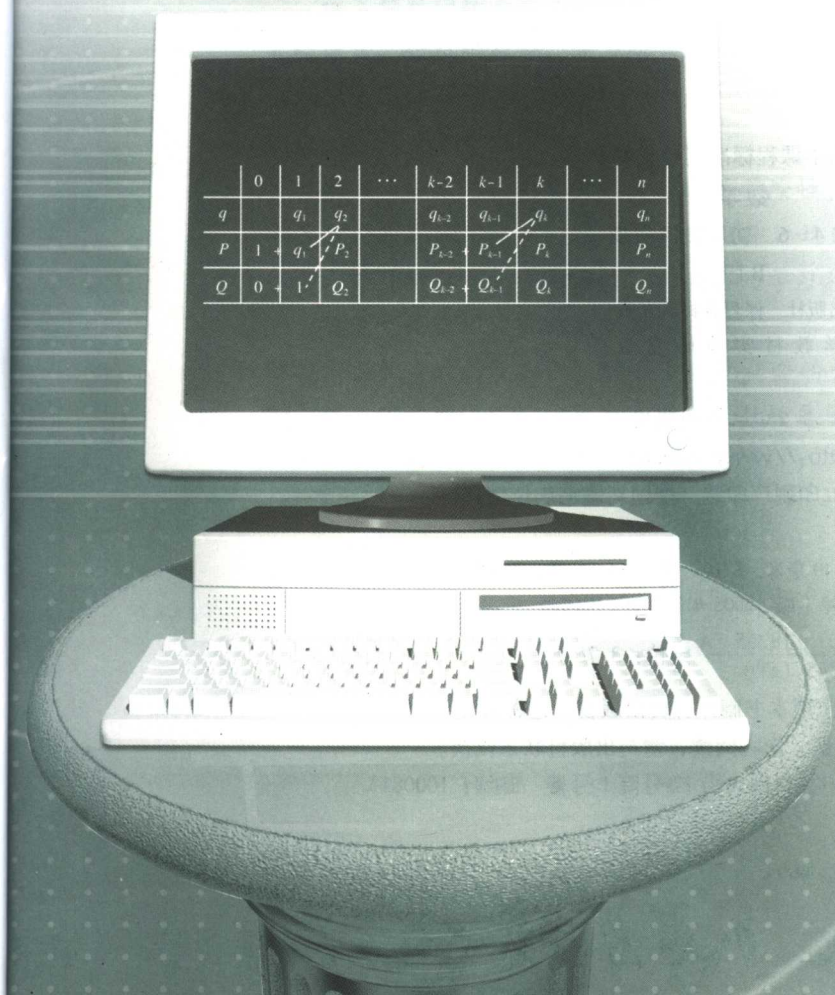
普通高中课程标准实验教科书

数学

选修 4–6

初等数论初步

人民教育出版社　课程教材研究所
中学数学教材实验研究组　编著



人民教育出版社
B版

主　　编　高存明

编　　者　曹惠中　罗声雄

责任编辑　徐伯勋　张唯一

美术编辑　李宏庆　王　喆

封面设计　李宏庆

普通高中课程标准实验教科书

数学

选修4－6　初等数论初步

B版

人民教育出版社　课程教材研究所

中学数学教材实验研究组　编著

*

人民教育出版社出版发行

网址：http://www.pep.com.cn

人民教育出版社印刷厂印装　全国新华书店经销

*

开本：890毫米×1 240毫米　1/16　印张：4　字数：75 000

2005年6月第1版　2006年7月第2次印刷

ISBN 7－107－18755－4

G·11845（课）　定价：3.76元

（联系地址：北京市海淀区中关村南大街17号院1号楼　邮编：100081）

本册导引

人类早期就认识了自然数. 它好像很简单，可又神秘莫测. 在征服自然界的进程中，人们要向自然数的奥秘进军，如同探索宇宙和生命的奥秘，经过几千年的奋斗，人类已经揭示出自然数的很多规律，但时至今日，还有许多问题没有解决. 在研究自然数的进程中，形成了一门数学学科，叫做数论. 数论者，乃论数也，专门讨论整数.

当你翻阅本书时，出现在你面前的是一堆抽象数字和生疏符号，你的第一感觉也许是陌生，甚至有点畏惧，当你怀着探索的欲望，真正进入书本后，你会发现那是错觉. 原来，你从刚懂事开始，便与自然数打交道，与它的亲密接触达十多年之久，随着学习的深入，你会逐渐感受到数论的亲和力，以及它的魅力.

同学们在以往的学习中，用各种方法和技巧解决了许多整数问题，同时也遇到了不少困难. 本书的目的是提供一些初等的一般理论与方法，在这些理论与方法的引导下，解决现实的整数问题，其中包括一些古老的、经典的整除问题和现代信息技术问题.

许多整数问题看上去好像很简单，其实十分艰深. 毋庸置疑，学数论有一定的难度，但征服困难，正是培养毅力，提高智力水平的重要途径. 本书力图深入浅出，结合同学实际，帮助同学们度过一道道难关，以获得数论的初步知识.

本书共分三章，内容分别为整数的整除性、同余及同余方程. 这三部分内容是数论的基础. 同学们在以往的学习中，均有所接触. 我们相信，只要你有信心，并且用心就能学好用好，为今后的学习和工作奠定良好的基础.

数论无论在理论方面或在实际应用方面都有重要作用，它是数学的基础学科，掌握数论的初步知识，对一个现代社会的文明公民是十分必要的. 我们热切希望，同学们选修这门课程，向自然数的奥秘进军.

目　录

第一章 整数的整除性

在日常生活中，我们经常遇到整数的整除问题. 例如，一箱苹果有48个，按个数分给7个人，能否分配公平？你马上知道，这不可能，原因是7不能整除48. 又如，本年级105人参加团体操，要求队形呈长方形（不能排成一行或一列），问排列的行数如何选择？你会立即给出答案：行数可为3，5，7，15，21，35. 这是因为只有这六个正整数能整除105.

研究整除问题，不仅是现实的需要，而且饶有兴味. 研究整数的整除不仅是数论的开端，而且所形成的方法与理论是数论的基础. 同学们与整除打交道有丰富的经验，本章不过是将你的经验与知识加以整理，使之更具普遍性和系统性.

1.1 整 除

同学们在做整数除法的时候，都知道三件事：（1）除数切忌为0；（2）除法是乘法的逆运算，例如，$3\times7=21$，那么$21\div7=3$；（3）如果$a\div b$商为整数，余数为0，则说b整除a，否则就说b不能整除a. 由此引出

定义 设a，b是整数，$b\neq0$. 如果有整数q，使$a=qb$，则称b整除a，记作$b\mid a$. 并称b是a的约数（或因数），a是b的倍数. 否则称b不能整除a，记作$b\nmid a$.

例如，$7\mid105$，105是7的倍数；$7\nmid48$，48不是7的倍数；1，3，5，7，15，21，35，105都是105的约数；1和11是11的约数；等等.

注意，0不是任何整数的约数，但0是任何整数的倍数. 符号$b\mid a$本身包含了条件$b\neq0$. a，b可以是负整数.

整除具有如下性质，请同学们自己验证.

（1）若$b\mid a$，$c\mid b$，则$c\mid a$.

（2）若$c\mid a$，$c\mid b$，则对任意整数x，y，必有$c\mid(ax+by)$.

（3）若$b\mid a$，$a\neq0$，则$|b|\leqslant|a|$.

(4) 若 $b|a$，$a\neq 0$，则 $\frac{a}{b}\Big|a$.

例 1 设 $3|m$，$7|m$，则 $21|m$.

证明：由 $3|m$，可写 $m=3q$，由此及 $7|m$ 知 $7|3q$. 由 $7|7q$，$7|3q$ 及性质(2)可得 $7|[7q-2\times(3q)]$，即 $7|q$. 因此可令 $q=7d$，于是，有 $m=3q=3\times 7d=21d$，故 $21|m$.

例 2 设 q_1，q_2，…，q_k 是正整数 n 的所有的正约数，证明

$$(q_1q_2\cdots q_k)^2=n^k.$$

证明：由性质(4)知，$\frac{n}{q_1}$，$\frac{n}{q_2}$，…，$\frac{n}{q_k}$也是 n 的全部正约数. 不妨设 $q_1<q_2<\cdots<q_k$，则有 $q_1=\frac{n}{q_k}$，$q_2=\frac{n}{q_{k-1}}$，…，$q_k=\frac{n}{q_1}$. 因此，

$$q_1q_2\cdots q_k=\frac{n}{q_k}\times\frac{n}{q_{n-1}}\times\cdots\times\frac{n}{q_1},$$

$$\Rightarrow(q_1q_2\cdots q_k)^2=n^k.$$

例如，1，2，3，4，6，12 是 12 的全部正约数，因而 $\frac{12}{1}$，$\frac{12}{2}$，$\frac{12}{3}$，$\frac{12}{4}$，$\frac{12}{6}$，$\frac{12}{12}$也是 12 的全部正约数. 后者不过是将前者倒过来排列. 因此

$$1\times2\times3\times4\times6\times12=\frac{12}{12}\times\frac{12}{6}\times\frac{12}{4}\times\frac{12}{3}\times\frac{12}{2}\times\frac{12}{1},$$

$$\Rightarrow(1\times2\times3\times4\times6\times12)^2=12^6\ (\text{这里 } k=6).$$

例 3 证明：若正整数 n 的全部正约数有奇数个，则 n 为平方数.

证明：由例 2 可知，将 n 的全部正约数从小到大排列 q_1，q_2，…，q_k，q_{k+1}，…，q_{2k+1}（设约数个数为 $2k+1$）. 则与约数$\frac{n}{q_{2k+1}}$，…，$\frac{n}{q_{k+1}}$，$\frac{n}{q_k}$，…，$\frac{n}{q_1}$对应相等. 位于中央的一对是 q_{k+1}，$\frac{n}{q_{k+1}}$，因此 $q_{k+1}=\frac{n}{q_{k+1}}$，于是 $n=q_{k+1}^2$.

习题 1-1

1. 证明：(1) 若 $a|b$，$m\neq 0$，则 $ma|mb$；

(2) 设 a，b 为正整数，$a|b$ 且 $b|a$，则 $a=b$.

2. 证明：三个连续正整数之和是 3 的倍数.

3. 证明：若 $6|(a+b)$，则 $6|(a^3+b^3)$.

4. 设 n 为正整数，证明 $6|[n(n+1)(2n+1)]$. （提示：$2n+1=(n+2)+(n-1)$）

5. 15 位校友聚会，能否每个人都握手 5 次？

6. 设 $n>1$，$(n-1)|(n+11)$，求 n. （提示：将 $n+11$ 表为 $(n-1)+12$）

1.2 素数与合数

同学们知道，2，3，5，7，11，13，17，19，…除去 1 和自身外，不能被其他整数整除，这类大于 1，而且正约数只有 1 和自身的整数叫做素数. 素数也称为质数. 要特别注意，1 不是素数. 如果大于 1 的整数不是素数，则称其为合数. 研究素数是数论的核心内容之一.

素数在自然数中的分布很不规律，有时隔一个数就有一个素数，如 3，5；有时隔三个数有一个素数，如 19，23. 有的相邻两素数相隔很远，寻找素数和判别一个数是否为素数是很艰难的. 下面的定理给出了一个寻找素数的有效算法.

定理 1 设 a 是任一大于 1 的整数，则 a 的除 1 以外的最小正约数 q 必是素数. 当 a 是合数时，$q\leqslant\sqrt{a}$.

证明：用反证法. 设 q 不是素数，由 $q>1$ 知 q 是合数. 由此可知存在 q 的正约数 q_1，使 $1<q_1<q$. 由 $q_1|q$，$q|a$，可得 $q_1|a$，这与 q 是 a 除 1 以外的最小正约数矛盾.

当 a 是合数时，设 $a=a_1q$，其中 q 是 a 的大于 1 的最小正约数. 则 $a_1\geqslant q$，故 $q^2\leqslant a$，即 $q\leqslant\sqrt{a}$.

由定理 1 知，对于每一个合数 n，存在素数 p，使 $p|n$，且 $p\leqslant\sqrt{n}$. 由此可得出找出不超过 N 的全体素数的方法：

先找出不超过$\sqrt{N}$的全体素数，且按大小顺序排列

$$2=P_1<P_2<\cdots<P_S\leqslant\sqrt{N}.$$

然后把大于 1，且不超过 N 的自然数按大小顺序排列

$$2,3,\cdots,N. \tag{1}$$

在(1)中留下 $P_1=2$，而把 P_1 的倍数全部划掉. 再留下

$P_2=3$，而把 P_2 的倍数全部划掉. 继续这一手续，直到最后留下 P_S，而把 P_S 的倍数全部划掉. 留下的就是不超过 N 的全体素数. 这种寻找素数的方法，称为厄拉多塞筛法.

例如，为寻求 100 以内的全体素数，先找出不超过 $\sqrt{100}=10$ 的全体素数：

2，3，5，7.

把从 2 到 100 的数按大小排列，把 2，3，5，7 留下，再先后划掉 2，3，5，7 这四个数的倍数，剩下的就是 100 以内的全部素数.

判断一个正整数 a 是否为素数，原则上要用不超过 $\sqrt{a}$ 的素数逐个试除. 对较小的数 a，工作量不是很大. 例如，$a=97$，你会一眼看出它是素数，因为 97 不是 2，3，5，7 的倍数. 又如 $a=191$，$\sqrt{a}<14$，容易看出，191 不是 2，3，5，7，11，13 的倍数，因此 191 是素数.

现在提出一个问题，素数究竟只是有限多个呢？还是有无穷多个？

定理 2 素数有无穷多个.

证明：用反证法. 假设自然数中只有有限多个素数，不妨记为 P_1，P_2，…，P_k. 考虑整数 $N=P_1P_2\cdots P_k+1$. 由 $N>1$ 及定理 1 知存在素数 $P\mid N$. 此时必有 $P\neq P_i$，$1\leqslant i\leqslant k$，否则 $P\mid 1$. 所以 P 是上述 k 个素数以外的素数. 这导出矛盾. 所以素数有无穷多个.

习题 1-2

1. 判断 359 是不是素数.
2. 利用厄拉多塞筛法找出 100 以内的全体素数.
3. 找出 5 个连续自然数，每个数都是合数.
4. 证明：大于 11 的自然数可以表示成两个合数之和.（提示：分奇、偶数考虑）

1.3 带余除法

同学们都会做整数除法，例如 $201\div 13$，得到整数商

15，余数 6. 我们可以用除数、商和余数还原被除数：$201=13\times15+6$. 这就是带余除法，一般地，带余除法表述为如下定理.

定理 1 设 a，b 是两个整数，其中 $b>0$，则存在惟一的一对整数 q 及 r，使

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

证明：存在性 作整数序列

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

则 a 或者等于这个序列的某一项，或者在某相邻两项之间，即存在整数 q，使

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

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

惟一性 设 q_1，r_1 是满足(1)式的另一对整数，则有

$$bq_1+r_1=bq+r,$$

于是有

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

及

$$b|q-q_1|=|r_1-r|.$$

因为 r 和 r_1 都是小于 b 的非负整数，所以 $0\leqslant|r_1-r|<b$. 但 $b\mid|r_1-r|$，故有 $|r_1-r|=0$. 因此 $r=r_1$，$q=q_1$.

思考与讨论

如果定理 1 中的条件 $b>0$ 改成 $b\neq0$，定理 1 应做怎样的修改？

例 写出 a 被 b 除的带余除法表示式：

(1) $a=255$，$b=15$；　　(2) $a=-81$，$b=15$.

解：(1) $255=15\times17+0$；

(2) $-81=15\times(-6)+9$.

注意，虽然 $-81=15\times(-5)-6$，$-81=15\times(-7)+24$ 也成立，但它们都不是带余除法表达式，因为不满足余数条件：$0\leqslant r<b$.

同学们知道，十进制数

$$a_na_{n-1}\cdots a_1a_0=a_n\times10^n+a_{n-1}\times10^{n-1}+\cdots+a_1\times10+a_0.$$

其中 a_n，a_{n-1}，…，a_1，a_0 在 0，1，2，…，9 中取值($a_n\neq 0$，$n>0$)．例如 $4\ 376=4\times 10^3+3\times 10^2+7\times 10^1+6$.

我们平常所用的数都是十进位的，现在计算机上用的数是 2，8 及 16 进位的，下述结论表明自然数可以表示成任意 $q(>1)$进制数.

设 q 是大于 1 的整数，则任意自然数 n 可表示为

$$n=c_mq^m+\cdots+c_1q+c_0, \tag{2}$$

其中 $m\geqslant 0$，$0\leqslant c_i<q$，$0\leqslant i\leqslant m$，$c_m\neq 0$．对于给定的 q，这种表示方法是惟一的.

(2) 式称为 n 的 q 进制表示.

例如，运用带余除法，可将十进制数 101 分别表为 2 进制数和 8 进制数：

$$101=2^6+2^5+2^2+1=(1100101)_2,$$

$$101=8^2+4\times 8+5=(145)_8.$$

在十进制中，数字符号有 10 个：0，1，2，…，9．在二进制中，数字符号只有 2 个：0，1．在 q 进制中，数字符号有 q 个：0，1，2，…，$q-1$.

将 q 进制数化为 10 进制数，可按公式(2)直接计算．将 10 进制数化为 q 进制数的方法如下：设 a 为 10 进制数，用 q 去除 a，余数就是右起第一位数．将商除以 q 的余数，得到右起第二位数．如此继续，直到商小于 q 为止.

习题 1-3

1. 写出 $-1\ 999$ 被 17 除的带余除法表示式.
2. 请在 503 后面添加 3 个数字，使所得的 6 位数能被 7，9，11 整除.
3. 将 101 表成 3 进制数.
4. $5\times 6=42$ 是什么进制的乘法？

1.4 辗转相除法与最大公约数

本节讲述辗转相除法，此方法在本书中有重要的应用.

在我国古代的著名数学著作《九章算术》里就有了辗转相除法，书中把此方法叫做“更相减损术”.

对整数 $a>0$，$b>0$ 反复运用带余除法，可得下列等式

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

由于 $b>r_1>r_2>\cdots$，故经过有限次带余除法后，最终总可以得到一个余数是零的带余除法表达式，即(1)中最后一式，其中 $r_{n+1}=0$.

(1) 式所指出的计算方法叫辗转相除法，也称欧几里得算法.

例如，$a=361$，$b=93$，做辗转相除：

$$\begin{aligned}
&361=93\times3+82,\\
&93=82\times1+11,\\
&82=11\times7+5,\\
&11=5\times2+1,\\
&5=1\times5.
\end{aligned}$$

又如，$a=-360$，$b=93$，做辗转相除：

$$\begin{aligned}
&-360=93\times(-4)+12,\\
&93=12\times7+9,\\
&12=9\times1+3,\\
&9=3\times3.
\end{aligned}$$

由(1)式可知，

$$\begin{aligned}
r_1&=a-q_1b,\\
r_2&=b-r_1q_2=b-(a-q_1b)q_2\\
&=-q_2a+(1+q_1q_2)b.
\end{aligned}$$

一步一步计算下去，总可以得到 r_n 关于 a，b 的表达式：

$$r_n=pa+qb,$$

其中 p，q 为整数. 如何求出 p，q 呢？下面的定理给出了一个递推算法.

定理 1 设 a，b 是任意两个正整数，并进行了辗转相除法(1)式，则有

$$Q_ka-P_kb=(-1)^{k-1}r_k,\ 1\leqslant k\leqslant n.\tag{2}$$

其中 $\begin{cases} P_0=1,\ P_1=q_1,\ P_k=q_kP_{k-1}+P_{k-2}, \\ Q_0=0,\ Q_1=1,\ Q_k=q_kQ_{k-1}+Q_{k-2}, \end{cases} 2\leqslant k\leqslant n.$

证明：对 k 使用数学归纳法. 由(1)式知 $a=bq_1+r_1$，可写成 $Q_1a-P_1b=(-1)^{1-1}r_1$. 同样由(1)式可得

$$\begin{aligned} b &= r_1q_2+r_2 \\ &= (a-bq_1)q_2+r_2, \end{aligned}$$

即 $$q_2a-(q_1q_2+1)b=-r_2,$$

可写成 $$Q_2a-P_2b=(-1)^{2-1}r_2.$$

故当 $k=1$，2 时，(2) 式成立. 以下可设 $n\geqslant 3$.

现在设定理对$(k-1)$，$k(2\leqslant k\leqslant n-1)$成立. 下证定理对$(k+1)$成立.

由 $r_{k-1}=r_kq_{k+1}+r_{k+1}$和归纳假设可得

$$\begin{aligned} r_{k+1} &= r_{k-1}-r_kq_{k+1} \\ &= (-1)^{k-2}(Q_{k-1}a-P_{k-1}b)- \\ &\quad (-1)^{k-1}(Q_ka-P_kb)q_{k+1}, \end{aligned}$$

于是有

$$\begin{aligned} (-1)^kr_{k+1} &= Q_{k-1}a-P_{k-1}b+q_{k+1}Q_ka-q_{k+1}P_kb \\ &= (q_{k+1}Q_k+Q_{k-1})a-(q_{k+1}P_k+P_{k-1})b \\ &= Q_{k+1}a-P_{k+1}b. \end{aligned}$$

注：在定理 1 的证明中使用了下述形式的数学归纳法：

设 $f(n)$是关于自然数 n 的一个命题，如果 (1) 当 $n=1$，2 时，$f(1)$，$f(2)$成立. (2) 设 $k\geqslant 2$. 如假设 $f(k-1)$，$f(k)$成立，推出 $f(k+1)$成立. 那么，$f(n)$对所有正整数 n 成立.

下面我们用辗转相除法求最大公约数. 先考虑两个实际问题：

(1) 一个地面面积为 3.6 m×5.6 m 的房间，假设不计缝隙和不剪裁地板砖，问最大能用边长是多少厘米的正方形地板砖铺地?

不难想出所需边长就是 360 cm 与 560 cm 的公约数中的最大数.

(2) 某超市销售某种货物，去年总收入为 36 963 元，今年每件货物的售价不变，总收入 59 570 元. 如果单价(元) 是大于 1 的整数，问今年和去年至少各售出这种货物多少件?

回答这个问题，关键要知道货物可能的最高单价，它

就是 36 963 元与 59 570 元的公有约数中的最大数.

定义 设 a_1，a_2，…，a_k 是不全为零的整数. 如整数 d 是每一个 $a_i(1\leqslant i\leqslant k)$的约数，则称 d 为 a_1，a_2，…，a_k 的公约数. a_1，a_2，…，a_k 的公约数中最大的一个，称为这 k 个数的最大公约数，记为$(a_1, a_2, \cdots, a_k)$. 当 $(a_1, a_2, \cdots, a_k)=1$ 时，称 a_1，a_2，…，a_k 为互素. 特别当 a_1，a_2，…，a_k 中的任何两个数都互素时，称 a_1，a_2，…，a_k 为两两互素.

由于整数 a 与 $|a|$ 的约数相同，故有

$$(a_1,a_2,\cdots,a_k)=(|a_1|,|a_2|,\cdots,|a_k|).$$

因此在以下讨论中可设 $a_i(1\leqslant i\leqslant k)$是正整数.

首先讨论 $k=2$ 的情况.

设 a，b 是两个整数，其中 $b>0$，由带余除法知存在惟一的一对整数 q，r，使 $a=bq+r$，$0\leqslant r<b$，此时有

定理 1 $(a,b)=(b,r)$.

证明：设 $d_1=(a, b)$，$d_2=(b, r)$. 由 $d_1|a$，$d_1|b$ 及 $r=a-bq$ 知 $d_1|r$，故 d_1 是 b，r 的公约数. 因此有 $d_1\leqslant d_2$. 同理可证 d_2 是 a，b 的公约数，故有 $d_2\leqslant d_1$. 于是得到 $d_1=d_2$.

对 a，b 使用辗转相除法，不妨设算式为 §1.4 节的(1)式❶，则有

定理 2 $(a, b)=r_n$.

证明：由定理 1 和算式(1)即得

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

定理 2 给出了求(a, b)的一个具体算法.

例 求(6 409，42 823).

解：因为

$$\begin{aligned}
42\,823&=6\,409\times6+4\,369,\\
6\,409&=4\,369\times1+2\,040,\\
4\,369&=2\,040\times2+289,\\
2\,040&=289\times7+17,\\
289&=17\times17,
\end{aligned}$$

所以

$$(6\,409,\ 42\,823)=17.$$

使用辗转相除法不仅可以实际算出(a, b)，而且可以导出下述的在理论证明中极为重要的裴蜀恒等式.

定理 3 （裴蜀恒等式）任给整数 $a>0$，$b>0$，存在整

注

❶ 为了方便，以下凡对 a，b 使用辗转相除法，都假设算式为 §1.4 节的 (1) 式.

数 m，n，使

$$(a，b)=ma+nb.$$

证明：在 1.4 节定理 1 中取 $k=n$，即得

$$(-1)^{n-1}r_n=Q_na-P_nb.$$

因此

$$(a,b)=[(-1)^{n-1}Q_n]a+[(-1)^nP_n]b.$$

例如，

$$(6，15)=3\times6-1\times15,$$

$$(36，8)=1\times36-4\times8.$$

推论 a，b 的任一公约数是其最大公约数的约数.

定理 4 设 $d|ab$，且$(d，a)=1$，则 $d|b$.

证明：由定理 3 知：使用辗转相除法可求得一对整数 x_0，y_0，使

$$dx_0+ay_0=1,$$

从而

$$(db)x_0+(ab)y_0=b.$$

由 $d|db$，$d|ab$ 及上式得 $d|b$.

定理 5 当 $m>0$ 时，有$(am，bm)=(a，b)m$.

证明：对 a，b 使用辗转相除法，再乘 m，则有

$$am=(bm)q_1+r_1m,$$

$$bm=(r_1m)q_2+r_2m,$$

$$\cdots,$$

$$r_{n-1}m=(r_nm)q_{n+1}.$$

因此

$$(am，bm)=r_nm=(a，b)m.$$

现在讨论一般情况.

下述的定理表明求 k 个数 a_1，a_2，…，a_k($k\geqslant3$)的最大公约数可以由求两个数的最大公约数而逐步求出.

定理 6 设$(a_1，a_2)=d_2$，$(d_2，a_3)=d_3$，…，$(d_{k-1}，a_k)=d_k$，则

$$(a_1，a_2，\cdots，a_k)=d_k.$$

证明：记$(a_1，a_2，\cdots，a_k)=d$. 由 $d_k|a_k$，$d_k|d_{k-1}$，$d_{k-1}|a_{k-1}$，$d_{k-1}|d_{k-2}$即得

$$d_k|a_{k-1}，d_k|d_{k-2}.$$

由此类推，最后可得

$$d_k|a_k,\ d_k|a_{k-1},\ \cdots,\ d_k|a_1.$$

由 d_k 是 a_1，a_2，…，a_k 的公约数知 $d_k \leqslant d$.

另一方面，由 $d|a_1$，$d|a_2$ 可得 $d|d_2$. 由此类推，最后可得 $d|d_k$，因此有 $d \leqslant d_k$. 于是得到 $d=d_k$.

习题 1-4

1. 求(198，252)，(1 008，1 260).
2. 求(1 008，1 260，882，1 134).
3. 证明：对任意的整数 x，y，$(a_1, a_2)=(a_1, a_2+a_1x)=(a_1+a_2y, a_2)$.
4. 证明：当 $(c, a)=1$ 时，有 $(c, ab)=(c, b)$.
5. 证明：当 $(a, b)=1$ 时，有 $(c, ab)=(c, a)(c, b)$.
6. 证明：$\left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right)=1$.
7. 证明：$21n+4$ 与 $14n+3$ 互素.

1.5 最小公倍数

先考虑两个实际问题：

(1) 金星和地球在某一时刻相对于太阳处于某一确定位置. 已知金星绕太阳一周为 225 天，地球绕太阳一周为 365 天，问这两个行星至少要经过多少天才同时回到原来位置?

不难想到所要天数就是 225 与 365 的公有倍数中的最小数.

(2) 排练团体操时，要使队伍排成 10 行，15 行，18 行，24 行，队形都成矩形，问最少需要多少人参加排练?

易知所需人数就是 10，15，18，24 这四个数的公有倍数中的最小者.

定义 设 b_1，b_2，…，b_k 是都不为零的整数，如果整数 d 是每一个 $b_j(1 \leqslant j \leqslant k)$ 的倍数，则称 d 为 b_1，b_2，…，b_k 的公倍数. b_1，b_2，…，b_k 的公倍数中的最小正数，称为这 k 个数的最小公倍数，记为$[b_1, b_2, \cdots, b_k]$.