# 初等数论

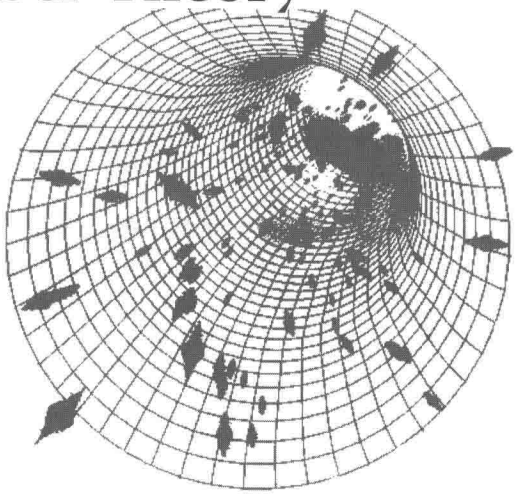
# Elementary Number Theory

张贤科

高等教育出版社

# 初等数论

# Elementary Number Theory



张贤科

高等教育出版社·北京

内容提要

本书是“初等数论”课本，浅易简明，便于快捷入门，视角较新．前四章为课内教材，内容基本．后四章及附录，可选学或参考，内容渐丰．全书涵盖较广，包含：因子分解，同余与同余类，原根与高次同余式，数论函数，二次互反律，不定方程与 Gauss 数，连分数及各种应用，二次数域与代数数，解析方法与素数分布．附录含乐律与连分数，e，π 与超越数定理，有限域，$p$-adic 数，三、四次互反律，椭圆曲线简介，以及数表．书中有较多例题、习题，附有习题解答和提示．

本书是作者基于长期科研和教学及讲课稿，参阅大量文献写就．融入心得感悟，多有评述．

本书适于做各类学校的初等数论教材，可做数学、信息、计算机、电子等科技人员，爱好者和大中学生的参考或自学材料，也为有志于深造的读者奠定现代视角的数论基础．

**图书在版编目（CIP）数据**

初等数论/张贤科编著．--北京：高等教育出版社，2016．9

ISBN 978-7-04-045728-5

Ⅰ．①初… Ⅱ．①张… Ⅲ．①初等数论-高等学校-教材 Ⅳ．①O156．1

中国版本图书馆 CIP 数据核字（2016）第 140812 号

| | | | |
|---|---|---|---|
| 策划编辑 田 玲 | 责任编辑 田 玲 | 特约编辑 张建军 | 封面设计 钟 雨 |
| 版式设计 马敬茹 | 插图绘制 杜晓丹 | 责任校对 张小镝 | 责任印制 毛斯璐 |

| | | | |
|---|---|---|---|
| 出版发行 | 高等教育出版社 | 网 址 | http://www.hep.edu.cn |
| 社 址 | 北京市西城区德外大街 4 号 | | http://www.hep.com.cn |
| 邮政编码 | 100120 | 网上订购 | http://www.hepmall.com.cn |
| 印 刷 | 国防工业出版社印刷厂 | | http://www.hepmall.com |
| 开 本 | 787mm×960mm 1/16 | | http://www.hepmall.cn |
| 印 张 | 21.25 | | |
| 字 数 | 380 千字 | 版 次 | 2016 年 9 月第 1 版 |
| 购书热线 | 010-58581118 | 印 次 | 2016 年 9 月第 1 次印刷 |
| 咨询电话 | 400-810-0598 | 定 价 | 37.30 元 |



物 料 号 45728-00

# 引　言

本书是“初等数论”教本. 主旨在于尽量浅显、初等地引领读者，逐步入门数论，不需要预备知识，不需其他协助. 中学生即可开始学习. 后部分内容逐渐丰富.

前四章是公认基本内容，是教学范围，写得最为初等而简洁. 后四章渐渐丰厚一些.

全书内容全面，涵盖初等数论常有内容. 渐次也稍微介绍采用现代数学的眼光和思想. 后部分(主要在附录)有些特色内容，可供选读参考，带星号内容初学者可略. 有较多的例题和习题，大多附有提示或解答，利于初学入门.

总体而言，学习了前四章即可认为基本掌握了本科初等数论，就可以转入后续学习(例如代数数论等). 当然，后四章有更深层作用. 学完本书，就具有了现代理念下的坚实深厚基础，十分利于后续深造或应用——这里后续学习可指数学各学科(特别是代数数论、解析数论、超越数论、计算数论、代数各学科、代数几何、代数拓扑、表示论、泛函分析、代数编码、信息加密、分析和几何等)和信息、计算机、物理等个学科，应用则更广泛.

本书是基于长期教学科研及讲课稿，参阅大量文献写就，融入了教学科研中的心得感悟和对一些概念方法的看法. 作为教本，为了更贴近课堂教学效果，多数章节后附有注记和评述、警句诗文，以强化读者的理解、印象和兴趣.

本书特色之处，简介如下：

第一章，因子分解，特色是多项式、连分数应用；强调带余除法—辗转相除—最大公因子和 Bézout 等式—唯一分解，这一逻辑链.

第二章，同余，特色是强调同余类集合；强调“孙子分解”，而不只是解同余式.

第三章，原根和高次剩余，特色是引入循环群的概念，易于理解，利于将来；引入 Möbius 反演与数论函数，Dirichlet 卷积.

第四章，二次互反律，尽量简洁，证明比较新.

第五章，不定方程，特色是 Gauss 整数及其性质和使用. 这就渐渐引入近代数学方法，介绍了 Fermat 大定理，弦切律方法.

*第六章，连分数，特色是全面、细腻深入，含逼近、二次数、Pell 方程、超越数与逼近.

*第七章，二次域与代数数，开始很古典，渐渐简洁介绍有关的现代数学若干知识.

*第八章，解析方法，主线是 Euler 乘积，开始很浅，后有 Dirichlet $L$-函数等较深内容.

附录部分：

附录 1，音乐与连分数等，各种乐律的制定和关系原理.

附录 2，e，π 超越性的古典证明，Lindemann-Weierstrass（超越数基本）定理.

附录 3，系统介绍了有限域，对将来学习及到信息领域应用十分有利.

附录 4，介绍了 $p$-adic 数，深化了模算术，又引向现代数学.

附录 5，介绍了三、四次互反律.

附录 6，简要介绍了椭圆曲线、模形式、Fermat 大定理证明、BSD 猜想等.

附录 7，含 3 份相关数表.

数论，既优美又晦涩. 尤其是现代数论，使用了很多高度抽象的代数和代数几何等综合方法. 作者一向鼓励指导青年积极进取，勇攀科学高峰. 最近在教师节，感到 Prometheus（普罗米修斯）盗取天火传授人类，很像老师将科学真理和科学精神，不畏任何艰险地传授给青年. 教师本着这样的精神去教，学生也应本着这样的精神，像盗取天火（勇夺真理）一般地去学. 故作“师法普罗米修斯”（七律·教师节有感）曰：

盗来天火照人间，　暗授神机预知前.
雷电不屈缚崖壁，　鸷鹰恶啄痛胆肝.
何惜一己心血尽，　必使文明薪火传.
千载为师师为谁？　普罗米修斯觉先.

数论，被誉为最纯粹的科学，是“数字化”始祖、“软件”之最，在理论和应用两方面都意义重大. 数学王子 Gauss 有名言：

“数学是科学之女皇，数论是数学之女皇. 她经常屈尊谦和地帮助天文学和所有自然科学，但是无论在哪方面，她都有权高居至尊.”

数论，引古今天下无数英才竞折腰. 到现代，数论相关学科也是获得 Fields 奖和许多大奖最多的学科. 尊严华贵，高高在天. 但有志事竟成，敲门即开门. 作者告这“数论女皇”之情形于志士痴子曰：

瑶池女王绮窗开，　折桂痴子何时来？
未须八骏寻万里，　天门三叩即为开！

张贤科

2016 年 3 月于西丽湖山庄

# 目　录

# 第一章　因子分解

## §1.1　整除与带余除法

开辟鸿蒙，先有数一．一加一为二，二加一为三．如此继续，生出自然数．**自然数** 1，2，3，…的集合记为$\mathbb{N}$. 这是人类智慧知识的发源家园．自然数集合$\mathbb{N}$内部，数之间可加可乘，但相减则不一定可行．

随着人类智慧渐开，人们逐渐承认 0 是“数”，又承认 $0-1=2-3=3-4$，$0-2=1-3=2-4$ 等为“数”，记为 $-1$，$-2$ 等；它们与自然数一起合称为**整数**(integers)．整数的集合记为$\mathbb{Z}$(源自德文 Zahlen)，即

$$\mathbb{Z}=\{\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \cdots\}.$$

整数集合$\mathbb{Z}$内部，整数之间可以相加、相减、相乘，且其结果(分别称为和、差、积)仍然是整数．此性质被称为**整数集合$\mathbb{Z}$对加、减、乘运算是封闭的**．注意，整数集合$\mathbb{Z}$对除法不封闭(例如除法 $3\div 2$ 在$\mathbb{Z}$中不能进行，或者说在$\mathbb{Z}$中无结果)．也因此之故，“整数的除法”就成为一个需要人类探讨的问题．

**定义 1**(整除)　设 $a$，$b$ 均为整数，$b\neq 0$. 若存在整数 $q$ 使得

$$a=bq,$$

则称 $b$ **整除** $a$，记为 $b\mid a$(即 $b$ divides $a$)；且称 $b$ 是 $a$ 的**因子**(factor，divisor)，$a$ 是 $b$ 的**倍数**或**倍**(multiple)．也可记为 $a\div b=q$，称 $a$ 是被除数，$b$ 是除数，$q$ 是商．(反之，如果不存在整数 $q$ 使得 $a=bq$，则称 $b$ 不整除 $a$，记为 $b\nmid a$.)

例如：$2\mid 6$，$(-2)\mid 6$，$(-2)\mid(-6)$，$1\mid 7$，$(-1)\mid 7$，$7\mid 7$，$7\mid 0$.

注意，任意非零整数 $b$ 整除 0，因为 $0=b\cdot 0$(但是，约定永不用 0 做除数)．整除性有如下简单性质(读者自证之)：

(1) 若 $b\mid a$ 且 $a\mid b$，则 $a=\pm b$.　　(2) 若 $a\mid b$，$b\mid c$，则 $a\mid c$.

(3) $a\mid b$ 当且仅当 $ac\mid bc(c\neq 0)$.　　(4) 若 $b\mid a_1$ 且 $b\mid a_2$，则 $b\mid a_1\pm a_2$.

设 $p\neq\pm 1$ 为非零整数，而 $p$ 的正因子只有 1 和 $p$，则称 $p$ 为**素数**(prime number)．例如，2，3，5，7 和 $-2$，$-3$ 都是素数．不是素数或 $\pm 1$ 的整数称为**合数**(composite number)．例如，4，6，$-6$ 都是合数．

换句话说，**素数是不可分解的**(即若素数 $p=bc$，则必然 $b=\pm1$ 或 $c=\pm1$)．而**合数可分解**，即合数 $a$ 可写为 $a=bc$(其中 $b$，$c\neq\pm1$；或者说 $b$，$c\neq\pm a$)．注意，若 $p$ 为素数，则 $-p$ 也是素数．故一般只考虑正素数．1 不是素数．小于 100 的正素数为

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$
$$43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

更多的素数见附录 7. 将证明，素数有无限多个．以 $\pi(x)$ 记不超过正数 $x$ 的正素数个数，则 $\pi(x)$ 与 $x/\ln x$ 近似(素数定理)，即二者比值趋于 1(当 $x$ 趋于无穷大．这里 $e=2.718\ 28\cdots$ 是自然对数 $\ln x$ 的底)．

**引理 1**(因子分解)　任一整数 $n(\neq0,\ \pm1)$可写为有限个素数之积．

**证明**　只需对自然数 $n$ 证明．用数学归纳法．首先，对 $n=2$，引理显然成立(此称为归纳起点)．假设对任意固定的自然数 $n>2$，引理对小于 $n$ 的自然数均成立(此称为归纳法假设)；现需要证明引理对 $n$ 成立(此为归纳法关键步骤)．(i) 若 $n$ 是素数，自然是一个素数之积，引理对 $n$ 成立．(ii) 若 $n$ 不是素数，则可写为 $n=mq$，其中 $m$，$q$ 为小于 $n$ 的自然数，由归纳法假设可知，$m$，$q$ 均为有限个素数之积，可写为 $m=p_1\cdots p_s$，$q=p_{s+1}\cdots p_t$，二者相乘，可知$n=mq=p_1\cdots p_sp_{s+1}\cdots p_t$为有限个素数之积，故引理对 $n$ 成立．证毕．　□

**说明**　数学归纳法(的有效性)是基于“自然数集的每个非空子集都含有最小数”(这称为自然数的**良序性**)．事实上，假若经过数学归纳法证明后定理仍对某些自然数不成立，则不满足定理的自然数子集合必含最小数(据自然数的良序性)，记为 $n_0$．因为 $n_0$最小，所以对小于 $n_0$的自然数定理都成立．而我们在数学归纳法的关键步骤中已经证明了：“假设定理对小于 $n_0$的自然数均成立，则定理对 $n_0$成立”，故矛盾．此矛盾表明了数学归纳法的有效性．

引理 1 中“$n$ 写为素数之积”被称为 $n$ 的**(素)因子分解**，或**析因**(factorization)．以后，我们会证明这种分解是唯一的，称为“唯一析因”．常约定“1 是 0 个素数之积”．

**定理 1**(**带余除法**，Euclid(欧几里得)除法，Euclidean division)　*若 $a$，$b$ 均为整数，$b\neq0$，则存在整数 $q$ 和 $r$ 使得*

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

*且 $q$ 和 $r$ 是唯一的．*

**说明**　定理 1 中的 $r$ 称为**余数**(remainder)，$q$ 称为不完全商(quotient)．当

$b>0$ 时，带余除式可改写为

$$\frac{a}{b}=q+\frac{r}{b},\quad 0\leqslant\frac{r}{b}<1.$$

可见 $q=\left\lfloor\frac{a}{b}\right\rfloor$ 是$\frac{a}{b}$的**整数部分**，即不超过$\frac{a}{b}$的最大整数.

**证明** 先设 $b>0$，取 $q=\left\lfloor\frac{a}{b}\right\rfloor$，令 $r=a-bq$，则得 $a=bq+r$. 也可考虑整数序列

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

(这些整数将实数轴分割为无限多个长为 $b$ 的小段，则 $a$ 必落在某小段之中，设落在 $qb$ 与$(q+1)b$ 之间). 则必存在整数 $q$ 使

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

令 $r=a-qb$(即 $a$ 到小段左端点的距离)，则得到带余除式 $a=bq+r$ 且 $0\leqslant r<b$.

当 $b<0$ 时，则 $b'=-b>0$，故有 $a=(-b)q'+r$ 且 $0\leqslant r<(-b)$. 令 $q=-q'$，则化为$a=(-b)(-q)+r=bq+r$ 且 $0\leqslant r<|b|$.

现证 $q$ 和 $r$ 是唯一的. 假若 $a=bq+r=bq_1+r_1$. 相减得到 $b(q-q_1)=r_1-r$. 若 $q-q_1\neq 0$，则 $|r_1-r|=|b(q-q_1)|\geqslant|b|$，矛盾(因 $0\leqslant r,\ r_1<|b|$). 所以 $q=q_1$，从而 $r=r_1$. □

定理 1 中的余数 $r$ 满足 $0\leqslant r<|b|$，称为**最小非负(剩)余数**. 我们也可以要求余数 $r'$满足$-|b|/2<r'\leqslant|b|/2$，称为**绝对(值)最小(剩)余数**.

**评述** L. Kronecker(克罗内克，1823—1891)有名言："上帝创造了自然数，其余的一切皆是人为(God made natural numbers; all else is the work of man)." 然而，整数集$\mathbb{Z}$ 才是数论的首个良好用武之地. $\mathbb{Z}$ 对加、减、乘法封闭(因而称为环). 整数的除法常遗留余数(带余除法)，这是整数集的最重要性质(因而称为 Euclid 环)，它可推导出整数许多其他性质.

整数的这些性质，在两千多年前古希腊即已发现，例如在 Euclid 的 *Elements*(《几何原本》)中. 但至今鲜亮夺目、意义非凡. 论数者单道这"整数之奇妙"曰：

开辟鸿蒙先有一，　一生二三整数集.
加减乘法皆封闭，　除法有遗生传奇.

## 习 题 1.1[①]

1. 证明：(1) 设 $n^2=4q+r$，则 $r=0$ 或 1(即平方数除以 4 余 0 或 1).

(2) 若 $n$ 为奇数，则 $n^2=8q+1$，$q\in\mathbb{Z}$.

2. 证明：(1) 若 $b\mid a$ 且 $a\mid b$，则 $a=\pm b$.

(2) 若 $a\mid b$，$b\mid c$，则 $a\mid c$.

(3) $a\mid b$ 当且仅当 $ac\mid bc(c\neq 0)$.

3. 设 $b\mid a_i$，证明：$b\mid k_1a_1+\cdots+k_sa_s$(对任意 $k_i(i=1,\ \cdots,\ s)$).

4. 设 $a+b=c$. 试证明：若 $d$ 整除 $a$，$b$，$c$ 三者中之二，则必整除第三者.

5. 设 $a$，$m$，$n$ 为正整数，$n\mid m$，证明：$(a^n-1)\mid(a^m-1)$.

6. (1) 证明：$3\mid n(4n+1)(5n+1)$.

(2) $a$，$b$ 满足何条件时，$3\mid n(an+1)(bn+1)$对任意整数 $n$ 成立?

*7. 设 $M$ 是一些整数构成的非空集合，对加、减法封闭(例如偶数全体. 再如 $4x+6y$ 全体($x$，$y$ 遍历整数)). 设 $d$ 是 $M$ 中最小正整数，求证：$M$ 恰为 $d$ 的倍数全体.

8. ($m$ 进($m$-adic)表示)设正整数 $m\geqslant 2$，则每个正整数 $a$ 可唯一表示为

$$a=a_0+a_1m+a_2m^2+\cdots+a_sm^s,$$

其中 $0\leqslant a_i\leqslant m-1$，$a_i$和 $s$ 为非负整数.

## §1.2 辗转相除与 Bézout 等式

**定义 1**(最大公因子) 设 $a$，$b$ 为整数，若有整数 $d$ 满足：(1) $d$ 是 $a$ 和 $b$ 的公因子；(2) $a$ 和 $b$ 的任意公因子都是 $d$ 的因子，则称 $d$ 是 $a$ 和 $b$ 的一个**最大公因子**(greatest common divisor，简写为 gcd).

最大公因子的存在性将在下面证明. 现在看它的唯一性(除非相差正负号)：若 $d$ 和 $d'$都是 $a$ 和 $b$ 的最大公因子，则应 $d'\mid d$ 且 $d\mid d'$，从而 $d=d'q$，$d'=dr=d'qr$，$1=qr$，$q=\pm 1$，故 $d'=\pm d$. 故 $a$ 和 $b$ 的正的最大公因子 $d$ 是唯一的，以 $(a,\ b)$或$\gcd(a,\ b)$记之. 例如$(4,\ 6)=2$，$(-4,\ 6)=2$，$(4,\ 0)=4$.

当最大公因子$(a,\ b)=1$时，称 $a$ 与 $b$ **互素**(relatively prime，coprime).

易知$(a,\ b)=(a-b,\ b)=(a-2b,\ b)=(a-qb,\ b)$，故有：

① 注：字母均表示整数，除非特殊说明.

**定理 1** 若 $a=bq+r$，其中 $a$，$b$，$r$ 为整数（$a$，$b$ 不全为 0），则

$$(a,\ b)=(r,\ b).$$

**证明** 只需证明等式左、右互相整除（因均为正整数）. 首先，$(a,\ b)$ 整除 $a$ 和 $b$，从而也整除 $r=a-bq$，故 $(a,\ b)$ 是 $b$ 和 $r$ 的公因子，所以 $(a,\ b)$ 整除 $(r,\ b)$（因为 $(r,\ b)$ 是最大公因子）. 反之，同样可证明 $(r,\ b)$ 整除 $(a,\ b)$. □

定理 1 说明，余数 $r$ 可做原数 $a$ 的“替身”去求最大公因子. 我们又可找 $b$ 的替身 $r_1$ 代替 $b$，等等. 如此继续，就是著名的**辗转相除法**（Euclidean algorithm）：

$$\begin{aligned}
&a=bq_0+r_1, && 0<r_1<|b|,\\
&b=r_1q_1+r_2, && 0<r_2<r_1,\\
&r_1=r_2q_2+r_3, && 0<r_3<r_2,\\
&\cdots\cdots\\
&r_{s-2}=r_{s-1}q_{s-1}+r_s, && 0<r_s<r_{s-1},\\
&r_{s-1}=r_sq_s \quad (r_{s+1}=0). &&
\end{aligned}$$

其中不完全商 $q_i$ 和余数 $r_i$ 都是逐步唯一确定的（可记 $b=r_0$，$a=r_{-1}$）. 因为非负余数 $r_0$，$r_1$，$r_2$，…逐步减小，终会为零，故可设 $r_{s+1}=0$，即 $r_s\mid r_{s-1}$. 从前向后看，即得最大公因子

$$d=(a,\ b)=(r_1,\ b)=(r_1,\ r_2)=\cdots=(r_{s-1},\ r_s)=r_s.$$

**定理 2** 任意两整数 $a$，$b$（$b\neq 0$）的正最大公因子 $d=(a,\ b)$ 是唯一存在的，即 $d=r_s$（是 $a$ 与 $b$ 辗转相除的最后非零余数）. 而且存在整数 $u$，$v$ 使

$$ua+vb=d$$

（Bézout（贝祖）等式，Bézout's identity）.

**证明** 只需证 Bézout 等式：从后向前看辗转相除诸式. 首先有

$$r_s=r_{s-2}-r_{s-1}q_{s-1}.$$

而再前一式为 $r_{s-1}=r_{s-3}-r_{s-2}q_{s-2}$，以此 $r_{s-1}$ 代入上式，可知 $r_s$ 是“$r_{s-2}$ 和 $r_{s-3}$ 的整数倍之和”. 再前推一式以 $r_{s-2}$ 代入，可得 $r_s$ 是“$r_{s-3}$ 和 $r_{s-4}$ 的整数倍之和”. 由此不断上推，最终可得 $r_s$ 是“$a$ 与 $b$ 的整数倍之和”，即得 Bézout 等式. □

**系 1** 两整数 $a$，$b$ 互素当且仅当存在整数 $u$，$v$ 使

$$ua+vb=1\ (\text{Bézout 等式}).$$

**证明** 若 $ua+vb=1$，因 $(a,\ b)$ 整除 $a$ 与 $b$，故整除右边的 1，从而 $(a,\ b)=1$.

反之，若$(a, b)=1$，则由定理 2 知 $ua+vb=1$ 成立． □

定理 2 和系 1 中的 $u$，$v$ 称为 Bézout 系数，不是唯一的．可以递归求出．将在习题 1.4 的 6，7 等习题和连分数等处进一步讨论．

**系 2** 设 $a$，$b$ 为整数，$(a, b)=d$. 则

$$\{am+bn \mid m, n\in\mathbb{Z}\}=\{dk \mid k\in\mathbb{Z}\}.$$

**说明** 常将$\{am+bn \mid m, n\in\mathbb{Z}\}$简记为 $a\mathbb{Z}+b\mathbb{Z}$ 或$(a, b)$. 故上式也可记为

$$a\,\mathbb{Z}+b\,\mathbb{Z}=d\,\mathbb{Z}, \quad \text{或} \quad (a, b)=(d).$$

**证明** $am+bn$ 显然是 $d$ 的倍数．另一方面，由 Bézout 等式知 $d=ua+vb$，故

$$kd=kua+kvb=ma+nb.$$ □

系 2 表明，由 $xa+yb=c$ 只能得出$(a, b) \mid c$. 另外注意，Bézout 等式的系数 $u$，$v$ 不是唯一的，例如 $d=ua+vb=(u-2b)a+(v+2a)b$.

任意 $s$ 个非零整数 $a_1$，…，$a_s$的最大公因子 $d$ 可类似 $s=2$ 情形定义，即定义 $d$ 满足

(1) $d \mid a_i(i=1, \cdots, s)$； (2) 若 $\delta \mid a_i(i=1, \cdots, s)$，则 $\delta \mid d$.

显然 $a_1$，…，$a_s$的两个最大公因子可互相整除，故最多相差正负号，其中正的最大公因子记为$(a_1, \cdots, a_s)$或 $\gcd(a_1, \cdots, a_s)$. 若$(a_1, \cdots, a_s)=1$，则称 $a_1$，…，$a_s$互素(读者注意这与“$a_1$，…，$a_s$两两互素”的区别).

**定理 3** *任意 $s$ 个非零整数 $a_1$，…，$a_s$的正最大公因子 $d=(a_1, \cdots, a_s)$存在且唯一，且*

$$(a_1, \cdots, a_{s-1}, a_s)=((a_1, \cdots, a_{s-1}), a_s).$$

*而且存在整数 $u_1$，…，$u_s$使得*

$$u_1a_1+\cdots+u_sa_s=d \quad \text{(Bézout 等式)}.$$

**证明** 由最大公因子定义可知，$(a_1, \cdots, a_s)$整除 $a_i(i=1, \cdots, s)$，从而整除 $(a_1, \cdots, a_{s-1})$ 与 $a_s$，从而整除$((a_1, \cdots, a_{s-1}), a_s)$. 同理可知$((a_1, \cdots, a_{s-1}), a_s)$整除$(a_1, \cdots, a_s)$. 因二者均为正整数，故相等．由此等式可归纳地得出，3 个，4 个，…，任意 $s$ 个整数 $a_1$，…，$a_s$的最大公因子 $d$ 是存在的．假设 $s-1$ 个整数情形的 Bézout 等式成立，设为

$$u_1a_1+\cdots+u_{s-1}a_{s-1}=(a_1, \cdots, a_{s-1}),$$

则应存在整数 $u$，$v$ 使得

$$\begin{aligned} d&=(a_1, \cdots, a_{s-1}, a_s)=((a_1, \cdots, a_{s-1}), a_s)=u(a_1, \cdots, a_{s-1})+va_s \\ &=u(u_1a_1+\cdots+u_{s-1}a_{s-1})+va_s=uu_1a_1+\cdots+uu_{s-1}a_{s-1}+va_s, \end{aligned}$$

这就得到 $s$ 个整数情形的 Bézout 等式. □

**例 1**(秦九韶：大衍求一术) 求解方程 $65x+83y=1$.

作辗转相除反复推演(大衍)得

$$83=65\cdot 1+18,\ 65=18\cdot 3+11,\ 18=11+7,\ 11=7+4,\ 11=4\cdot 2+3,\ 4=3+1.$$

最后得非零余数 $d=1$(大衍求索最终得到一). 再从后往前推演诸式，得

$$\begin{aligned}1&=4-3=4-(11-4\cdot 2)=3\cdot 4-11=3\cdot(11-7)-11=2\cdot 11-3\cdot 7\\&=2\cdot 11-3\cdot(18-11)=5\cdot 11-3\cdot 18=5\cdot(65-3\cdot 18)-3\cdot 18\\&=5\cdot 65-18\cdot 18=5\cdot 65-18\cdot(83-65)=23\cdot 65-18\cdot 83,\end{aligned}$$

即得到 Bézout 等式 $1=23\cdot 65-18\cdot 83$. 故得原方程的解 $x=23$, $y=-18$.

**例 2** $(ak,\ bk)=(a,\ b)k$; $(a/\delta,\ b/\delta)=(a,\ b)/\delta$(这里设 $\delta$ 是 $a$ 和 $b$ 的正公因子，$k$ 为正整数，$a$，$b$ 是不全零的整数). 特别可知，当 $d=(a,\ b)$ 时，$(a/d,\ b/d)=1$.

**解** 将所有的整数都放大 $k$ 倍，则它们之间的整除关系是保持的，故若 $a$，$b$ 的最大公因子是 $d$，则 $ak$，$bk$ 的最大公因子为 $dk$. 另外证法是：由 Bézout 等式

$$ua+vb=(a,\ b),$$

得

$$uak+vbk=(a,\ b)k.$$

因 $(ak,\ bk)\mid uak+vbk$，故 $(ak,\ bk)\mid(a,\ b)k$. 因 $(a,\ b)k\mid ak$ 与 $bk$，故 $(a,\ b)k\mid(ak,\ bk)$，从而二者相等. 再由上述可知

$$(a/\delta,\ b/\delta)\delta=(a,\ b),$$

即得

$$(a/\delta,\ b/\delta)=(a,\ b)/\delta.$$

**例 3** 证明：(1) 若 $a\mid bc$，$(a,\ b)=1$，则 $a\mid c$.

(2) 若 $a\mid c$，$b\mid c$，$(a,\ b)=1$，则 $ab\mid c$.

**证明** (1) $ua+vb=1$，$uac+vbc=c$，$a\mid$ 左边，故 $a\mid c$.

(2) 设 $c=bq$. 由 $a\mid c$ 即 $a\mid bq$，以及 $(a,\ b)=1$，由(1)知 $a\mid q$，故 $c=bq=baq_1$，$ab\mid c$. □

**评述** 辗转相除法最早出现于 Euclid 的《几何原本》，故也称为 Euclid 算法(Euclidean algorithm)，是可以追溯到 3 000 年前的古老算法，是求最大公因子的奇妙方法(不需要预先分解因子). 其方法和所得 Bézout 等式，意义深远. 近现代用到现代数论，多项式、欧环、纽结，到天文，历法，乐律，密码和各种算法等不可胜数的理论发展和实际应用中. 中国也独立发现(见于《九章算

术》等），秦九韶谓之“大衍求一术”. 论数者单赞这“辗转相除之妙”曰：

千古神算数辗转，　天地轮回翻大衍.
到底大道归于一，　能推律历规矩天.

## 习　题　1.2[①]

1. 用辗转相除法求最大公因子及其 Bézout 等式：

（1）$d=(648, 525)$.　　（2）$d=(70, 21, 15)$.

2. 证明：（1）$(a, a+k) \mid k$.

（2）若$(a, b)=1$，则$(a+b, a-b)=1$ 或 2.

（3）若$(a, b)=1$，$c \mid (a+b)$，则$(c, a)=(c, b)=1$.

（4）若$(a, b)=1$，$(a, c)=1$，则$(a, bc)=1$.

3. 证明：若$(a, b)=d$，$a \mid c$，$b \mid c$，则 $ab \mid dc$.

4. 证明：若$(a, c)=1$，则$(a, bc)=(a, b)$（这里设整数 $a$，$b$ 不全为零）.

5. 证明：若$(a_i, b_j)=1$（对 $1 \leqslant i \leqslant s$，$1 \leqslant j \leqslant t$），则$(a_1 \cdots a_s, b_1 \cdots b_t)=1$.

6. 设 $a$，$m$，$n$ 为正整数，$m>n$，试求 $d=(a^{2^m}+1, a^{2^n}-1)$.

7. 设 $m$，$n$ 为正整数，试求 $d=(2^m-1, 2^n-1)$.

*8. 设 $a$，$b$ 为正整数，$d=(a, b)$，证明：数集 $S=\{ma+nb\}$（$m$，$n$ 遍历正整数）包含 $d$ 的大于 $ab$ 的所有倍数.

# §1.3　唯一析因定理

**定理 1**（算术基本定理（fundamental theorem of arithmetic），整数唯一析因定理）　任一整数 $n(\neq 0, \pm 1)$ 可写为有限个素数之积，且写法是唯一的（不计素数次序和正负号）. 也就是说，$n$ 可写为

$$n=p_1 p_2 \cdots p_t, \tag{1}$$

其中 $p_1$，$p_2$，…，$p_t$ 为素数.

在定理 1 中，“$n$ 唯一地写为素数之积”被称为 $n$ 的（唯一素）因子分解，或唯一析因（unique factorization）. 将相同的素数因子乘在一起，正负号提到前面，则非零整数 $n$ 的素因子分解可写为

① 注：字母均表示整数，除非特殊说明.

$$n=(-1)^{\varepsilon}p_1^{v_1}p_2^{v_2}\cdots p_r^{v_r}, \tag{2}$$

其中 $p_1$，…，$p_r$为互异正素数，$v_i$是正整数，$\varepsilon=0$ 或 1. $n$ 的因子分解式也可写为

$$n=(-1)^{\varepsilon}\prod_p p^{v_p}, \tag{3}$$

其中 $p$ 遍历正素数，$v_p$是非负整数且只对有限多个 $p$ 取值非零(约定 $p^0=1$. 故上述乘积是有限的). $v_p$也写为 $v_p(n)$或 $\mathrm{ord}_p(n)$，是使得 $p^r \mid n$ 的最大整数 $r$，称为 $n$ 在 $p$ 的**指数**(exponent)或**阶**. 此时记为 $p^{v_p} \| n$，符号 $\|$ 读为**恰整除**.

用这种符号可知：$n \mid m$ 当且仅当 $v_p(n) \leqslant v_p(m)$(对任意正素数 $p$).

**引理 1** (1) 设 $p$ 为素数，且 $p \nmid a$，则$(p, a)=1$.

(2) 设 $p$ 为素数，$a$，$b$ 为整数. 若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$.

**证明** (1) 因$(p, a) \mid p$，故$(p, a)=p$ 或 1. 前者意味着 $p \mid a$，不合条件. 故

$$(p, a)=1.$$

(2) 若 $p \nmid a$，则$(p, a)=1$，有整数 $u$，$v$ 使 $up+va=1$，$upb+vab=b$，$p \mid$ 左边，故 $p \mid b$. □

**定理 1 的证明** 分解的存在性已证(§1.1 引理 1)，现证唯一性. 若有两种分解

$$p_1p_2\cdots p_t=n=q_1q_2\cdots q_s,$$

则

$$p_t \mid q_1q_2\cdots q_s=(q_1q_2\cdots q_{s-1})q_s,$$

由本节引理 1(2)知，若 $p_t \nmid q_s$，则 $p_t \mid q_1q_2\cdots q_{s-1}$. 继而可知，若 $p_t \nmid q_{s-1}$，则 $p_t \mid q_1\cdots q_{s-2}$. 如此继续讨论可知，$p_t \mid q_i$必对某 $i$ 成立，不妨设为 $p_t \mid q_s$(可重排 $q_1$，…，$q_s$的下标顺序). 而因 $q_s$为素数，只有平凡因子，故知 $p_t=\pm q_s$. 从上述两种分解的等式中消去 $p_t=\pm q_s$，得

$$p_1p_2\cdots p_{t-1}=\pm q_1q_2\cdots q_{s-1}.$$

如此继续进行，不断消去素数因子，必会有一方化为$\pm 1$，此时另一方也只能是$\pm 1$，故 $t=s$，$p_i=q_i(i=1, \cdots, t.$ 不计正负号和素数排列顺序). 定理得证.

□

**定义 1**(最小公倍) 设 $a_1$，…，$a_s$为非零整数，若整数 $M$ 是所有 $a_i$的倍数 $(i=1, \cdots, s)$，则称 $M$ 是 $a_1$，…，$a_s$的公倍数. 最小的正公倍数 $M_0$，称为**最小公倍数**(或**最小公倍**，least common multiple，简写为 lcm)，记为$[a_1, \cdots, a_s]$.

**引理 2** (1) 任意公倍数 $M$ 必是最小公倍数 $M_0$的倍数.

(2) $[a_1, \cdots, a_{s-1}, a_s]=[[a_1, \cdots, a_{s-1}], a_s]$.