华章数学译丛

27

Advanced Modern Algebra

高等近世代数

(美) Joseph J. Rotman
伊利诺伊大学 著

章亮 译

机械工业出版社
China Machine Press

华 章 数 学 译 丛

27

Advanced Modern Algebra

高等近世代数

(美) Joseph J. Rotman
伊利诺伊大学 著

章亮 译

机械工业出版社
China Machine Press

本书完整而清晰地介绍了近一个世纪以来代数理论发展的主要成果，涉及群、交换环、模、主理想整环、代数、上同调和表现、同调代数等主题，引领读者沿着代数思想发展的过程，步步深入，逐步掌握近世代数理论．

本书兼具理论的深度和广度，可作为高等院校数学专业学生的教材和自学用书．对于科技工作者来说，本书则是一本极佳的参考书．

本书版权登记号：图字：01-2004-3688

图书在版编目（CIP）数据

高等近世代数/（美）罗特曼（Rotman, J. J.）著；章亮译. -北京：机械工业出版社，2007.1

（华章数学译丛）

书名原文：Advanced Modern Algebra

ISBN 7-111-19160-9

Ⅰ. 高…　Ⅱ. ①罗…　②章…　Ⅲ. 抽象代数　Ⅳ. O153

中国版本图书馆CIP数据核字(2006)第050591号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）

责任编辑：方　敏　迟振春

北京京北制版印刷厂印刷 · 新华书店北京发行所发行

2007年1月第1版第1次印刷

186mm×240mm · 48印张

定价：89.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：(010) 68326294

译 者 序

作者在前言中说："每一代人都应纵览和总结代数学使之服务于到来的时代．"这是作者对本书提出的任务．这本书囊括了近一个世纪以来代数学发展的主要成果，涉及群、环、域、模、代数、范畴和同调等方面的基本理论，并概览当前各主要分支研究的状况．作者有意继承上个时代的经典著作，为我们这个时代的代数学者提供一个合适的起点，本书完成了这一历史任务，无愧于继承者的职责．

作为研究生的代数教材，这样生动的表述是很少见的，也许我们可以从不同的代数著作中学习重要的概念和结果，在逻辑上编织一个理论的体系，然后逐渐领悟到一些思想的萌发和发展的线索，但也可能我们未能觉察出内在的动力而感到茫然．这本书引领我们沿着代数思想发展的线索，步步深入，画出一条埋伏在逻辑之下的红线，这是本书的突出特色，不妨举几个例子．

当我们沿着代数的峭岩向上攀登的时候，一个接着一个的抽象险峰挡在我们前面，也许我们来不及思考代数为什么构造那样多的抽象，书中解释了这个现象——抽象使我们更加经济有效，用抽象建立的定理可以一劳永逸地运用于各种相关的具体场合，不仅如此，抽象还把事物的本质揭示得更为清晰，从而可以轻而易举地证明某些事实．书中令人信服地举出有限群的每个元素的阶有限的例子，使我们领悟到抽象思想产生的内在动力，从而从具体的置换群走到抽象的群，从抽象的群、环、域、模等走到抽象的抽象——范畴．

伽罗瓦理论解决了多项式的根式可解性问题，从根式可解到伽罗瓦群有一条逻辑的长链——难怪伽罗瓦被公认为杰出的天才，书中把正多边形上的对称群和伽罗瓦理论的要素对应起来，生动地阐述了伽罗瓦理论．

学了很多群的知识，也许我们没有想过群到底是什么，书中点出群是描述对称的．难道这没有使我们多少悟出一点群的内涵吗？

纯代数地介入同调使我们十分茫然，书中从拓扑中的边界问题指明了同调理论的起源，使我们多少有些启发．

又例如，由费马最后定理（即费马大定理）引发戴得金环的研究；由罗素悖论导致公理集合论的建立；希尔伯特基定理的非构造性证明，穿插进关于戈丹（Gordan）的趣闻．

只有具备下列三个条件才能写出这样的教材：理论的深度和广度，丰富的教学经验，出色的表达能力．

本书还提供了大量考证：一个术语是怎样得来的，为什么起这个名称，由谁首先使用，例如自由群、自由模、挠群、挠模、同态、同调、同伦、正合、射影幺模群、交错群、环、根理想、辛群、G-理想等；一个定理由谁得到，或由谁得到部分结果，又由谁加以完善，例如凯莱的一个结果起先是正确的，后来却又有疑问了，不禁感叹"智者千虑，必有一失"．这种考证不仅使我们增加了历史知识，纪念那些创立概念和发现定理的杰出人物，而且也使我们从中悟出思想发展的进程，帮助我们明确和记忆一个术语所界定的概念．

作者说他尽量写得详细，感谢作者的巨细靡遗，为此我们可以像聆听作者亲自讲授一样阅读本

书，从而使本书也可以作为极佳的自学教材．

最后，这是一本参考书，“它包含了使用代数的人必须知道的许多通常定理和定义”．当今数学的分支越来越细，大多数代数学者都在某一个分支进行工作，而各个分支不可避免地和代数学的主干相遇，具备这样的一本参考书，是十分有益的．另外，书后的索引可使我们方便地查找有关的术语和结果．

在翻译过程中，参考作者网站（http://www.math.uiuc.edu/～rotman/）上给出的勘误表以及翻译过程中新发现的错误，对译稿进行了修改．

译完本书，译者深切地感到这本书“不仅是一碟开胃小菜，也是一席丰盛大餐”．

本书的翻译得到同济大学叶家琛教授的很多帮助，谨表示衷心的感谢．对于审阅本稿或部分审阅本稿并指出错误的各位一并表示感谢．原著的某些疏漏虽然做了更正，但新的疏漏又会出现，加之译者水平有限，差错之处恳请广大读者指正．

译　者

于同济西苑

前　言

事实上所有的数学分支，如分析学、组合学、计算机科学、几何学、逻辑学、数论和拓扑学都要用到代数．现在每个人都会赞同具备一些线性代数、群和交换环的知识是必需的，这些课题已经在大学课程中作了简介，而本书将在此基础上继续深入研究．

本书可作为研究生一年级的代数教材，但并不仅限于此．它也可作为有志于本领域的高年级研究生的自学用书；本书虽然没有达到学科前沿，然而提供了一个领域中所取得的成就和方法．最后，本书是一本参考书，它包含了使用代数的人必须知道的许多通常定理和定义．因此，本书不仅是一碟开胃小菜，也是一席丰盛大餐．

在我的学生时代，伯克霍夫（Birkhoff）和麦克莱恩（Mac Lane）所著的《A Survey of Modern Algebra》是我的第一本代数课本，范德瓦尔登（van der Waerden）所著的《Modern Algebra》是第二本代数课本．它们都是极好的书（我把本书命名为《Advanced Modern Algebra》以示对他们的敬意）．但自这两本书问世之后，时代已经变迁：伯克霍夫和麦克莱恩的书于1941年问世，范德瓦尔登的书于1930年问世．现在有许多研究方向60年前或者尚未存在，或者它们的重要性还没有被人们所认识，这些新方向包括代数几何、计算机、同调和表示论（麦克莱恩和伯克霍夫曾改写了《A Survey of Modern Algebra》一书，书名为《Algebra》，Macmillan，New York，1967，该版本介绍了范畴方法；范畴论源于代数拓扑，后被格罗滕迪克（Grothendieck）用于改革代数几何）．

对使用本书作为研究生一年级课本的读者和教师说几句话．如果假定每个人都读了我的《A First Course in Abstract Algebra》[㊀]，那么学习本书的先决条件自然就具备了，但这是不现实的．有大量不同的大学课程介绍抽象代数，其中，有许多局限于实数域上的矩阵和向量空间，强调求解线性方程组；而另一些把向量空间建立在任意域上，并包括了若尔当典范型和有理典范型；一些讨论了西罗定理，而另一些没有；一些讲述了有限域的分类，而另一些没有．

为适合具有不同背景的读者，前三章包含了许多熟知的内容，其中只有证明概要．第1章包括算术基本定理、同余、棣莫弗定理、单位根、分圆多项式以及诸如等价关系和在对称群中验证群公理等一些集合论的通常概念．接下来的两章既有熟知的内容，也有不熟知的内容，“新”结果是在初等课程中很少讲到的，有完整的证明，而“老”结果的证明通常是概要的．具体地说，第2章是群论的导引，复习置换、拉格朗日定理、商群、同构定理和群在集合上的作用．第3章是交换环的导引，复习整环、分式域、一元多项式环、商环、同构定理、不可约多项式、有限域以及任意域上的线性代数．读者可以用这些章节的“较老”部分来唤醒自己的记忆（也可以熟悉我所选用的记号）；另一方面，对于那些在早期课程中未曾学过此方面知识的人，这些章节也可以作为学习指导（完整的证明可以在《A First Course in Abstract Algebra》中找到）．这种形式可以使教师根据学生的水平自由地选择合适的讲授起点．我想多数教师会从第2章的中间某处开始，然后在第3章的中间某处继续．这种形式也方便了作者，使我在讨论或证明时回顾那些早期的结果．在随后的章节中

㊀ 中文书名为《抽象代数基础教程》，由机械工业出版社引进出版．——编辑注

证明都是完整的、不省略的.

我力图表达清楚并给出完整的证明，只省略那些确实十分简单的部分，因此教师不必在讲课中面面俱到，学生可以自己阅读课文.

以下是本书后面几章的详细内容.

第 4 章从介绍伽罗瓦理论开始，讨论环和群相互关联的产物——域. 证明一般五次多项式的不可解性和伽罗瓦理论的基本定理及其应用，如证明代数基本定理和伽罗瓦定理——特征 0 的域上的多项式有根式解当且仅当它的伽罗瓦群是可解群.

第 5 章涵盖了有限阿贝尔群（基定理和基本定理）、西罗定理、若尔当-赫尔德定理、可解群、线性群 PSL(2，k) 的单性、自由群、表现和尼尔森-施赖埃尔（Nielsen-Schreier）定理（自由群的子群是自由的）.

第 6 章介绍交换环的素理想和极大理想；高斯定理——R 是 UFD（唯一因子分解整环），则 $R[x]$ 也是 UFD；希尔伯特基定理、佐恩引理在交换代数中的应用（附录中有佐恩引理和选择公理等价性的证明）、不可分性、超越基、吕罗特（Lüroth）定理、仿射簇，包括对不可数代数闭域上的零点定理的证明（第 11 章对任意代数闭域上的簇，给出了零点定理的完整证明）；准素分解；格罗布纳（Gröbner）基. 第 5 章和第 6 章选自《A First Course in Abstract Algebra》中的两章，但多数大学课程中没有包含这两章的内容.

第 7 章介绍交换环上的模（主要证明一切 R-模和 R-映射形成阿贝尔范畴）；范畴和函子（包括积和余积）、拉回和推出、格罗滕迪克群、反向极限和正向极限、自然变换；伴随函子；自由模、投射和内射.

第 8 章介绍非交换环，证明有限除环是交换环的韦德伯恩（Wedderburn）定理，以及作出半单环分类的韦德伯恩-阿廷（Wedderburn-Artin）定理. 用张量积、平坦模和双线性型讨论非交换环上的模. 接着介绍特征标理论，以此证明 p^mq^n 阶有限群是可解群的伯恩赛德（Burnside）定理. 最后介绍多重传递群和弗罗贝尼乌斯（Frobenius）群，证明弗罗贝尼乌斯核是弗罗贝尼乌斯群的正规子群.

第 9 章考察主理想整环（PID）上的有限生成模（推广了前面关于有限阿贝尔群的定理），随后把这些结果应用到域上的矩阵，讨论它的有理典范型、若尔当典范型和史密斯（Smith）正规型（利用史密斯正规型可以计算矩阵的初等因子）. 接着给出 PID 上的投射模、内射模和平坦模的分类. 对 k 是交换环的分次 k-代数的讨论，导出张量代数、中心单代数和布饶尔（Brauer）群、外代数（包括格拉斯曼（Grassmann）代数和二项式定理）、行列式、微分形式和李代数简介.

第 10 章从半直积和群的扩张问题开始介绍同调方法，然后用因子组展示扩张问题的施赖埃尔（Schreier）解，直至舒尔-扎森豪斯（Schur-Zassenhaus）引理. 随后是刻画 Tor 和 Ext 的公理（用导函子证明这些函子的存在性）、若干群的上同调、少量叉积代数和谱序列简介.

第 11 章回到交换环，讨论局部化、整扩张、一般的零点定理（用约翰逊环）、戴得金环、同调维数、如同刻画有限整体维数的诺特局部环那样给出正则局部环的塞尔（Serre）刻画定理、正则局部环是 UFD 的奥斯兰德-布赫斯包姆（Auslander-Buchsbaum）定理.

每一代人都应纵览和总结代数学使之服务于到来的时代.

感谢下列数学家，他们的建议极大地改善了我的初稿：Ross Abraham、Michael Barr、Daniel

Bump、Heng Huat Chan、Ulrich Daepp、Boris A. Datskovsky、Keith Dennis、Vlastimil Dlab、Sankar Dutta、David Eisenbud、E. Graham Evans、Jr.，Daniel Flath、Jeremy J. Gray、Daniel Grayson、Phillip Griffith、William Haboush、Robin Hartshorne、Craig Huneke、Gerald J. Janusz、David Joyner、Carl Jockusch、David Leep、Marcin Mazur、Leon McCulloh、Emma Previato、Eric Sommers、Stephen V. Ullom、Paul Vojta、William C. Waterhouse 和 Richard Weiss.

Joseph Rotman

词　源

索引中 etymology（词源）项指出某种数学术语的出处. 其他数学术语的起源，建议读者参考我的书《Journey into Mathematics》和《A First Course in Abstract Algebra》，它们包含下列术语的词源.

《Journey into Mathematics》

π，代数（algebra），算法（algorithm），算术（arithmetic），完全平方（completing the square），余弦（cosine），几何（geometry），无理数（irrational number），等周（isoperimetric），数学（mathematics），周长（perimeter），极式分解（polar decomposition），根（root），标量（scalar），正割（secant），正弦（sine），正切（tangent），三角学（trigonometry).

《A First Course in Abstract Algebra》

仿射（affine），二项式（binomial），系数（coefficient），坐标（coordinates），系（corollary），次数（degree），因子（factor），阶乘（factorial），群（group），归纳法（induction），拉丁方（Latin square），引理（lemma），矩阵（matrix），模（modulo），正交（orthogonal），多项式（polynomial），拟循环（quasicyclic），9 月（September），随机（stochastic），定理（theorem），平移（translation).

目　录

第1章　相关知识回顾

本章复习数论、单位复根和集合论基础的一些熟知内容，大多数证明只有概要.

1.1　数论

首先讨论数学归纳法. 回顾**自然数**集$\mathbb{N}$是由

$$\mathbb{N}=\{\text{整数 } n: n\geqslant 0\}$$

定义的，即$\mathbb{N}$是一切非负整数的集合. 数学归纳法是基于$\mathbb{N}$的下列性质的一种证明方法：

最小整数公理⊖　*在$\mathbb{N}$的每个非空子集C中都有最小整数.*

假定公理成立则对于任意固定的、可以是负的整数m，每个大于或等于m的整数集合C都有最小整数. 如果$m\geqslant 0$，它就是最小整数公理. 如果$m<0$，则$C\subseteq\{m,m+1,\cdots,-1\}\cup\mathbb{N}$且

$$C=(C\cap\{m,m+1,\cdots,-1\})\cup(C\cap\mathbb{N}).$$

如果有限集$C\cap\{m,m+1,\cdots,-1\}\neq\varnothing$，则它包含一个最小整数，显然该数就是$C$中的最小整数；如果$C\cap\{m,m+1,\cdots,-1\}=\varnothing$，则$C$包含在$\mathbb{N}$中，最小整数公理保证$C$有最小整数.

定义　*自然数p为**素数**，如果$p\geqslant 2$且没有因数分解$p=ab$，其中$a<p,b<p$为自然数.*

命题 1.1　*每个自然数$n\geqslant 2$不是素数就是素数的乘积.*

证明　设C是由一切大于1的、不满足该性质的自然数组成的集合$\mathbb{N}$的子集，要证$C=\varnothing$. 如果C非空，则它含有最小整数，譬如说m. 因$m\in C$，所以m不是素数，从而有自然数a和b使得$m=ab, a<m$和$b<m$. 由于a和b都比m小，而m是C中的最小整数，因此两者都不在C中，所以它们的每一个或者是素数，或者是素数的乘积，由此$m=ab$是素数（至少两个）的乘积，这与m不满足本命题相矛盾. ■

有两种归纳法.

定理 1.2（数学归纳法）　*设m是固定的整数，且对每个整数$n\geqslant m$，$S(n)$是一个命题. 如果*

（ⅰ）$S(m)$真，且

（ⅱ）$S(n)$真蕴涵$S(n+1)$真，

则对所有整数$n\geqslant m$，$S(n)$都真.

证明　设C是一切使得$S(n)$不真的整数$n\geqslant m$的集合，如果C空，定理已得到证明. 否则，在C中有最小整数k，由（ⅰ），$k>m$，因而存在命题$S(k-1)$. 因为k是C中的最小整数，所以$k-1<k$蕴涵$k-1\notin C$. 于是，$S(k-1)$为真. 由（ⅱ），$S(k)=S([k-1]+1)$也为真，这与$k\in C$矛盾（$S(k)$是C中的命题，故为假）. ■

定理 1.3（第二归纳法）　*设m是固定的整数，且对每个整数$n\geqslant m$，$S(n)$是一个命题. 如果*

（ⅰ）$S(m)$真，且

（ⅱ）如果对一切满足$m\leqslant k<n$的k，$S(k)$真，则$S(n)$本身也真，

则对所有整数$n\geqslant m$，$S(n)$都真.

⊖　该性质通常称为良序原则.

证明概要 与第一归纳法的证明类似. ■

现在回顾初等数论的一些结果.

定理 1.4（带余除法） 给定整数 a,b，其中 $a\neq 0$，存在唯一的整数 q 和 r 使得

$$b = qa + r, 0 \leqslant r < |a|.$$

证明概要 考虑一切形如 $b-na$ 的非负整数，其中 $n\in\mathbb{Z}$. 定义 r 为形如 $b-na$ 的最小非负整数，并令 q 为出现在表达式 $r=b-na$ 中的整数 n.

如果 $qa+r=q'a+r'$，其中 $0\leqslant r'<|a|$，则 $|(q-q')a|=|r'-r|$. 现在 $0\leqslant|r'-r|<|a|$，
2 如果 $|q-q'|\neq 0$，则有 $|(q-q')a|\geqslant|a|$. 由此可知，等式两端都为 0，即 $q=q'$ 和 $r=r'$. ■

定义 如果 a 和 b 都是整数且 $a\neq 0$，则称带余除法中的 q 和 r 为 a 除 b 的**商**和**余数**.

注 特别地，当 b 为负数时带余除法也有意义. 粗心人会以为 b 和 $-b$ 除以 a 有相同的余数，这通常是错的. 例如 7 除 60 和 -60，

$$60 = 7\cdot 8 + 4 \text{ 和 } -60 = 7\cdot(-9)+3$$

由此，7 除 60 和 -60 的余数是不同的.

系 1.5 有无限个素数.

证明（欧几里得） 假设只有有限个素数，它们是 $p_1,p_2,\cdots,p_k$. 令 $M=(p_1\cdots p_k)+1$. 由命题 1.1，M 不是素数就是素数的乘积，但 M 既不是素数（对每个 i，$M>p_i$）也没有素因子 p_i，因为 p_i 除 M 得余数 1 而不是 0，例如，p_1 除 M 得 $M=p_1(p_2\cdots p_k)+1$，商 $q=p_2\cdots p_k$，余数 $r=1$；p_2 除 M 得 $M=p_2(p_1p_3\cdots p_k)+1, q=p_1p_3\cdots p_k, r=1$；等等. 这一矛盾证明不可能只有有限个素数，从而必有无限个. ■

定义 设 a 和 b 都是整数，如果存在整数 d 使得 $b=ad$，则称 a 是 b 的**因数**. 也称 a **整除** b 或 b 是 a 的**倍数**，记为

$$a \mid b.$$

下面要转移我们的视点. 在开始学习长除法的时候，强调商 q，而余数 r 不过是丢弃的零头. 这里关注给定的数 b 是否为数 a 的倍数，而究竟多少倍是次要的. 因此，从现在起要强调余数. 于是 $a\mid b$ 当且仅当 b 除以 a 得余数 $r=0$.

定义 整数 a 和 b 的**公因数**是指满足 $c\mid a$ 和 $c\mid b$ 的整数 c. a 和 b 的**最大公因数**或 gcd 记为 (a,b)，定义如下：

$$(a,b)=\begin{cases}0, & \text{如果 } a=0=b\\ a \text{ 和 } b \text{ 公因数中的最大者}, & \text{其他}\end{cases}$$

命题 1.6 如果 p 是素数，b 是任一整数，则

$$(p,b)=\begin{cases}p, & \text{如果 } p\mid b\\ 1, & \text{其他}\end{cases}$$

3 **证明概要** 一个正的公因数也是素数 p 的因数，因此不是 p 就是 1. ■

定理 1.7 如果 a 和 b 是整数，则 $(a,b)=d$ 是 a 和 b 的线性组合，即存在整数 s 和 t 使得 $d=sa+tb$.

证明概要 设

$$I=\{sa+tb : s,t\in\mathbb{Z}\}$$

（包括正数和负数的一切整数的集合记为$\mathbb{Z}$）. 如果 $I\neq\{0\}$，令 d 为 I 中的最小正整数，作为 I

的成员，有整数 s 和 t 使得 $d=sa+tb$. 可以断定 $I=(d)$，(d) 是指 d 的一切倍数的集合. 显然，$(d)\subseteq I$. 对于反包含，取 $c\in I$，由带余除法，$c=qd+r$，其中 $0\leqslant r<d$. 如果 $r\neq 0$，则 $r=c-qd\in I$ 与 d 是最小相矛盾. 因此，$d\mid c$，$c\in(d)$ 且 $I=(d)$. 由此，d 是 a 和 b 的公因数且是最大的. ■

命题 1.8 设 a 和 b 都是整数，a 和 b 的非负公因数 d 是 gcd 当且仅当对每个公因数 c 有 $c\mid d$.

证明概要 如果 d 是 gcd，则 $d=sa+tb$，因此，如果 $c\mid a$ 且 $c\mid b$，则 $c\mid sa+tb=d$. 反之，如果 d 是公因数且对每个公因数 c 有 $c\mid d$，则对所有的 c 有 $c\leqslant d$，因此 d 是最大的. ■

系 1.9 设 I 是 $\mathbb{Z}$ 的子集满足

(ⅰ) $0\in I$;

(ⅱ) 如果 a，$b\in I$，则 $a-b\in I$;

(ⅲ) 如果 $a\in I$ 且 $q\in\mathbb{Z}$，则 $qa\in I$.

则存在自然数 $d\in I$ 使得 I 由 d 的一切倍数组成.

证明概要 这正是用来证明定理 1.7 的子集 I 所具备的性质. ■

定理 1.10（欧几里得引理） 如果 p 是素数且 $p\mid ab$，则 $p\mid a$ 或 $p\mid b$. 更一般地，如果素数 p 整除乘积 $a_1a_2\cdots a_n$，则 p 至少整除其中的一个因数 a_i.

证明概要 如果 $p\nmid a$，则 $(p,a)=1$ 且 $1=sp+ta$. 因此，$b=spb+tab$ 是 p 的倍数. 第二个结论可对 $n\geqslant 2$ 用归纳法证明. ■

定义 称整数 a 和 b **互素**，如果它们的 $\gcd(a,b)=1$.

系 1.11 设 a，b 和 c 都是整数. 如果 c 和 a 互素且 $c\mid ab$，则 $c\mid b$.

证明概要 因为 $1=sc+ta$，所以有 $b=scb+tab$. ■ 4

命题 1.12 如果 p 是素数，则 $p\mid\binom{p}{j}$，其中 $0<j<p$.

证明概要 由二项式系数的定义，$\binom{p}{j}=p!/j!(p-j)!$，于是

$$p!=j!(p-j)!\binom{p}{j}.$$

根据欧几里得引理，$p\nmid j!(p-j)!$ 蕴涵 $p\mid\binom{p}{j}$. ■

命题 1.13 (ⅰ) 如果 a 和 b 都是整数，则 a 和 b 互素当且仅当存在整数 s 和 t 使得 $1=sa+tb$.

(ⅱ) 如果 $d=(a,b)$，其中 a 和 b 不全为 0，则 $(a/d,b/d)=1$.

证明 (ⅰ) 由定理 1.7 得必要性. 对于充分性，注意到 1 是最小正整数，因而此时 1 是 a 和 b 的最小正线性组合，从而 $(a,b)=1$. 或者用另一种证法，如果 c 是 a 和 b 的公因数，则 $c\mid sa+tb$，因此 $c\mid 1$，从而 $c=\pm 1$.

(ⅱ) 因 d 是公因数，所以 $d\neq 0$ 且 a/d 和 b/d 是整数. 等式 $d=sa+tb$ 导出 $1=s(a/d)+t(b/d)$，根据 (ⅰ)，$(a/d,b/d)=1$. ■

下面的结果给出求两整数 gcd 的具体方法，同时可把它表示为线性组合.

定理 1.14（欧几里得算法） 设 a 和 b 都是正整数. 存在算法求它们的 $\gcd,d=(a,b)$，且存在算法求整数对 s 和 t 满足 $d=sa+tb$.

注 详情可见定理 3.40 对多项式的证明.

要知道希腊人如何发现该结果，见 Rotman 所著的《A First Course in Abstract Algebra》49 页关于 antanairesis 的讨论.

证明概要 辗转相除如下：开始 $b=qa+r$，其中 $0\leqslant r<a$. 第二步 $a=q'r+r'$，其中 $0\leqslant r'<r$. 再下一步 $r=q''r'+r''$，其中 $0\leqslant r''<r'$，等等. 最终该步骤停止，而最后的余数就是 gcd. 从最后的
5 等式倒推，可把 gcd 表示为 a 和 b 的线性组合. ■

命题 1.15 如果 $b\geqslant 2$ 是整数，则每个正整数 m 都有一个**底数为 b 的表达式**：存在整数 d_i 满足 $0\leqslant d_i<b$，使得

$$m = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_0;$$

此外，如果 $d_k\neq 0$，则该表达式唯一.

证明概要 由最小整数公理，存在整数 $k\geqslant 0$ 使得 $b^k\leqslant m<b^{k+1}$，又由带余除法，$m=d_k b^k+r$，其中 $0\leqslant r<b^k$. 对 $m\geqslant 1$ 用归纳法可证明各 b-进位数字的存在性. 唯一性也可以对 m 作归纳证明，但要注意一切可能产生的情形. ■

称数 d_k，d_{k-1}，…，d_0 为 m 的 **b-进位数字**.

定理 1.16（算术基本定理） 假定整数 $a\geqslant 2$ 有因数分解

$$a = p_1\cdots p_m \text{ 和 } a = q_1\cdots q_n,$$

其中所有的 p 和所有的 q 都是素数. 则 $n=m$ 且各个 q 可以重新标号使得对一切 i 有 $q_i=p_i$. 因此存在唯一的互不相同的素数 p_i 和唯一的 n 个整数 $e_i>0$ 使得

$$a = p_1^{e_1}\cdots p_n^{e_n}.$$

证明 对 m 和 n 的大者 ℓ 用归纳法证明本定理.

如果 $\ell=1$，则给出的等式为 $a=p_1=q_1$，结论显然成立. 关于归纳步，注意给出的等式表明 $p_m \mid q_1\cdots q_n$. 由欧几里得引理，必有某个 i 使得 $p_m \mid q_i$. 但 q_i 是素数，除 1 和它自身外没有正因数，所以 $q_i=p_m$. 重新标号后，可以假定 $q_n=p_m$. 消去 p_m 得 $p_1\cdots p_{m-1}=q_1\cdots q_{n-1}$. 由归纳假设，$n-1=m-1$ 且对所有 q 重新标号后，对一切 i 有 $q_i=p_i$. ■

定义 整数 a 和 b 的**公倍数**是指满足 $a \mid c$ 和 $b \mid c$ 的整数 c. a 和 b 的**最小公倍数**或 lcm 记为 $[a,b]$，定义如下：

$$[a,b] = \begin{cases} 0, & \text{如果 } a=0=b \\ a \text{ 和 } b \text{ 的最小正公倍数}, & \text{其他} \end{cases}$$

命题 1.17 设 $a=p_1^{e_1}\cdots p_n^{e_n}$ 和 $b=p_1^{f_1}\cdots p_n^{f_n}$，其中对一切 i，$e_i\geqslant 0$，$f_i\geqslant 0$；令

$$m_i = \min\{e_i,f_i\}, M_i = \max\{e_i,f_i\}.$$

则 a 和 b 的 gcd 和 lcm 为

$$(a,b) = p_1^{m_1}\cdots p_n^{m_n} \text{ 和 } [a,b] = p_1^{M_1}\cdots p_n^{M_n}.$$

6 **证明概要** $p_1^{e_1}\cdots p_n^{e_n} \mid p_1^{f_1}\cdots p_n^{f_n}$ 当且仅当对一切 i，$e_i\leqslant f_i$. ■

定义 固定 $m\geqslant 0$. 如果 $m \mid (a-b)$ 则称整数 a 和 b **对模 m 同余**，记为

$$a \equiv b \bmod m.$$

命题 1.18 设 $m\geqslant 0$ 是固定的整数，则对所有整数 a，b，c，

（ⅰ） $a\equiv a \bmod m$；

（ⅱ） 如果 $a\equiv b \bmod m$，则 $b\equiv a \bmod m$；

（ⅲ） 如果 $a\equiv b \bmod m$ 且 $b\equiv c \bmod m$，则 $a\equiv c \bmod m$.

注 （ⅰ）说明同余是**自反的**，（ⅱ）说明同余是**对称的**，（ⅲ）说明同余是**传递的**.

证明概要 所有结论容易从同余的定义得出. ■

命题 1.19 设 $m\geqslant 0$ 是固定的整数.

（ⅰ）如果 $a=qm+r$，则 $a\equiv r \bmod m$.

（ⅱ）如果 $0\leqslant r'<r<m$，则 $r\not\equiv r' \bmod m$；即 r 和 $r' \bmod m$ 不同余.

（ⅲ）$a\equiv b \bmod m$ 当且仅当 m 除 a 和 m 除 b 的余数相等.

（ⅳ）如果 $m\geqslant 2$，则每个整数 a 恰和 0，1，…，$m-1$ 之一对模 m 同余.

证明概要 （ⅰ）和（ⅲ）是简单事实；（ⅱ）只需注意 $0<r'-r<m$ 就可推出，而（ⅳ）由（ⅰ）和（ⅱ）推出. ■

下面的结果表明同余与加法相容，同余与乘法也相容.

命题 1.20 设 $m\geqslant 0$ 是固定的整数.

（ⅰ）如果 $a\equiv a' \bmod m$ 且 $b\equiv b' \bmod m$，则

$$a+b\equiv a'+b' \bmod m.$$

（ⅱ）如果 $a\equiv a' \bmod m$ 且 $b\equiv b' \bmod m$，则

$$ab\equiv a'b' \bmod m.$$

（ⅲ）如果 $a\equiv b \bmod m$，则对一切 $n\geqslant 1$，$a^n\equiv b^n \bmod m$.

证明概要 命题显然成立. ■ 7

先前 7 除 60 和 -60 分别得到余数 4 和 3，而 $4+3=7$，这不是偶然的巧合. 如果 a 是整数且 $m\geqslant 0$，设 $a\equiv r \bmod m$ 且 $-a\equiv r' \bmod m$，则由上面的命题得到

$$0=-a+a\equiv r'+r \bmod m.$$

下面的例子说明怎样运用同余. 在每种情形下，关键是要在解题时用余数代替该数.

例 1.21 （ⅰ）证明：如果 a 是 $\mathbb{Z}$ 中的数，则 $a^2\equiv 0$，1，或 $4 \bmod 8$.

如果 a 是整数，则 $a\equiv r \bmod 8$，其中 $0\leqslant r\leqslant 7$；又由命题 1.20（ⅲ），$a^2\equiv r^2 \bmod 8$. 因此只需观察余数的平方.

表 1.1 平方 mod8

r	0	1	2	3	4	5	6	7
r^2	0	1	4	9	16	25	36	49
$r^2 \bmod 8$	0	1	4	1	0	1	4	1

从表 1.1 可知，8 除一个完全平方数其余数只能是 0，1 或 4.

（ⅱ）证明 $n=1\ 003\ 456\ 789$ 不是完全平方数.

因为 $1\ 000=8\cdot 125$，有 $1\ 000\equiv 0 \bmod 8$，所以

$$n=1\ 003\ 456\ 789=1\ 003\ 456\cdot 1\ 000+789\equiv 789 \bmod 8.$$

8 除 789 得余数 5，于是 $n\equiv 5 \bmod 8$. 如果 n 是完全平方数，则 $n=0$，1 或 $4 \bmod 8$.

（ⅲ）如果 m 和 n 是正整数，是否存在形如 3^m+3^n+1 的完全平方数？

再来观察 mod8 的余数. $3^2=9\equiv 1 \bmod 8$，由此可求得 $3^m \bmod 8$ 如下：如果 $m=2k$，则 $3^m=3^{2k}=9^k\equiv 1 \bmod 8$；如果 $m=2k+1$，则 $3^m=3^{2k+1}=9^k\cdot 3\equiv 3 \bmod 8$. 于是

$$3^m = \begin{cases} 1\bmod 8, & \text{如果 } m \text{ 是偶数;} \\ 3\bmod 8, & \text{如果 } m \text{ 是奇数.} \end{cases}$$

用除以 8 的余数代替该数，根据 m 和 n 的不同配对，得到 3^m+3^n+1 的各种可能的余数：

$$3+1+1 \equiv 5\bmod 8$$
$$3+3+1 \equiv 7\bmod 8$$
$$1+1+1 \equiv 3\bmod 8$$
8
$$1+3+1 \equiv 5\bmod 8.$$

无论哪种情形余数都不是 0，1 或 4，因此由 (i)，形如 3^m+3^n+1 的数不可能是完全平方数. ■

命题 1.22 一正整数 a 被 3（或被 9）整除当且仅当它的各位（十进制）数字的和被 3（或被 9）整除.

证明概要 观察 $10^n \equiv 1\bmod 3$ ($10^n \equiv 1\bmod 9$). ■

命题 1.23 如果 p 是素数，a 和 b 是整数，则

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

证明概要 运用二项式定理和命题 1.12. ■

定理 1.24 (费马 (Fermat)) 如果 p 是素数，则对$\mathbb{Z}$ 中的每个 a，

$$a^p \equiv a \bmod p.$$

更一般地，对每个整数 $k \geqslant 1$，

$$a^{p^k} \equiv a \bmod p.$$

证明概要 如果 $a \geqslant 0$，对 a 用归纳法证明，其中归纳步运用命题 1.23. 第二个命题可对 $k \geqslant 1$ 用归纳法证明. ■

系 1.25 设 p 是素数，n 是正整数. 如果 $m \geqslant 0$ 且 Σ 是 m 的 p-进位各位数字之和，则

$$n^m \equiv n^{\Sigma} \bmod p.$$

证明概要 用底为 p 的指数表出 m，再用费马定理. ■

计算 7 除 10^{100} 的余数. 第一步，$10^{100} \equiv 3^{100} \bmod 7$. 第二步，因 $100 = 2 \cdot 7^2 + 2$，由上面的系得 $3^{100} \equiv 3^4 = 81 \bmod 7$. 因 $81 = 11 \times 7 + 4$，可得余数为 4.

定理 1.26 如果 $(a,m)=1$，则对每个整数 b，同余式

$$ax \equiv b \bmod m$$

关于 x 有解；事实上，$x = sb$ 就是一个解，其中 $sa \equiv 1\bmod m$. 此外，任两个解关于模 m 同余.

证明概要 如果 $1 = sa + tm$，则 $b = sab + tmb$. 因此 $b \equiv a(sb) \bmod m$. 又如果 $b \equiv ax \bmod m$，则
9
$0 \equiv a(x - sb) \bmod m$，所以 $m \mid a(x-sb)$. 因 $(m,a) = 1$，由系 1.11，$m \mid (x - sb)$，因此 $x \equiv sb \bmod m$. ■

系 1.27 如果 p 是素数，a 不能被 p 整除，则同余式

$$ax \equiv b \bmod p$$

恒有解.

证明概要 如果 a 不能被 p 整除，则 $(a,p) = 1$. ■

定理 1.28 (孙子剩余定理) 如果 m 和 m' 互素，则下面两个同余式

$$x \equiv b \bmod m$$
$$x \equiv b' \bmod m'$$