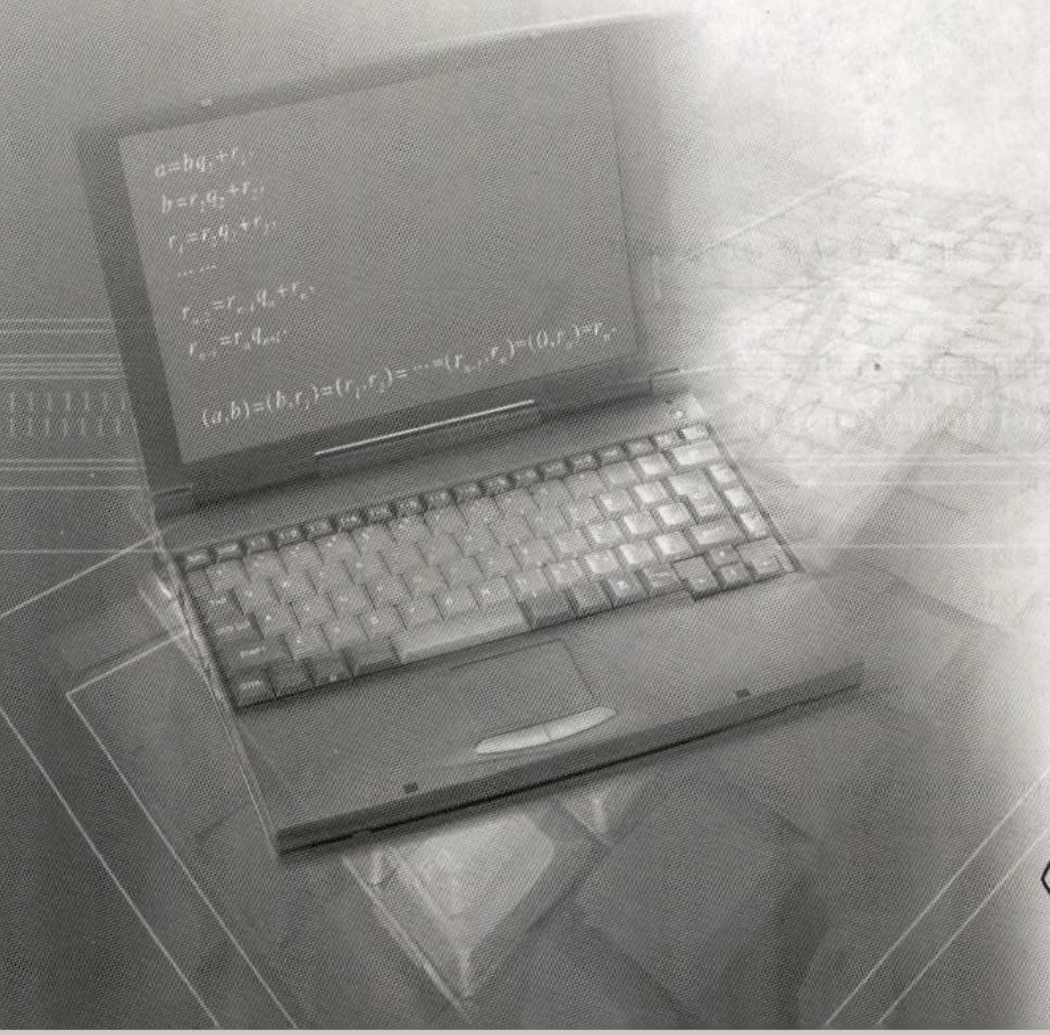
普通高中课程标准实验教科书

数学 选修 4-6

初等数论初步

教师教学用书

人民教育出版社 课程教材研究所
中学数学课程教材研究开发中心 编著



人民教育出版社 A版

图书在版编目（CIP）数据

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（A版）教师教学用书/人民教育出版社，课程教材研究所中学数学课程教材研究开发中心编著．—2版．—北京：人民教育出版社，2007.5（2018.10重印）

ISBN 978－7－107－19489－4

Ⅰ．①普… Ⅱ．①人… ②课… Ⅲ．①中学数学课—高中—教学参考资料 Ⅳ．①G633.603

中国版本图书馆CIP数据核字（2012）第031316号

普通高中课程标准实验教科书 数学 选修 4－6 A版 教师教学用书

出版发行 人民教育出版社
（北京市海淀区中关村南大街17号院1号楼 邮编：100081）
网 址 http://www.pep.com.cn
经 销 全国新华书店
印 刷 大厂益利印刷有限公司
版 次 2007年5月第2版
印 次 2018年10月第11次印刷
开 本 890毫米×1240毫米 1/16
印 张 3.75
字 数 92千字
定 价 9.10元

主　　编：刘绍学
副 主 编：钱珮玲　章建跃

编　　者：胡永建
责任编辑：张劲松

说明

人教版普通高中课程标准实验教材·数学（A版），是以教科书为基础的系列化教材，包括基本教材和配套教学资源. 基本教材是教科书和教师教学用书，配套教学资源包括新课程导学·数学、教学设计与案例、教学投影片、信息技术支持系统等.

人教版《普通高中课程标准实验教科书·数学（A版）》包括教育部制订的《普通高中数学课程标准（实验）》中规定的全部内容. 本套教科书在坚持我国数学教育优良传统的前提下，认真处理继承、借鉴、发展、创新之间的关系，体现**基础性、时代性、典型性和可接受性**等，具有如下特点：

1. “亲和力”：以生动活泼的呈现方式，激发兴趣和美感，引发学习激情.

尽量选取与内容密切相关的、典型的、丰富的和学生熟悉的素材，用生动活泼的语言，创设能够体现数学的概念、结论及其思想方法发生发展过程的学习情境，使学生感到数学是自然的，水到渠成的，激发学生对数学的亲切感，引发学生“看个究竟”的冲动，兴趣盎然地投入学习.

在体现知识归纳概括过程中的数学思想、解决各种问题中数学的力量、数学探究和论证方法的优美和精彩之处、数学的科学和文化价值等地方，将作者的感受用“旁批”等方式呈现，与学生交流，增强了教科书的“亲和力”，启发学生更深入的数学思考，不断引发学习激情.

2. “问题性”：以恰时恰点的问题引导数学活动，培养问题意识，孕育创新精神.

在知识形成过程的“关键点”上，在运用数学思想方法产生解决问题策略的“关节点”上，在数学知识之间联系的“联结点”上，在数学问题变式的“发散点”上，在学生思维的“最近发展区”内，通过“观察”“思考”“探究”等栏目，提出恰当的、对学生数学思维有适度启发的问题，引导学生的思考和探索活动，使他们经历观察、实验、猜测、推理、交流、反思等理性思维的基本过程，切实改进学生的学习方式.

提问是创新的开始. “看过问题三百个，不会解题也会问”，通过恰时恰点地提出问题，提好问题，给学生示范提问的方法，使他们领悟发现和提出问题的艺术，引导他们更加主动、有兴趣地学，富有探索性地学，逐步培养学生的问题意识，孕育创新精神.

3. “思想性”：螺旋上升地安排核心数学概念和重要数学思想，加强数学思想方法的渗透与概括.

以数及其运算、函数、空间观念、数形结合、向量、导数、统计、随机观念、算法等数学核心概念和基本思想为贯穿整套教科书的“灵魂”，体现寻求一般性模

式的思想和追求简洁与形式完美的精神等，引导学生领悟数学本质，体验数学中的理性精神，加强数学形式下的思考和推理训练，从而提高教科书的“思想性”.

4. “联系性”：通过不同数学内容的联系与启发，强调类比、推广、特殊化、化归等思想方法的运用，学习数学地思考问题的方式，提高数学思维能力，培育理性精神.

利用数学内容的内在联系，使不同的数学内容相互沟通，提高学生对数学的整体认识水平. 特别地，在教科书中强调类比、推广、特殊化、化归等思想方法，尽最大可能展示以下常用的逻辑思考方法：

以使学生体会数学探索活动的基本规律，逐步学会借助数学符号和逻辑关系进行数学推理和探究，推求新的事实和论证猜想，从而发展学生认识事物的“数”“形”属性和规律、处理相应的逻辑关系的悟性和潜能，养成逻辑思维的习惯，能够有条理地、符合逻辑地进行思考、推理、表达与交流.

教科书力求使数学内容的呈现做到脉络清晰，重点突出，体系简约，在学生原有认知结构基础上，依据数学学习规律、相关内容在不同模块中的要求以及数学内在的逻辑联系，以核心知识（基本概念和原理，重要的数学思想方法）为支撑和联结点，循序渐进、螺旋上升地组织学习内容，形成结构化的教材体系.

选修系列4的教师教学用书，按照相应教科书的内容顺序编排，包括总体设计、教科书分析、习题解答、教学设计案例、自我检测题、拓展资源等栏目.

1. 总体设计是对整个专题作概括性介绍，重点说明教科书设计思想. 包括：课程目标、学习目标、内容安排（知识结构框图及说明）、课时分配等.

（1）课程与学习目标说明学生通过学习本专题内容应达到的要求，表述时关注了目标的可测性；

（2）内容安排中给出了本专题的知识结构框图及其对内容安排的概括性说明，以利于教师从整体上把握本章知识发生、发展的脉络；

（3）课时分配根据具体内容的分量提出课时分配的建议，教师可以根据自己的教学实际进行调整.

2. 教科书分析按照教科书内容顺序、以讲为单位进行分析，着重说明了编写意图与教学建议. 主要包括：本讲知识结构、重点与难点、编写意图与教学建议等.

(1) 本讲知识结构说明本讲知识点及其发生、发展过程（逻辑关系）. 说明学习本讲内容时，涉及的前后相关知识，采用“知识框图”或“表格”的方式表述；

(2) 重点不仅指数学概念、数学结论，而且包括数学思想方法、数学能力等方面的内容；难点说明学生在学习过程中可能遇到的困难和问题；

(3) 编写意图与教学建议主要对教科书“为什么要这样写”进行分析，包括学习相应内容应具备的认知发展基础，如何理解其中的一些关键概念，知识中蕴含的数学思想方法，突破重点、难点的建议，如何激发学生学习兴趣，渗透能力培养，以及数学应用意识、创新意识的培养等；对例题要达到的目的进行说明；对“观察”“思考”“探究”中的内容以及边空中的问题，给出解释或解答.

教学建议主要对教师如何引导学生学习进行分析，从教科书编写者的角度结合具体内容给教师提出一些建议.

(4) 教学设计案例选取了一些具有典型性的、教学难度大、新增知识、适宜使用信息技术的内容，包括概念课、研究（探究）课、习题课、复习课等不同课型. 具体包括了下面一些内容：

1° 教学任务分析重点对学习相应内容时的认知要求进行分析；

2° 教学基本流程以框图的形式表示出教学的基本进程；

3° 重点和难点表述了本课内容的重点，以及学习中可能碰到的困难；

4° 教学情境设计以“问题串”为主线，在提出问题的同时，说明了设计意图.

(5) 习题解答不仅给出解答过程，讲清楚“可以这样解”，而且还对一些典型问题分析了解答中的数学思想方法，说明“为什么可以这样解”，从而体现了习题在巩固知识，深化概念学习，深刻理解知识，开展研究性学习，应用知识解决实际问题，培养学生的数学能力、创新精神和实践能力等方面的功能.

(6) 拓展资源为教师提供了一些教学中有用的资料，既有知识性的，又有数学历史、数学文化方面的资料. 同时，在适当的地方，对数学教学中如何使用科学计算器、计算机、网络等进行说明或解释.

3. 自我检测题提供了本专题的自我检测题目，目的是检测学生掌握本专题知识内容的情况. 教学时，教师可直接使用.

本书是选修系列 4-6《初等数论初步》的教师教学用书，它包含整数的整除、同余与同余方程、一次不定方程和数论在密码中的应用等四讲内容. 全书共 18 课

时，具体分配如下（仅供参考）：

第一讲 整数的整除	约 5 课时
第二讲 同余与同余方程	约 7 课时
第三讲 一次不定方程	约 3 课时
第四讲 数论在密码中的应用	约 2 课时
学习总结报告	约 1 课时

由于“第四讲 数论在密码中的应用”主要是介绍性的知识，属于学生了解的内容，供学生阅读. 目的是进一步加深对数论在密码中应用的了解，知道数论不仅是一门学科，而且在实践中有广泛的应用. 在本书“教科书分析”部分略去该讲相应的内容.

参加本书编写的是胡永建，责任编辑张劲松.

我们在广泛听取广大教师、教学研究人员意见的基础上，对教师教学用书进行了较大的改进，希望它能够较好地满足广大教师的教学需要. 由于是对教师教学用书编写工作的一次新尝试，其中肯定存在许多值得改进的地方，希望广大教师在使用过程中提出宝贵意见，我们愿意根据大家的意见作出修正，使其更好地为教师教学服务.

目录

I 总体设计

一、课程与学习目标

1. 课程目标

本专题包括四方面内容：整数的整除、同余与同余方程、一次不定方程、数论在密码中的应用.

通过本专题学习，应当使学生达到如下目标：

(1) 获得必要的数学基础知识和基本技能，理解基本的数学概念，理解定理的本质和证明过程，了解数学概念、定理等产生的相关背景和应用. 能够解决与数论有关的一些简单的实际问题.

(2) 通过不同形式的自主学习和探究活动，体验数学发现和创造的历程，掌握探究数学问题的基本方法，如类比、由特殊到一般、推广等，提高数学表达和交流的能力，发展独立获取数学知识的能力.

(3) 提高数学地提出、分析和解决问题的能力，以及抽象概括、推理论证的能力，能够编写计算机程序解决一些简单的数论问题.

(4) 发展数学应用意识和创新意识，对现实世界中的信息安全传送的数学模型进行思考和做出判断.

(5) 体会数论中常用的数学思想方法，了解我国古代在数论方面取得的一些重要成就，提高学习数学的兴趣，树立学好数学的信心，形成锲而不舍的钻研精神和科学态度.

(6) 开阔数学视野，逐步认识数学的科学价值、应用价值和文化价值，形成批判性的思维习惯，崇尚数学的理性精神.

2. 学习目标

第一讲　整数的整除

(1) 整除

①理解整除、因数和倍数的概念，能够证明整除的下列基本性质：

若 $a|b$，$b|a$，则 $a=b$，或 $a=-b$；

若 $a|b$，$b|c$，则 $a|c$；

若 $a|b$，$a|c$，则对任意整数 x，y，恒有 $a|bx+cy$；

②探索能被 3，9，11，7 等整除的整数的判别法，能够用判别法解决某些整除问题；

③理解带余除法的内容，能够用带余除法解决简单的数论问题，探索用取整函数表示带余除法中的商和余数；

④理解素数的概念，了解确定素数的一种方法，如埃拉托斯特尼筛法，知道素数有无穷多个；

⑤理解任何大于 1 的整数可以分解成一些素数的乘积.

(2) 最大公因数与最小公倍数

①理解公因数、最大公因数、互素等概念，通过实例探索利用辗转相除法求两个整数的最大公因数的方法；

②理解辗转相除法的算法程序框图，能够根据程序框图编写计算机程序，并在条件允许的情况下

上机实现；

③通过实例探索三个、多于三个整数的最大公因数的求法，体会由特殊到一般发现数学结论的方法；

④能够用辗转相除法证明最大公因数的如下重要性质：

设整数 a，b 不同时为零，则存在一对整数 m，n，使得 $(a, b)=am+bn$；

⑤能够用最大公因数的上述性质证明整除的下列两条性质：

若 $a|bc$，且 $(a, b)=1$，则 $a|c$；

设 p 为素数，若 $p|ab$，则 $p|a$，或 $p|b$；

⑥理解公倍数、最小公倍数的概念以及它们之间的整除关系，即两个非零整数的最小公倍数一定整除它们的公倍数；

⑦通过具体例子探索 (a, b)，$[a, b]$ 和 ab 之间的关系，进一步体会由特殊到一般发现数学结论的方法；

⑧能够通过求最大公因数来求两个或多个非零整数的最小公倍数.

(3) 算术基本定理

①理解算术基本定理的内容和定理的证明过程；

②能够用素因数分解式计算两个整数的最大公因数和最小公倍数.

第二讲 同余与同余方程

(1) 同余

①理解同余的概念，认识同余和整除之间的内在联系；

②探索同余的下列三条基本性质：

$a\equiv a(\mathrm{mod}\ n)$；

若 $a\equiv b(\mathrm{mod}\ n)$，则 $b\equiv a(\mathrm{mod}\ n)$；

若 $a\equiv b(\mathrm{mod}\ n)$，$b\equiv c(\mathrm{mod}\ n)$，则 $a\equiv c(\mathrm{mod}\ n)$，

体会模 n 同余是整数之间的一种关系，利用它可以对整数集进行分类；

③能类比等式的性质，探究同余式的其他性质，体会类比探究数学问题的方法；

④理解同余意义下的消去律，以及消去律成立的条件；

⑤能够用同余的性质解决星期几问题，体会同余方法在解决整除问题中的应用.

(2) 剩余类及其运算

①理解剩余类的概念，以及剩余类的表示与代表元的选取无关；

②通过实例探索剩余类加法和剩余类乘法运算，理解剩余类加法和剩余类乘法运算的定义，开阔关于运算的眼界；

③理解模 n 的剩余类环的概念，认识一些具体的剩余类环；

④通过实例，探索剩余类加法和剩余类乘法运算遵循交换律、结合律和分配律；

⑤通过探索认识剩余类环中零元、单位元、负元和逆元，能类比数中的相反数和倒数的概念理解剩余类中的负元和逆元的概念；

⑥探索模 n 的剩余类环中一个非零元有逆元的充要条件，并能给出证明；

⑦体会数的乘法运算与剩余类乘法运算的联系和区别.

(3) 费马小定理和欧拉定理

①通过实例探索模 m（m 为素数）的剩余类环中存在如下规律：

对任意整数 a，$[a^m]=[a]$；

由实例归纳出费马小定理，体会从特殊到一般发现数学结论的方法；

②理解费马小定理的内容和费马小定理的证明过程；

③理解欧拉定理内容的本质，会证明欧拉定理；

④了解欧拉函数的概念及其表达式，知道费马小定理是欧拉定理的特殊情形；

⑤通过具体的例子，体会费马小定理和欧拉定理在整除问题和同余问题中的应用.

(4) 一次同余方程

①了解同余方程产生的背景，理解一次同余方程及其解的概念，认识一次同余方程的解与一元一次方程的解之间的联系与区别；

②探索一次同余方程 $ax\equiv b(\mathrm{mod}\ n)$有解的充要条件、解的个数、有解时解的描述等问题；

③会解一次同余方程 $ax\equiv b(\mathrm{mod}\ n)$；

④了解大衍求一术算法的历史背景和内容，能够用现代数学的语言正确叙述大衍求一术的算法步骤；

⑤通过探索将大衍求一术算法步骤中余数 r_i 表示成 $ax+ny$ 形式的规律，理解大衍求一术的算法原理；

⑥能够用大衍求一术解形如 $ax\equiv 1(\mathrm{mod}\ n)$的一次同余方程.

(5) 拉格朗日插值法和孙子定理

①了解“物不知其数”问题、孙子定理（或中国剩余定理）、程大位的算法口诀及其相关的历史背景知识；

②认识同余方程组，理解同余方程组解的概念；

③经历拉格朗日插值公式的建立过程，体会先特解而后求通解的思路；

④能够依照先特解而后求通解的思路求解“物不知其数”问题，并解释程大位的算法口诀；

⑤能够从实例抽象出孙子定理，理解孙子定理的内容，能用孙子定理求解一些简单的同余方程组.

(6) 弃九验算法

①理解弃九验算法的内容及其原理，能够用弃九验算法验算算式的正确性；

②通过具体的例子，认识弃九验算法只能“检错”，不能“判正”的事实.

第三讲　一次不定方程

(1) 二元一次不定方程

①了解我国古代数学家在不定方程研究方面取得的重要成就；

②探索二元一次不定方程有整数解的条件、解的个数、有解时通解的描述等问题，能够根据二元一次不定方程的一个特解写出通解的表达式；

③能够解一些简单的二元一次不定方程.

(2) 二元一次不定方程的特解

①理解用辗转相除法计算二元一次不定方程特解的过程以及算法程序框图，尝试根据程序框图编写计算机程序，在条件允许的情况下上机实现；

②能够用辗转相除法计算二元一次不定方程的一个特解.

(3) 多元一次不定方程

①经历三元一次不定方程有整数解的充要条件，体会三元一次不定方程的解法，会将三元一次不定方程化归为二元一次不定方程进行求解；

②探索四元一次不定方程有整数解的充要条件，会将四元一次不定方程化归为二元一次不定方程进行求解.

第四讲　数论在密码中的应用

(1) 信息的加密与去密

①了解信息传送的一些简单模型和这些模型中信息传送的机制，了解同余在信息的加密和去密过程中的应用；

②了解传统信息传送模型在信息安全方面的不足.

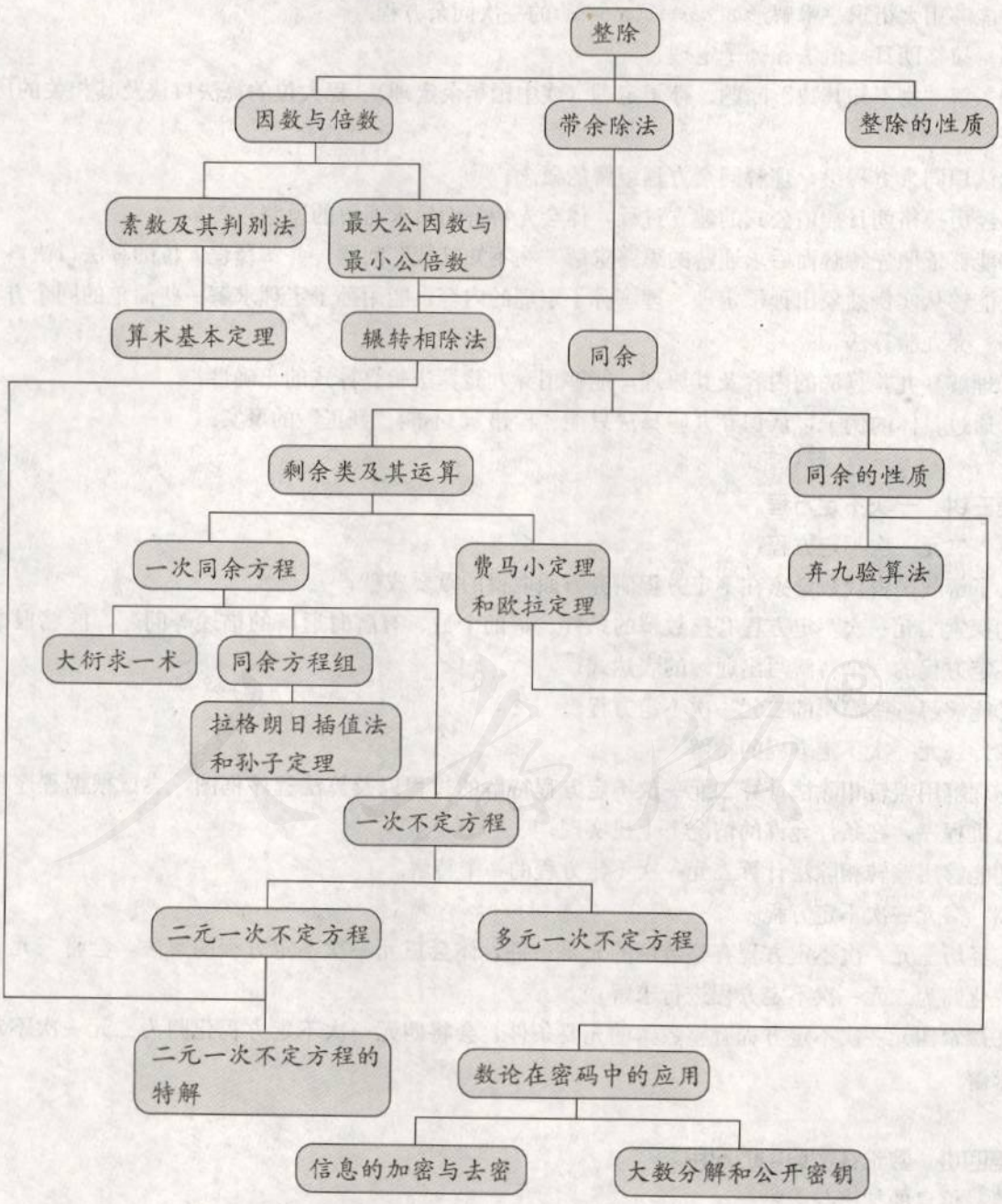
(2) 大数分解和公开密钥

①了解大数分解和公开密钥体制，了解欧拉定理在公开密钥体制中的应用.

二、内容安排

1. 本专题知识结构框图

本专题分为四讲，每讲的内容有相对的独立性，同时又有内在的联系. 知识结构框图如下：



2. 对内容安排的说明

学习初等数论的初步知识，可以培养学生的逻辑思维能力、发展学生的智力. 围绕这个目标，本专题在内容的安排上体现如下特点：

(1) 注重知识系统性与逻辑性. 第一、二、三、四讲的内容相对独立，每一讲的内容依托自身的逻辑起点展开，自成一个系统的知识体系，同时这四者之间又有一定的逻辑关系. 例如，第一讲介绍的整数的整除理论是本专题其他三讲的理论基础，其中介绍的辗转相除法在第二讲求解一次同余方程和第三讲求解一次不定方程时经常要用到. 又如，第二讲介绍的费马小定理和欧拉定理在通信技术中的重要应用体现在第四讲介绍的公开密钥体制中. 另外，第二讲介绍的一次同余方程和第三讲介绍的一次不定方程可以相互转化，一个典型的例子就是“物不知其数”问题.

(2) 强调从特殊到一般地引入知识. 例如，通过观察月历表中同一列整数被 7 除后的余数的特征，引出同余的概念. 又如，通过考察一些特殊的模 n（n 为素数）的剩余类环中乘法运算的规律，归纳、猜想出费马小定理的结论，然后给出证明. 这种由特殊到一般的引入方式，既符合知识产生的历程，也符合学生的认识规律，对于培养学生提出问题的意识和能力都是有益的.

(3) 突出知识的探究与发展，在重要性质的引入方面，通过知识形成的方式展开，力图使学生在经历知识的产生过程中认识对象和建构知识. 本专题一方面在对重要结论的呈现上突出探究性，另一方面在一些例题和习题中渗透探究思想，使学生既掌握“概念性”知识，又掌握“方法性”知识，同时发展学生探究新知的能力.

(4) 在知识中渗透数学思想方法. 本专题中的主要数学思想方法包括：特殊化思想方法、化归的思想方法、类比的思想方法、分类讨论的思想方法，还涉及到观察、猜想等合情推理的方法，也涉及到演绎推理、反证法等逻辑推理方法. 这些思想方法以知识为载体，是在知识的学习中形成和发展的.

三、课时分配

本专题教学时间为 18 课时，具体分配如下（仅供参考）：

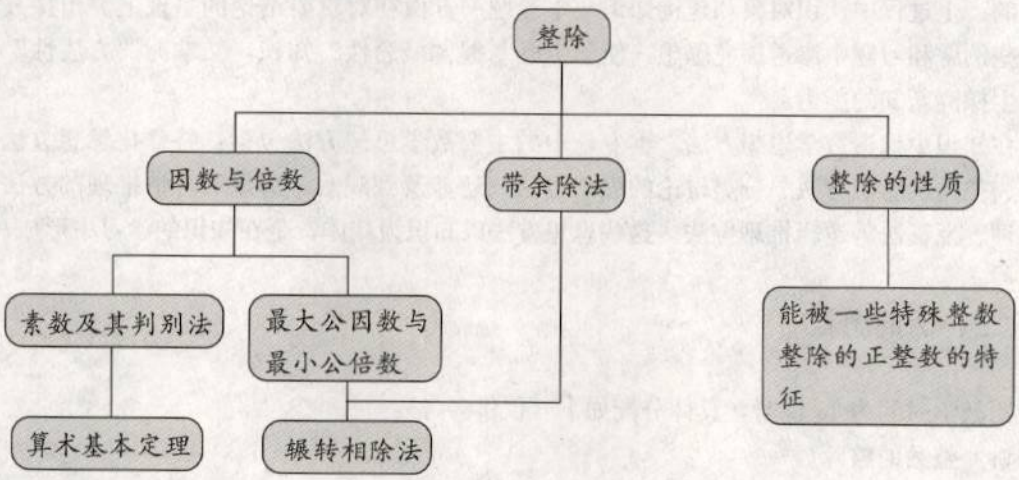
第一讲　整数的整除	约 5 课时
一、整除的概念和性质	约 2 课时
二、最大公因数与最小公倍数	约 2 课时
三、算术基本定理	约 1 课时
第二讲　同余与同余方程	约 7 课时
一、同余	约 1 课时
二、剩余类及其运算	约 2 课时
三、费马小定理和欧拉定理	约 1.5 课时
四、一次同余方程	约 1 课时
五、拉格朗日插值法和孙子定理	约 1 课时
六、充九验算法	约 0.5 课时
第三讲　一次不定方程	约 3 课时
一、二元一次不定方程	约 1 课时
二、二元一次不定方程的特解	约 1 课时
三、多元一次不定方程	约 1 课时
第四讲　数论在密码中的应用	约 2 课时

一、信息的加密与去密 约1课时
二、大数分解和公开密约 约1课时
学习总结报告 约1课时

II 教科书分析

第一讲 整数的整除

一、本讲知识结构



二、教学重点与难点

重点：

1. 理解整除、因数、倍数、素数、最大公因数与最小公倍数的概念和性质；
2. 理解带余除法的内容和证明过程；
3. 理解辗转相除法，会用辗转相除法求两个整数的最大公因数；
4. 理解算术基本定理的内容与证明过程；
5. 体验整数整除的本质，感受和体会蕴涵在知识与探究过程中的数学思想方法.

难点：

1. 带余除法定理的证明；
2. 应用辗转相除法求两个整数的最大公因数；
3. 理解最大公因数的性质，并会灵活运用这些性质解决整除问题；
4. 算术基本定理的证明.

三、编写意图与教学建议

整数的整除理论是整个初等数论的基础. 学生在小学学习过整除的一些初步知识，会运用整除的性质解决一些简单的数论问题. 需要指出的是，小学阶段讨论的是自然数集合中的整除问题，而这里讨论的是整数集合中的整除问题. 在介绍整除、因数、倍数、素数、最大公因数与最小公倍数这些概念时，应注意前后表述之间的联系与差别.

在编写教科书时，对一些基本的知识点，如整除的性质、能被一些特殊整数整除的整数特征、最大公因数与最小公倍数的性质等，我们不仅要求学生理解它们的内容，还要求学生说清道理；对一些重要的方法，如带余除法、埃拉托斯特尼筛法、辗转相除法、素因数分解式等，要求学生不仅会正确地运用这些方法解决简单的数论问题，还懂得这些方法的基本原理.

教材在介绍新概念、新结论和新方法之前，采用了观察、思考、探究等方式，让学生首先有一个感性认识，然后逐步上升到理性认识，最后通过例题和练习进行巩固. 这种做法，不仅可以降低学生的认知难度，还可以提高学生学习的积极性，培养学生提出问题、分析问题和解决问题的能力.

整除是本讲知识系统的逻辑起点，由它引出因数、倍数的概念和带余除法，再由因数和倍数引出素数及其判别法和最大公因数与最小公倍数，后面两部分内容的讨论又分别引出了辗转相除法和算术基本定理，其中辗转相除法是由有限次带余除法组成的.

1. 整除

从知识层面看，本节由三部分内容构成：整数的概念和性质、带余除法、素数及其判别法，其中带余除法的证明是学生学习的一个难点. 从方法层面看，本节涉及到观察、类比和特殊化方法. 教学中应从这两个层面去把握.

(1) 整除的概念和性质

介绍整除的概念时要注意如下几点：一是概念引入的背景，即除法运算在整数集合中的封闭性问题；二是整除的概念是在整数集合中定义的，而不是小学阶段的自然数集合，要注意语言表述的准确性和新旧知识之间的内在联系，在选用整除和不整除的例子时，突出负整数的例子，如 $6\mid -24$，$-4\nmid 14$等；三是引导学生提出需要研究的问题，如本讲在引言中提出的问题，通过这些问题把本专题的内容紧密联系起来.

教科书第 3 页让学生探究的是整除的一些最基本、最常用的性质，这些性质由整除的定义很容易给出证明. 例如，性质 (1) 的证明如下：

因为 $a\mid b$，所以 $b=ar$；

又因为 $b\mid a$，所以 $a=bs$.

于是，$ab=ab(rs)$，而又 $ab\neq 0$，所以 $rs=1$，从而 $r=s=1$，或 $r=s=-1$.

当 $r=s=1$ 时，$a=b$；

当 $r=s=-1$ 时，$a=-b$.

在介绍能被一些特殊整数 (如 3，9，11，7) 整除的正整数的特征时，我们采用的方式是先观察，然后归纳、猜想，最后给出证明. 限于篇幅，教科书中只介绍了能被 3 整除的正整数的特征发现的过程和证明，对于能被其他特殊的整数整除的正整数的特征作为学生探究的内容. 学生对能被 3，9，11，7 整除的正整数的特征并不会太陌生，所以教学时应把更多的注意力放在这些特征的证明上.

关于能被 3，9，11 整除的正整数的特征要用到整数的多项式表示形式：

$$\overline{a_n\cdots a_2a_1a_0}=a_n\times 10^n+\cdots+a_2\times 10^2+a_1\times 10+a_0. \tag{1}$$

能被 9 整除的正整数的特征的证明：

由（1）式知，

$$\begin{aligned}\overline{a_n\cdots a_2a_1a_0}&=a_n\times(99\cdots9+1)+\cdots+a_2\times(99+1)+a_1\times(9+1)+a_0\\&=9(11\cdots1a_n+\cdots+11a_2+a_1)+(a_0+a_1+\cdots+a_n).\end{aligned}$$

因为 $9\mid 9(11\cdots1a_n+\cdots+11a_2+a_1)$，如果 $9\mid a_0+a_1+\cdots+a_n$，那么 $9\mid\overline{a_n\cdots a_2a_1a_0}$.

能被 11 整除的正整数的特征的证明：

把（1）式中的 10 表示为“11－1”的形式，然后展开得

$$\begin{aligned}\overline{a_n\cdots a_2a_1a_0}&=a_n\times(11-1)^n+\cdots+a_2\times(11-1)^2+a_1\times(10-1)+a_0\\&=11R+(a_0+a_2+\cdots)-(a_1+a_3+\cdots).\end{aligned}$$

因为 $11\mid 11R$，如果 $11\mid(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$，那么 $11\mid\overline{a_n\cdots a_2a_1a_0}$.

至于能被 7（或 11）整除的正整数特征的证明，要用到下面的恒等式：

$$\overline{a_n\cdots a_3a_2a_1a_0}=\overline{a_n\cdots a_3}\times1\ 000+\overline{a_2a_1a_0}=\overline{a_n\cdots a_3}\times1\ 001+(\overline{a_2a_1a_0}-\overline{a_n\cdots a_3}).$$

由于 1 001 能被 7(或 11)整除，所以 $\overline{a_n\cdots a_3}\times1\ 001$ 能被 7(或 11)整除. 如果 7(或 11)能整除 $\overline{a_2a_1a_0}-\overline{a_n\cdots a_3}$，那么 7(或 11)能整除 $\overline{a_n\cdots a_2a_1a_0}$.

（2）带余除法

带余除法是初等数论中的重要结论之一，它也称为欧氏除法算式. 带余除法是本讲后面将要介绍的辗转相除法的基本组成部分. 在小学阶段，学生接触过类似的表示形式，如 $14\div3=4\cdots\cdots2$，即 $14=3\times4+2$. 带余除法只不过是这种表示在整数集合中的推广. 通过建立与旧知识之间的联系，学生理解和接受起来会容易一些.

学生在学习带余除法时，最容易出错的地方是余数 r 的范围，教学时一定要强调余数总是非负整数，且不超过除数的绝对值. 在引出商和余数的概念后，教师可通过一些具体的例子巩固对商和余数的认识. 例如，让学生回答下面的问题：

（1）16 除以 7 的商和余数是多少？

（2）16 除以－7 的商和余数是多少？

（3）－16 除以 7 的商和余数是多少？

（4）－16 除以－7 的商和余数是多少？

（结果分别为 2，2；－2，2；－3，5；3，5）

带余除法的证明是本节教学的一个难点. 教科书关于存在性的证明是结合图形进行的，比用集合的方法（对整数集合进行划分）直观且容易理解. 而惟一性的证明是学生不太熟悉的，过去一些教科书中很少严格证明有关惟一性的结论. 所以，具体教学时，教师在证明惟一性之前要引导学生，让学生明白对具体的问题如何去证明惟一性. 教科书在这里采用的是关于惟一性的一种最常用的证明方法.

另外，反证法也是证明惟一性的一种常用证明方法.

教科书上的例 2 介绍带余除法的应用. 问题是已知被除数和商，要求除数和余数. 问题解决的关键是通过余数的变化范围确定除数的变化范围，再利用除数是整数的特征确定除数的取值，进而确定余数.

取整函数$[x]$是数论中一个常见的函数，对于给定的实数 x，它的值为不超过 x 的最大整数. 取整函数$[x]$也称为高斯函数，具有许多有趣的性质，我们将在本讲“拓展资源”部分作简要介绍. 本小节的“探究”要求用取整函数表示 a 除以正整数 b 的商和余数. 教学时，教师可以先让学生通过一些具体的例子，观察$\left[\frac{a}{b}\right]$与 a 除以正整数 b 的商 q 和余数 r 之间的关系.

结果如下：

设 a 除以正整数 b 的商为 q，余数为 r，则 $a=bq+r$，$0\leqslant r<b$. 于是

$$\left[\frac{a}{b}\right]=\left[\frac{bq+r}{b}\right]=\left[q+\frac{r}{b}\right]=q,\qquad r=a-b\left[\frac{a}{b}\right].$$

如果除数 $b<0$，结论如何？这时要分 b 整除 a 和 b 不整除 a 两种情形讨论. 当 b 整除 a 时，$r=0$，$q=\left[\frac{a}{b}\right]$；当 b 不整除 a 时，$0<r<|b|=-b$，于是，$-1<\frac{r}{b}<0$，$0<1+\frac{r}{b}<1$. 因此，

$$\left[\frac{a}{b}\right]=\left[\frac{bq+r}{b}\right]=\left[q+\frac{r}{b}\right]=\left[q-1+\left(1+\frac{r}{b}\right)\right]=q-1.$$

所以，

$$q=\left[\frac{a}{b}\right]+1,\qquad r=a-b\left(\left[\frac{a}{b}\right]+1\right).$$

(3) 素数及其判别法

本小节首先考察正整数的正因数个数，由正因数的个数把正整数分为三类：只有一个正因数的正整数即 1，只有两个正因数的正整数，至少有三个正因数的正整数. 其中只有两个正因数的正整数叫做素数，至少有三个正因数的正整数叫做合数，由此引出素数与合数的概念. 这样通过考察的方式引入概念，容易引起学生的研究兴趣.

关于素数与合数，教科书中直接叙述了两个基本事实，它们在处理与数论有关的问题时经常用到，是学生应当了解的：

(1) 2 是惟一的偶素数，也是最小的素数；

(2) 每个合数总可以表示成两个大于 1 的正整数的乘积，而素数则不能.

为了得到如下重要结论：

(3) 任何大于 1 的正整数一定有一个素数因数.

教科书采用先观察，后证明的方式，目的是降低学生的认知难度. 通过观察发现，每个大于 1 的正整数中除 1 外最小的正因数就是一个素数.

紧接着，由结论 (3) 可以推出：任何大于 1 的正整数总可以分解成一些素数因数的乘积. 这就得到本讲最后一节中介绍的算术基本定理的两个重要内容之一，从而将本讲最后一节内容的难度分解了.

素数有无穷多个是一个基本的结论，也是《普通高中数学课程标准（实验）》中要求学生知道的. 关于这一基本结论的证明，教科书采用的是传统的反证法. 除此之外，还有许多有趣的方法，我们将在“拓展资源”中进行介绍.

关于素数的一个重要而又有趣的问题是素数的判定，《普通高中数学课程标准（实验）》中要求学生了解确定素数的一种方法. 教科书上介绍的是埃拉托斯特尼筛法，是一种非常传统的方法. 教学过程中，教师在引出素数的判定这个问题后，让学生具体地判断 61 是不是素数. 引导学生逐步思考下列问题：

(1) 若 61 是合数，则 61 可分解成两个大于 1 的整数的乘积，其中较小的一个整数一定不超过 $\sqrt{61}$；

(2) 若 61 是合数，则 61 一定能被某个大于 1 且不超过 $\sqrt{61}$ 的正整数 d 整除；

(3) 若 61 是合数，则 61 一定能被某个不超过 $\sqrt{61}$ 的素数整除. 这是因为，上面的正整数 d 一定能被某个素数整除，这个素数显然不超过 d.

综合上述，我们就可以总结出确定素数的一般方法：一个大于 1 的整数 a 不能被所有不超过 $\sqrt{61}$ 的素数整除，那么 a 一定是素数.

教科书中的例 3 是为了加深学生对埃拉托斯特尼筛法的认识.

关于素数的确定还有其他的一些方法，我们将在“拓展资源”中介绍另一种筛法——钱德拉筛法.

2. 最大公因数与最小公倍数

本节从因数和倍数的概念出发，引出公因数和公倍数的概念，进而引出最大公因数和最小公倍数的概念，并介绍计算两个整数的最大公因数的一种重要方法——辗转相除法. 辗转相除法是初等数论中最重要的方法之一，在第二讲介绍大衍求一术和第三讲介绍二元一次不定方程特解的算法时还会涉及. 学生除了要会准确运用辗转相除法计算两个整数的最大公因数外，还要理解辗转相除法的内容和原理.

本节的一个难点是证明最大公因数的如下重要性质：

设整数 a，b 不同时为零，则存在一对整数 m，n，使得 $(a, b)=am+bn$.

上述性质在求解一次同余方程和不定方程时经常要用到，由它还可以推出整除的一些重要性质.

至于两个整数的最小公倍数的计算问题，我们可以利用恒等式：

$$(a, b)[a, b]=|ab|$$

将其转化为计算这两个整数的最大公因数.

(1) 最大公因数

由两个整数公共的因数引出公因数的概念，继而引出最大公因数和互素的概念. 在理解最大公因数的概念时，要注意两点：一是最大公因数首先是公因数，二是最大公因数是所有公因数中最大的那一个. 在小学阶段，学生已经学习过相关概念，不同的是以前只讨论两个正整数的最大公因数和互素的问题. 教师在选择例子时，选取的两个整数最好不全是正整数.

对多于两个整数的最大公因数和互素的概念可类似地给出，具体教学时可通过一个或两个例子作简要说明. 例如，-6，15，-30 的公因数为 1，-1，3，-3，其中最大的公因数为 3，所以 $(-6, 15, -30)=3$.

关于最大公因数的一个重要问题是最大的公因数的计算. 在小学，我们已经学习过短除法，短除法是否真的能解决好最大公因数的计算问题呢？教科书在“思考”栏目中让学生用短除法计算两组整数的最大公因数，目的是让学生认识到短除法求最大公因数的局限性，即每一次操作必须事先观察到一个大于 1 的公因数，而这一点对两个较大的整数有时难以做到.

例如，用短除法计算 (375，105)：

$$\begin{array}{r|ll} 5 & 375 & 105 \\ \hline 3 & 75 & 21 \\ \hline & 25 & 7 \end{array}$$

所以，(375，105)$=5\times3=15$. 但是，用短除法计算 (1 840，667) 时比较困难，因为我们事先很难观察到 1 840 和 667 的一个大于 1 的公因数. 这样一来，学生马上会产生这样的问题：如何有效地计算任意两个整数的最大公因数呢？一个自然的想法是，把两个较大整数的最大公因数的计算问题转化为两个较小整数的最大公因数的计算问题.

教师引导学生观察、思考带余除法中 a，b 的最大公因数与 r，b 的最大公因数之间的关系. 通过分析发现，a，b 的公因数的集合与 r，b 的公因数集合相同，这表明 $(a, b)=(r, b)$. 所以，要计算 a 与 b 的最大公因数，只需计算 r 和 b 的最大公因数. 然后，教科书按这种思路具体计算 (1 840，667)，加深学生对这种计算最大公因数的方法的认识. 根据学生理解的情况，教师决定是否需要补充其他的例子进行说明.

在此基础上，教师介绍辗转相除法的概念和一般形式. 辗转相除法的一般形式和原理要求学生理解和掌握，这些内容在本专题后面的学习中经常要用到. 另外，要求学生能准确地应用辗转相除法计算两个整数的最大公因数.

辗转相除法与短除法相比，它不需要事先观察出这两个整数的一个大于 1 的公因数，因此它是一个有效的算法，并且容易通过计算机编程实现.

为了体现信息技术在初等数论中的应用，教材上介绍了辗转相除法的算法程序框图，学生可以根据这个算法程序框图，编写一个计算机程序求两个整数的最大公因数. 如下计算机程序（Matlab）可供参考选用：

```
a=1 840;
b=667;
r=mod(a, b);
    while r~=0
    a=b;
    b=r;
    r=mod(a, b);
end
b
```

关于三个整数的最大公因数的求法，教科书是通过“探究”栏目实现的，即通过一些实例，计算发现(a, b, c)与$((a, b), c)$是相等的. 这样一来，让学生认识到可将三个整数的最大公因数的计算转化两次计算两个整数的最大公因数. 并且，对于多于三个整数的情形，也有类似的结论.

关于关系式$(a, b, c)=((a, b), c)$的严格证明，可放在证明了最大公因数的如下重要性质之后：

设整数 a，b 不同时为零，则存在一对整数 m，n，使得$(a, b)=am+bn$. （*）

上述性质非常重要，在第二讲求解一次同余方程和第三讲求解不定方程时经常要用到. 它的证明是本节课的一个难点. 教科书上用辗转相除法证明了性质（*），这是因为《普通高中数学课程标准（实验）》中要求用辗转相除法证明整除的如下性质：

若 $a|bc$，且$(a, b)=1$，则 $a|c$，

而这条性质可由性质（*）导出.

教科书上并没有给出完整的证明过程，只是通过一些具体的步骤让学生理解性质（*）的正确性，过多的抽象符号推演会增加学生认知的难度.

除了辗转相除法外，我们还可以采用下面的证明方法：

令 S 为形如 $ax+by$ 的整数构成的集合，其中 x，y 为任意整数. 显然，集合 S 中至少有一个正整数. 设 S 中最小的正整数为 d，则存在整数 m，n，使得 $d=am+bn$. 下面，我们只需证明 $d=(a, b)$ 即可.

对 S 中任意整数 $ax+by$ 和 d 用带余除法：

$$ax+by=dq+r,\ 0\leqslant r<d.$$

若 $r>0$，则 $r=ax+by-dq=ax+by-(am+bn)q=a(x-mq)+b(y-nq)$ 在集合 S 中，而 $r<d$，这与 d 为集合 S 中最小正整数矛盾，所以 $r=0$，从而 $d|ax+by$.

由于 a，b 都具有 $ax+by$ 的形式，故 $d|a$，$d|b$，即 d 为 a，b 的公因数. 另外，对 a，b 的任意公因数 d'，$d'|a$，$d'|b$，于是 $d'|am+bn=d$，$d'\leqslant d$.

这表明 d 就是 a，b 的公因数中最大的那一个，即 $d=(a, b)$.

由最大公因数的性质（*）还可以观察出：两个整数的公因数一定整除这两个整数的最大公因数，对于多于两个整数的情形，结论仍然成立. 利用这个事实，我们容易证明关系式：$(a, b, c)=((a, b), c)$，具体如下：

设 $d=(a, b, c)$，$d'=((a, b), c)$.

由于 $d|a$，$d|b$，故 $d|(a,b)$. 又由于 $d|c$，故 $d|((a,b),c)=d'$，$d'>d$.

另一方面，由于 $d'|(a,b)$，故 $d'|a$，$d'|b$. 又由于 $d'|c$，故 d' 为 a，b，c 的公因数，从而有 $d'\leqslant d$.

综上所述，$d=d'$.

本小节最后利用最大公因数的性质（*）证明素数的一个重要性质：设 p 为素数，若 $p|ab$，则 $p|a$，或 $p|b$. 这条性质在本讲最后一节“算术基本定理”的证明过程中将要用到.

(2) 最小公倍数

本小节先通过一个思考题引出两个整数的公倍数和最小公倍数的概念，然后通过具体的例子进行说明. 最小公倍数的概念在小学阶段也已经介绍过，当时介绍的是正整数的最小公倍数，现在介绍的是非零整数的最小公倍数，要注意新旧知识的联系和区别. 同样地，教师用例子进行说明时，选取的非零整数最好不全是正整数，这样便于加深学生的认识.

在理解最小公倍数的概念时，要注意两点：一是最小公倍数首先是正的公倍数；二是最小公倍数是所有正的公倍数中最小的一个. 对于多个非零整数的最小公倍数和记号可类似定义. 教师可以通过一个具体的例子说明，例如 4，-12，-6 的公倍数为 12，-12，24，-24，36，-36，…其中最小的正公倍数为 12，所以 $[4,-12,-6]=12$.

在上一小节，我们给出了公因数和最大公因数的关系，即两个整数的公因数总整除它们的最大公因数. 一个自然的问题是公倍数与最小公倍数之间有什么样的关系呢？教科书上证明了两个非零整数的最小公倍数整除它们的每一个公倍数.

为了给出两个整数的最小公倍数的计算方法，教科书让学生通过“探究”栏目认识非零整数 a，b，(a,b)和$[a,b]$之间的关系. 通过计算一些具体的例子，让学生观察到关系式：

$$(a,b)[a,b]=|ab|, \qquad (**)$$

教科书上省略了这个关系式的证明. 这个关系式的证明有两种途径可以实现，其一如下：

不失一般性，设 a，b 均为正整数. 记 $(a,b)=d$，则 $a=a'd$，$b=b'd$，这里 $(a',b')=1$（否则与 $(a,b)=d$ 矛盾）. 下面只需证明：

$$[a'd,b'd]=a'b'd.$$

显然，$a'b'd$ 为 $a'd$，$b'd$ 的正公倍数. 设 m 为 $a'd$，$b'd$ 的任意正的公倍数，m 是 $a'd$ 的倍数，故 $m=a'dm'$. 由于 m 也是 $b'd$ 的倍数，故 $b'd|m=a'dm'$，从而 $b'|a'm'$. 因为 $(a',b')=1$，所以 $b'|m'$，即 $m'=b'q$. 于是，$m=a'b'dq\geqslant a'b'd$. 所以，$[a'd,b'd]=a'b'd$.

另一种途径是运用下一节的算术基本定理.

利用关系式（**），我们可以通过计算两个非零整数的最大公因数来计算它们的最小公倍数. 本小节最后通过一个具体的例子来说明这一事实.

至于多个非零整数的最小公倍数的计算，也可以转化多次计算两个整数的最小公倍数. 教师可以通过三个整数的情形加以说明，如

$$[a,b,c]=[[a,b],c].$$

理由如下：

记 $m=[a,b,c]$，$m'=[[a,b],c]$.

一方面，$a|m$，$b|m$，所以 $[a,b]|m$，又 $c|m$，所以 m 是 $[a,b]$ 和 c 的公倍数. 于是，$m'=[[a,b],c]|m$，$m\geqslant m'$.

另一方面，$[a,b]|m'$，$[a,b]|m'$，由于 $a|[a,b]$，$b|[a,b]$，故 $a|m'$，$b|m'$. 又 $c|m'$，所以 m' 是 a，b 和 c 的正公倍数. 于是，$m'\geqslant m$.

综上所述，$m=m'$.

需要指出的是，最大公因数与最小公倍数的性质除了教科书给出的外，还有许多重要的性质，教师在课堂教学时无需一一列出. 对于学有余力的学生，教师可引导学生探究其中的部分性质，例如：

$(ac, bc)=(a, b)c$，$[ac, bc]=[a, b]c$，其中 $c>0$；

$(a, b)=1$ 当且仅当 $(a^m, b^n)=1$，其中 $m, n>0$. 等等.

3. 算术基本定理

算术基本定理是欧几里得在公元前 3 世纪建立的，是初等数论的基石. 它告诉我们每个大于 1 的正整数可以惟一分解成有限个素数的乘积（不计素数的次序）. 利用算术基本定理，我们可以研究整数的许多重要的性质. 在本节，我们用算术基本定理计算两个整数的最大公因数和最小公倍数. 需要注意的是，算术基本定理只是一个理论结果，实际上，具体计算一个正整数的素因数分解式是非常困难的.

算术基本定理的证明是本节的一个难点，其中素因数分解式存在性在本讲第一节中“素数及其判别法”部分给出，而惟一性的证明需要用到本讲第二节中“最大公因数”部分给出的素数的一个重要性质.

由素因数分解式，我们可以将任何一个正整数 n 根据需要写成有限（或无限）个素数的幂的乘积形式. 例如，将 n 写成所有素数的幂的乘积形式：

$$n=p_1^{k_1}p_2^{k_2}\cdots\ p_t^{k_t}\cdots, \qquad (***)$$

其中不是 n 的素因数的那些素数 p_t 的幂指数 k_t 为零.

若不计分解式中素数的次序，分解式（$***$）是惟一的. 利用分解式（$***$），我们可以计算两个非零整数 a, b 的最大公因数和最小公倍数，具体如下：

不失一般性，设 a, b 均为正整数（注意 a, b 的符号对最大公因数与最小公倍数无影响），并且

$$a=p_1^{k_1}p_2^{k_2}\cdots\ p_t^{k_t}\cdots, \quad b=p_1^{l_1}p_2^{l_2}\cdots\ p_t^{l_t}\cdots, \qquad (1)$$

那么，我们有

$$(a, b)=p_1^{\min\{k_1, l_1\}}①\,p_2^{\min\{k_2, l_2\}}\cdots p_t^{\min\{k_t, l_t\}}\cdots, \qquad (2)$$

$$[a, b]=p_1^{\max\{k_1, l_1\}}②\,p_2^{\max\{k_2, l_2\}}\cdots p_t^{\max\{k_t, l_t\}}\cdots. \qquad (3)$$

在实际应用中，我们通常将 a, b 表示成有限个素数幂的乘积形式，也就是既不是 a 的素因数，也不是 b 的素因数的那些素数在分解式（$***$）中略去不写. 另外，利用（1）（2）和（3）式，我们立即得到最大公因数和最小公倍数的关系式：$(a, b)[a, b]=|ab|$，这是因为

$$k_t+l_t=\min\{k_t, l_t\}+\max\{k_t, l_t\}, \qquad t=1, 2, \cdots.$$

应用算术基本定理，我们可以判断一个正整数是不是某个正整数的平方、立方的问题，还可以确定一个正整数究竟有多少个正因数的问题，这些内容将在“拓展资源”部分详细介绍.

四、教学设计案例

素数及其判别法（1 课时）

1. 教学任务分析

（1）理解素数、合数的概念；

（2）通过观察，理解每个大于 1 的整数一定存在一个素数因数；

（3）通过思考，理解每个大于 1 的整数可以分解成一些素数的乘积；

---

① $\min\{k_1, l_1\}$ 表示取 k_1, l_1 中较小的那个数.

② $\max\{k_1, l_1\}$ 表示取 k_1, l_1 中较大的那个数.

(4) 知道素数有无穷多个，了解确定素数的埃拉托斯特尼筛法.

2. 教学重点与难点

重点：

(1) 每个大于 1 的整数一定存在一个素数因数；

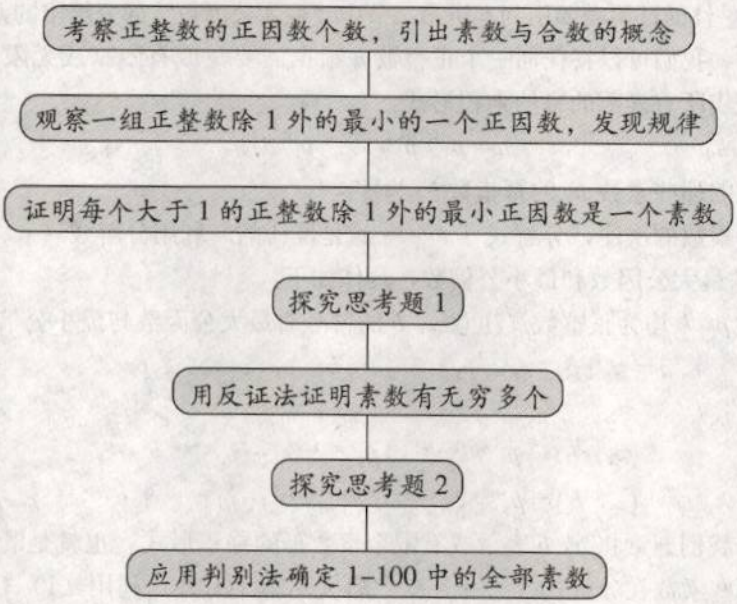
(2) 每个大于 1 的整数可以分解成一些素数的乘积；

(3) 素数有无穷多个；

(4) 确定素数的埃拉托斯特尼筛法.

难点：理解埃拉托斯特尼筛法的原理.

3. 教学基本流程



4. 教学情境设计

问题 1：考察正整数 1，3，13，31，12，14，81 的正因数个数，请问这些整数中哪些有一个正因数，哪些有两个正因数，哪些至少有三个正因数?

设计意图：通过考察正整数的正因数个数，引出素数和合数的概念.

师生活动：教师提出问题，学生讨论. 学生将这些整数根据正因数的个数分类. 教师叙述素数和合数的概念.

问题 2：上面的正整数中，哪一类正整数能分解成两个大于 1 的整数的乘积?

设计意图：让学生知道素数不能分解成两个大于 1 的整数的乘积，而合数能分解成两个大于 1 的整数的乘积，为后面的讨论作铺垫.

师生活动：学生观察上面的正整数，并回答问题. 教师引导学生对素数与合数的概念进行分析，得出一般结论.

问题 3：(1) 找出正整数 6，7，9，21，65，77，121 的正因数，观察每个正整数除 1 外的最小的正因数，从中你能发现什么规律?

(2) 你能说出理由吗?

设计意图：由特殊到一般，得出每一个大于 1 的整数至少存在一个素因数. 同时，让学生体验数

学探究的过程，又知道数学证明的必要性，感知数学的严谨性.

师生活动：学生计算、观察，教师引导，归纳出一般结论，然后尝试给出证明.

问题 4：是否总可将大于 1 的整数分解为一些素数的乘积？为什么？

设计意图：这个问题是前面结果的应用，同时证明了算术基本定理中素因数分解式的存在性，降低学生对算术基本定理的认知难度.

师生活动：学生独立思考后回答，并说明理由. 教师引导学生用问题 3 探究得到的结论解决问题 4，并通过具体的例子加深学生对结论“任何大于 1 的整数总可分解为一些素数的乘积”的正确性的认识.

问题 5：既然任何大于 1 的整数总可分解为一些素数的乘积，那么素数有多少个？有限还是无限？为什么？

设计意图：让学生知道素数有无限多个，并了解用反证法证明这个结论的过程和相关的历史背景知识.

师生活动：由于结论证明的技巧性比较强，让学生独立思考解决会有很大的困难，所以教师在问题解决的过程要加强引导.

师：素数有多少个？有限还是无限？

生 1：有限个.

生 2：无限个.

师：如果是有限个，不妨素数共有 k 个且为 m_1，m_2，…，m_k，那么我们从前面的探究中能发现什么？

生：每个大于 1 的整数一定有一个素数因数，从而一定能被 m_1，m_2，...，m_k 中某个素数整除.

师：这可能吗？

生：不可能. 因为可以找到某个大于的整数不能被 m_1，m_2，...，m_k 中任何一个整除.

师：找出一个这样的整数.

生：例如，整数 $N=m_1m_2\ldots m_k+1$ 就不能被 m_1，m_2，...，m_k 中任何一个素数整除.

师：这意味着什么？

生：素数不可能只有有限个. 也就是说，素数一定有无限个.

问题 6：对给定的大于 1 的整数，如何判断它是不是一个素数？例如，如何判断 61 是不是素数？

设计意图：判断一个整数是不是素数是一个很自然的问题，也是十分重要的问题.《普通高中数学课程标准（实验）》中要求学生了解一种判别法（筛法）.

师生活动：教师通过提出问题，引导学生思考，并逐步解决问题，最后归纳出一般结论.

师：要判断 61 是不是素数，关键在于 61 是否有介于 2－60 之间的因数，那么是否需要用 2－60 之间的数一一试除 61 呢？

生：不需要.

师：为什么？

生：d 是 61 的介于 2－60 之间的因数，$61/d$ 也是 61 介于 2－60 之间的因数，这两个因数中最小的一个不超过 $\sqrt{61}$.

师：要判断 61 是不是素数，是否需要将大于 1 且不超过 $\sqrt{61}$ 的整数一一试除 61 呢？

生：不需要. 因为大于 1 的整数一定存在素数因数，如果这个整数是 61 的因数，则它的素数因数也是 61 的因数. 所以只需用不超过 $\sqrt{61}$ 的素数一一试除 61 即可.

师：非常好. 61 是素数吗？

生：是. 因为不超过 $\sqrt{61}$ 的素数为 2，3，5，7，它们均不整除 61，所以 61 是素数.

师：对. 我们现在给出一般的判别法：如果大于1的整数 a 不能被所有不超过$\sqrt{a}$的素数整除，那么 a 一定是素数.

问题7：请同学们用前面的判别法找出1－100中的全部素数.

设计意图：加深学生对素数判别法的认识，同时了解埃拉托斯特尼筛法.

师生活动：师生一起分析思路，由学生完成求解.

最后，教师引导学生从知识和方法两个方面对本小节的内容进行小结，同时提出进一步思考的问题.

五、习题解答

习题（第7页）

1. 解：能被3整除的整数：45，120，189，56 382；

能被7整除的整数：98，189，1 001；

能被9整除的整数：45，189；

能被11整除的整数：1 001，1 331.

2. 能被11整除的5位正整数的特征：一个5位正整数的个、百、万位数字之和与十、千位数字之和的差能被11整除，那么这个5位正整数能被11整除.

证明：设5位正整数 N 的个、十、百、千、万位数字分别为 a，b，c，d，e，则

$$\begin{aligned}N&=e\times(11-1)^4+d\times(11-1)^3+c\times(11-1)^2+b\times(11-1)+a\\&=11R+(a+c+e)-(b+d).\end{aligned}$$

因为 $11\mid 11R$，如果 $11\mid(a+c+e)-(b+d)$，那么 $11\mid N$.

3. 解：设除数为 b，余数为 r，则

$$1\,626=81b+r,\ 0\leqslant r<b.$$

由此可得

$$81b\leqslant 1626<81b+b=82b,$$

从而有

$$81\leqslant\frac{1\,626}{b}<82,$$

所以

$$\frac{1\,626}{82}<b\leqslant\frac{1\,626}{81},$$

即

$$19\frac{34}{41}<b\leqslant 20\frac{6}{81}.$$

因此，$b=20$，$r=1\,626-81\times 20=6$.

4. 解：(1) 因为 $343<361=19^2$，$\sqrt{343}<19$，所以不超过$\sqrt{343}$的素数为2，3，5，7，11，13，17，依次检验这些素数是否整除343. 检验发现，7整除343，所以343不是素数.

(2) 因为 $2\,027<2\,116=46^2$，$\sqrt{2\,027}<46$，所以不超过$\sqrt{2\,027}$的素数为2，3，5，7，11，13，17，19，23，29，31，37，41，43. 依次检验这些素数是否整除2 027. 检验发现，这些素数均不整除2 027，所以2 027是素数.

习题（第13页）

1. 解：(1) $-39=52\times(-1)+13$，$52=13\times 4+0$，所以

$(-39, 52)=13$，　　$[-39, 52]=\dfrac{|-39\times 52|}{13}=156$；

(2) $161=46\times 3+23$，$46=23\times 2+0$，所以

$(161, 46)=23$，$[161, 46]=\dfrac{|161\times 46|}{23}=322$；

(3) $-144=76\times(-2)+8$，$76=8\times 9+4$，$8=4\times 2+0$，则

$(-144, 76)=4$，$[-144, 76]=\dfrac{|-144\times 76|}{4}=2\,736$；

$42=4\times 10+2$，$4=2\times 2+0$，则$(4, 42)=2$；

$2\,736=42\times 65+6$，$42=6\times 7+0$，则$(2\,736, 42)=6$，

$[2\,736, 42]=\dfrac{|2\,736\times 42|}{6}=19\,152$. 所以

$(-144, 76, 42)=((-144, 76), 42)=(4, 42)=2$，

$[-144, 76, 42]=[[-144, 76], 42]=[2\,736, 42]=19\,152$.

(4) $-56=84\times(-1)+28$，$84=28\times 3+0$，则

$(-56, 84)=28$，$[-56, 84]=\dfrac{|-56\times 84|}{28}=168$；

$76=28\times 2+20$，$28=20\times 1+8$，$20=8\times 2+4$，$8=4\times 2+0$，则$(28, 76)=4$；

$168=76\times 2+16$，$76=16\times 4+12$，$16=12\times 1+4$，$12=4\times 3+0$，则

$(168, 76)=4$，$[168, 76]=\dfrac{|168\times 76|}{4}=3\,192$. 所以

$(-56, 84, 76)=((-56, 84), 76)=(28, 76)=4$，

$[-56, 84, 76]=[[-56, 84], 76]=[168, 76]=3\,192$.

2. 解：$46=35\times 1+11$，$35=11\times 3+2$，$11=2\times 5+1$，所以

$1=11-2\times 5=11-(35-11\times 3)\times 5=11\times(1+3\times 5)-35\times 5$

$=11\times 16-35\times 5=(46-35\times 1)\times 16-35\times 5$

$=46\times 16-35\times(1\times 16+5)=46\times 16-35\times 21$.

于是选取 $m=-21$，$n=16$ 即可.

3. 证明：因为 $a|c$，所以 $c=aq$. 又因为 $b|c$，所以 $b\mid aq$，而$(a, b)=1$，所以 $b|q$，即 $q=bs$.

于是，$c=aq=abs$. 所以，$ab|c$.

4. 解：注意到 6，12，18，…，2 004 是 1－2 004 中所有 6 的倍数. 这些整数是 334 的倍数，当且仅当它们是[6，334]的倍数. 而(6，334)=2，所以

$$[6, 334]=\frac{6\times 334}{2}=1\,002,$$

而 1－2 004 中 1 002 的倍数为 1 002，2 004，共计 2 个.

因此，6，12，18，…，2 004 中 334 的倍数的个数为 2.

习题（第 14 页）

解：因为 152，216 所有的素因数为 2，3，19，并且

$$152=2^3\times 3^0\times 19^1,\qquad 216=2^3\times 3^3\times 19^0,$$

所以

$$(152, 216)=2^3\times 3^0\times 19^0=8,\qquad [152, 216]=2^3\times 3^3\times 19^1=4\,104.$$

用素因数分解式计算两个整数的最大公因数和最小公倍数需要事先确定这两个整数的所有素因数，

进而写出分解式，有时实现起来十分困难，尤其是两个整数较大时. 所以，与辗转相除法相比，利用素因数分解式计算最大公因数和最小公倍数的方法不是一个有效的算法. 但是，素因数分解式是一个重要的理论结果.

六、拓展资源

1. 素数有无限多的另证

关于素数有无限多个的结论，教科书中介绍了一种反证法，这里我们介绍另外一种证明方法. 我们先证明一个更强的结论：

设 n 为大于 2 的自然数，则在 n 与 $n!$ 之间一定存在一个素数. 其证明过程如下：

用 m_1，m_2，...，m_k 表示所有不超过 n 的素数，定义整数：

$$N=m_1m_2\cdots m_k-1.$$

显然，$N\geqslant 2$. 那么，N 一定有一个素因数 m. 注意到素数 m_1，m_2，...，m_k 均不是 N 的因数，所以 m 一定是大于 n 的素数. 而 $m\leqslant n!-1<n!$，故 m 为介于 n 与 $n!$ 之间的素数.

根据上述结论，3 与 $3!=6$ 之间存在一个素数，6 与 $6!=720$ 之间存在一个素数，720 与 $720!$ 之间存在一个素数……如此进行下去，我们就可以得到无限多个素数.

2. 桑达拉姆（Sundaram）筛法

教科书中介绍了确定素数的一种方法——埃斯托拉特尼筛法，这里我们补充介绍另一种筛法，称之为桑达拉姆筛法.

1934 年，东印度年轻学生桑达拉姆构造了如下一个关于主对角线对称的数阵：

4，7，10，13，16，19，…

7，12，17，22，27，32，…

10，17，24，31，38，45，…

13，22，31，40，49，58，…

16，27，38，49，60，71，…

19，32，45，58，71，84，…

… … … … … … …

其中第 k 行是首项为 $4+3(k-1)$，公差为 $2k+1$ 的等差数列，$k=1$，2，….

桑达拉姆发现：若正整数 n 出现在上面数阵中，则 $2n+1$ 不是素数；若正整数 n 不出现在上面数阵中，则 $2n+1$ 肯定是素数.

从数阵的构造方法中，我们可以发现位于数阵第 i 行、第 j 列交叉处数的表达式为：

$$a=3i+1+(2i+1)(j-1).$$

若正整数 n 出现在上面的数阵中，不妨出现在第 i 行、第 j 列交叉处，则

$$\begin{aligned}2n+1&=2[3i+1+(2i+1)(j-1)]+1\\&=2[(2i+1)j+i]+1\\&=(2i+1)j+2i+1\\&=(2i+1)(2j+1),\end{aligned}$$

其中 $2i+1$ 与 $2j+1$ 均大于 1，所以 $2n+1$ 是合数，不是素数.

若正整数 n 不出现在上面的数阵中，则 $2n+1$ 一定是素数而不是合数，否则 $2n+1=ab$，其中 a，

b 均为大于 1 的奇数. 不妨设 $a=2j+1$，$b=2i+1$，则

$$\begin{aligned}2n+1 &=(2j+1)(2i+1)\\ &=2[j(2i+1)+i]+1.\end{aligned}$$

于是，

$$n=j(2i+1)+i=3i+1+(j-1)(2i+1)$$

是数阵中 i 行、第 j 列交叉处的数，与假设矛盾.

需要指出的是，桑达拉姆筛法不能筛出偶素数 2.

3. 正因数的个数

我们知道，6 有 4 个正因数：1，2，3，6；12 有 6 个正因数. 那么，120，1 200，12 000 它们分别有多少个正因数呢？这里，我们介绍一种计算正整数的正因数个数的方法.

设 n 为正整数，用 $d(n)$ 表示 n 的正因数个数. 设 n 的素因数分解式为

$$n=p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}, \qquad (*)$$

其中 p_1，p_2，…，p_t 为互不相同的素数，k_1，k_2，…，k_t 为正整数. 如果正整数 d 为 n 的一个因数，那么 d 的素因数也一定是 n 的素因数，于是 d 可以写成下面的形式：

$$d=p_1^{l_1}p_2^{l_2}\cdots p_t^{l_t}. \qquad (**)$$

因为 $d\mid n$，根据素数的性质可以证明：$0\leqslant l_i\leqslant k_i$，$i=1,\ldots,t$. 反过来，如果一个正整数 d 可以表示成（**）的形式，且 $0\leqslant l_i\leqslant k_i$，$i=1,\cdots,t$，容易检验，$d$ 一定是 n 的正因数. 这样一来，给定一组非负整数 l_1，l_2，…，l_t，$l_i\leqslant k_i$，$i=1,\cdots,t$，就惟一对应着 n 的一个正因数，因此 n 的正因数个数为

$$d(n)=(k_1+1)(k_2+1)\cdots(k_t+1). \qquad (***)$$

例如，$120=2^3\times3^1\times5^1$，所以 120 的正因数个数为 $d(120)=(3+1)(1+1)(1+1)=16$. 类似地，我们可以计算得 1 200，12 000 的正因数个数分别为 30，48.

4. 完全平方数

一个正整数 n 是某个正整数的平方，则称 n 为完全平方数. 由于 $1=1^2$，$4=2^2$，$9=3^2$，$16=4^2$，$121=11^2$，所以 1，4，9，16，121 都是完全平方数. 对给定的正整数，如何判断它是不是一个完全平方数呢？下面利用素因数分解式给出完全平方数的一个判别法.

设 n 的素因数分解式如（*）式所示. 若 n 是一个完全平方数，且 $n=a^2$，则 a 是 n 的正因数. 于是，a 可以写成（**）式的形式：$a=p_1^{l_1}p_2^{l_2}\cdots p_t^{l_t}$，此时

$$n=p_1^{2l_1}p_2^{2l_2}\cdots p_t^{2l_t}. \qquad (****)$$

由于 n 的素因数分解式是惟一的，所以

$$k_1=2l_1,\ k_2=2l_2,\ \ldots,\ k_t=2l_t,$$

即 n 的素因数分解式中每个素因数的幂指数为偶数. 反过来，如果 n 的素因数分解式中每个素因数的幂指数为偶数，即（****）式成立，那么 n 一定是一个完全平方数，因为

$$n=p_1^{2l_1}p_2^{2l_2}\cdots p_t^{2l_t}=(p_1^{l_1}p_2^{l_2}\cdots p_t^{l_t})^2.$$

注意到，（*）式中所有的幂指数 k_i 为偶数当且仅当 $d(n)$ 为奇数. 于是，我们有下面的判别法.

定理 一个正整数 n 为完全平方数当且仅当 n 有奇数个正因数.

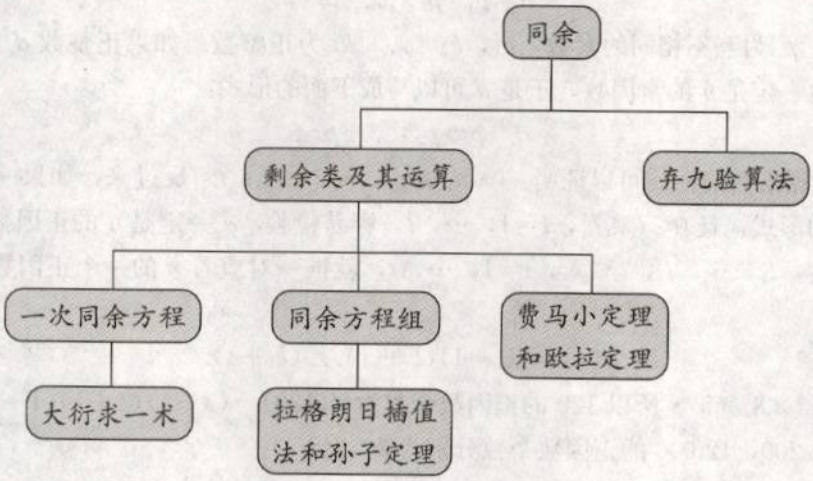
例 一个房间有一百盏灯，分别被编号为 1 至 100 的开关可控制着. 一开始房间内所有的灯是灭的. 第 1 个人进入房间后，把编号为 1 的倍数的开关拉一下；第 2 个人进入房间后，把编号为 2 的倍数的开关拉一下；如此进行下去，直至第 100 个人进入房间后，把编号为 100 的倍数的开关拉一下，

问最后房间内有哪些灯是开的?

解：由于房间内的灯一开始都是关的，故每一盏灯最后是开的还是关的，决定于控制它的开关被拉了奇数下还是偶数下. 而一个开关被拉了多少下与这个开关的编号的正因数个数是一致的. 所以，一个开关被拉了奇数下当且仅当它的编号有奇数个正因数. 于是，编号有奇数个正因数的开关控制的灯是开的. 由定理知，这些编号为完全平方数. 而1至100中的完全平方数为1，4，9，16，25，36，49，64，81，100，故最后编号为1，4，9，16，25，36，49，64，81，100的开关控制的灯是开的.

第二讲 同余与同余方程

一、本讲知识结构



二、教学重点与难点

重点：

1. 理解同余的概念和性质，会用同余的性质简化数论中的一些问题，如星期几问题、整除问题；

2. 理解剩余类的概念，体会剩余类加法、乘法运算与整数的加法、乘法运算之间的联系与差别；

3. 理解费马小定理和欧拉定理的内容与证明过程，会用这两个定理简化数论中的一些计算问题，如求余数问题；

4. 体验一次同余方程的求解过程，感受和体会其中所蕴含的数学思想方法，会解一次同余方程；

5. 理解大衍求一术的算法步骤和原理；

6. 理解拉格朗日插值公式的建立过程，以及用建立拉格朗日插值公式的思路推导孙子定理的过程，会用孙子定理解一次同余方程组；

7. 会用弃九验算法验算正整数的计算结果是否正确，知道弃九验算法只能“检错”，不能“判正”.

难点：

1. 剩余类的概念及其运算；

2. 费马小定理和欧拉定理的证明过程，以及灵活运用这两个定理简化数论中的一些计算；

3. 一次同余方程组的求解过程；

4. 大衍求一术的算法步骤和原理；

5. 建立拉格朗日插值公式和推导孙子定理.

三、编写意图与教学建议

同余理论是建立在整数的整除理论基础上的，它刻画了整数之间一种更精细的关系——同余关系. 同余概念的引入，极大地丰富了数论的内容，简化了数论中的许多问题. 本讲介绍同余理论中最基本的一些内容，如同余的概念与性质、费马小定理和欧拉定理、一次同余方程的求解、孙子定理、弃九验算法.

在介绍费马小定理和欧拉定理之前，我们先介绍了剩余类的概念及其运算，目的有三：一是为证明费马小定理和欧拉定理做准备；二是让学生了解除了通常的数集外，还有另外一类带有运算的集合，并感受它们运算性质的异同；三是为本讲后面引出一次同余方程或方程组的问题做铺垫. 另外，在介绍孙子定理之前，我们先介绍了拉格朗日插值公式的建立过程，这是因为孙子定理先特解而后求通解的思路与建立拉格朗日插值公式是一样的，因此列入建立拉格朗日插值公式一节有助于学生加强有关内容的联系的意识.

在编写教科书时，对一些基本的知识点，如同余的概念与性质、剩余类的概念与运算、同余方程（方程组）的解的概念，为了便于学生理解，我们安排了大量的例子进行说明. 对一些重要的方法，如利用同余简化数论中的问题、利用费马小定理和欧拉定理简化数论中的计算、大衍求一术、弃九验算法等，要求学生不仅会灵活运用这些方法解决一些简单的数论问题，还要求学生明白这些方法的基本原理.

在介绍新概念、新定理和新方法之前，教科书中采用了观察、思考、探究等方式，让学生通过考察具体的实例，逐步归纳总结出一般结论和方法，同时体验问题解决过程中蕴含的数学思想方法. 这样不仅可以降低学生的认知难度，还可以提高学生学习的积极性，以及提出问题、分析问题和解决问题的能力.

同余是本讲知识系统的逻辑起点，由它对整数集合进行分类，引出剩余类的概念及其运算，进而引出费马小定理和欧拉定理以及一次同余方程（方程组）. 再由一次同余方程的求解问题引出大衍求一术，由一次同余方程组的求解问题引出孙子定理. 为了推导孙子定理，增加了建立拉格朗日插值公式一节，因为它们先特解而后求通解的思路是一样的. 最后，本讲介绍同余在算术里的一个应用——弃九验算法.

1. 同余

本节由两部分内容构成：同余的概念和同余的性质. 同余的性质是本节的重点，而灵活运用同余的性质简化数论中的问题，如星期几问题、整除问题是学生学习的一个难点.

(1) 同余的概念

本小节通过观察月历表中位于同一列的整数的特征，引出同余的概念. 在介绍同余的概念时，教师一定要强调“模 n”两字. 因为对不同的模 n，整数 a 与 b 有时是模 n 同余的，有时不是模 n 同余的. 例如，1 与 3 是模 2 同余的，但不是模 5 同余的. 另外，在引入同余式的记号“$a\equiv b(\bmod n)$”时，要注意同余式与恒等式“$a=b$”的差别. 在书写同余式时，许多学生容易漏掉“$(\bmod n)$”.

同余和整除存在密切的联系，教科书的“思考”栏目旨在让学生明确这两个概念间的具体关系. 教学时，教师可以引导学生直接从同余的概念出发，由带余除法推导出下面的结论：

$$a\equiv b(\bmod n)\Leftrightarrow n\mid a-b. \qquad (*)$$

利用结论（*），我们容易证明教科书第 16 页“探究”栏目中同余的三条基本性质，具体如下：

(1) 因为 $n|a-a=0$，所以 $a\equiv a(\mathrm{mod}\ n)$；

(2) 因为 $a\equiv b(\mathrm{mod}\ n)$，所以 $n|a-b$，从而有 $n|b-a$，于是 $b\equiv a(\mathrm{mod}\ n)$；

(3) 因为 $a\equiv b(\mathrm{mod}\ n)$，$b\equiv c(\mathrm{mod}\ n)$，所以 $n|a-b$，$n|b-c$，从而有 $n|(a-b)+(b-c)=a-c$，于是 $a\equiv c(\mathrm{mod}\ n)$.

需要指出的是，模 n 同余实际上给出了整数之间一种比整除更精细的关系——同余关系. 同余的性质 (1) (2) 和 (3) 分别称为同余关系的自反性、对称性和传递性. 正是同余关系的这三个性质，使我们利用它可以将整数集分成若干类，使得每一类的任何两个整数彼此模 n 同余，不同类的任何两个整数彼此模 n 不同余. 本小节最后通过学生熟悉的事实进行说明：整数集可以分成奇数集和偶数集两类，而它们恰好是利用模 2 同余关系对整数集进行分类的结果.

(2) 同余的性质

从教科书第 16 页的“探究”可以看出，同余式 $a\equiv b(\mathrm{mod}\ n)$ 与等式 $a=b$ 具有许多类似的性质. 在本小节，我们将类比等式的性质进一步探讨同余式的其他性质. 这些性质对处理数论中的星期几问题和整除问题等有重要的作用.

本小节探究栏目中的性质 1 (1) 与性质 2 的证明在教科书中已经给出，性质 1(2)(3)(4) 的证明如下：

(2) 因为 $a\equiv b(\mathrm{mod}\ n)$，$c\equiv d(\mathrm{mod}\ n)$，所以 $n|a-b$，$n|c-d$. 而 $ac-bd=a(c-d)+d(a-b)$，所以 $n|ac-bd$，从而 $ac\equiv bd(\mathrm{mod}\ n)$；

(3) 因为 $a\equiv b(\mathrm{mod}\ n)$，所以 $n|a-b$，从而对任意整数 k，$n|k(a-b)=ka-kb$. 所以 $ka\equiv kb(\mathrm{mod}\ n)$；

(4) 因为 $a\equiv b(\mathrm{mod}\ n)$，所以 $n|a-b$，而对任意正整数 m，

$$a^m-b^m=(a-b)(a^{m-1}+a^{m-2}b+\cdots ab^{m-2}+b^{m-1}),$$

所以 $n|a^m-b^m$，从而 $a^m\equiv b^m(\mathrm{mod}\ n)$.

需要注意的是，性质 1 与等式相应的性质是一致的，性质 2 可以看作是同余意义下的消去律，消去律成立的前提条件是 a 与 n 互素，这与等式相应的性质有区别. 例如，$2\cdot 1\equiv 2\cdot 3(\mathrm{mod}\ 4)$，$2\neq 0$，但 $1\not\equiv 3(\mathrm{mod}\ 4)$.

作为同余性质的两个具体应用，教科书上的例 1 是学生比较熟悉的星期几问题，例 2 是整除问题. 如果用第一讲介绍的整数的整除性理论求解这两类问题，那么求解过程非常麻烦. 如果用同余的性质求解这两类问题，就简单多了. 这两类问题有一个共同的特点，就是求一个正整数去除另一个指数型整数的余数，后者的底数与指数通常较大. 注意，例 2 本质上是证明 17 除 $19^{1\,000}$ 的余数为 1. 我们采用的方法是将被除数逐步变小：先用除数去除被除数的底数，再用余数替换被除数的底数，然后再降次使底数变大，反复进行这个过程，直至去掉指数. 教科书第 18 页习题中第 4 题也是这一类型的问题，它实际上是求 100 除 3^{50} 的余数.

2. 剩余类及其运算

剩余类及其运算是本讲的一个难点，在本讲中起着承上启下的作用. 我们在本讲第一节中已经指出，利用同余关系可以对整数集进行分类. 例如，当 n 为正整数时，按模 n 是否同余可将整数集分成 n 个彼此不相交的子集，这 n 个集合分别为：

$S_1=\{kn|k\text{ 为任意整数}\}$，

$S_2=\{kn+1|k\text{ 为任意整数}\}$，

……

$S_n=\{kn+n-1|k\text{ 为任意整数}\}$.

其中 S_i 为所有模 n 同余于 $i-1$ 的整数构成的集合，$i=1,2,\cdots,n$.

特别地，当 $n=2$ 时，S_1 为偶数集，S_2 为奇数集. 教材上讨论了 $n=6$ 的情形，目的是进一步加深学生对这些子集的认识.

上面的集合 S_1，S_2，…，S_n 称为模 n 的剩余类，通常用符号 $[a]$ 表示整数 a 所在的剩余类，并称 a 为剩余类 $[a]$ 的一个代表元. 于是，$S_1=[0]$，$S_2=[1]$，…，$S_n=[n-1]$. 需要指出的是，同一剩余类可用不同的代表元表示，这一点往往是学生感到困惑的. 为了突出这一点，教科书证明了如下结论：

$$a\equiv b(\bmod n)\Leftrightarrow[a]=[b].$$

为了叙述简便，教科书在不引起混淆的情况下，将模 n 的剩余类 $[a]$ 简称为剩余类 $[a]$. 教学时教师应向学生说明，以免对学生产生误导.

教科书第 19 页的“探究”是为引入剩余类的加法、乘法运算做准备的，希望学生通过探究得到下面的认识：

设 $[a]$，$[b]$ 为模 n 的两个剩余类，对任意 $c\in[a]$，$d\in[b]$，

(1) 所有 $c+d$ 都在剩余类 $[a+b]$ 中；

(2) 所有 cd 都在剩余类 $[ab]$ 中.

有了上面的认识后，我们可以将剩余类视为一种特殊的“数”. 如同整数一样，对这些“整数”引入相应的运算，一种称为剩余类加法，一种称为剩余类乘法，进而引入模 n 的剩余类环的概念. 事实上，类似于整数的减法运算，我们也可以引入剩余类减法运算：

剩余类减法：$[a]-[b]=[a-b]$.

为了加深学生对剩余类加法、乘法运算的认识，同时为了考察这两种剩余类运算的运算律，教科书第 20 页的“探究”让学生填写模 5 的剩余类加法和乘法的运算表，并观察表中蕴含的运算律. 结果如下：

模 5 的剩余类加法运算表

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

模 5 的剩余类乘法运算表

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

由模 5 的剩余类加法和乘法运算表可以发现：

1^0 如同整数的加法、乘法，剩余类加法、乘法运算也满足交换律、结合律和分配律：

(1) 交换律：$[a]+[b]=[b]+[a]$，$[a][b]=[b][a]$；

(2) 结合律：$([a][b])[c]=[a]([b][c])$，

$$([a]+[b])+[c]=[a]+([b]+[c]);$$

(3) 分配律：$[a]([b]+[c])=[a][b]+[a][c]$.

2^0 剩余类 $[0]$，$[1]$ 与整数集中的 0，1 具有同样的运算性质：

$$[a]+[0]=[0]+[a]=[a];$$

$$[a][0]=[0][a]=[0];$$

$$[a][1]=[1][a]=[a].$$

3^0 对每个剩余类 $[a]$，存在剩余类 $[b]$，使得

$$[a]+[b]=[b]+[a]=[0].$$

4^0 对某些剩余类 $[a]$，存在剩余类 $[b]$，使得

$$[a][b]=[b][a]=[1].$$

基于事实 2^0，我们把$[0]$，$[1]$分别叫做模 n 的剩余类环的零元和单位元.

基于事实 3^0，我们把$[b]$叫做模 n 的剩余类环$[a]$的负元，每个剩余类$[a]$均有负元. 负元的概念类似于数集中一个数的相反数的概念.

基于事实 4^0，我们把$[b]$叫做模 n 的剩余类环$[a]$的逆元. 在模 5 的剩余类环中，每个非零元$[a]$均有逆元. 逆元的概念类似于数集中一个数的倒数的概念.

我们知道，在整数集中只有 1，-1 才有倒数. 因此，模 5 的剩余类乘法运算与整数的乘法运算是有区别的. 那么，在模 n 的剩余类环中，是不是每个非零元均有逆元，如果不是，什么样的非零元才有逆元?

教科书第 21 页的“思考”栏目通过填写模 6 的剩余类环的乘法运算表，考察在模 6 的剩余类环中是不是每个非零元均有逆元. 结果如下：

模 6 的剩余类乘法运算表

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

我们发现，在模 6 的剩余类环中，$[2]$，$[3]$，$[4]$不存在逆元，而$[1]$，$[5]$存在逆元. 并且，剩余类存在逆元当且仅当其代表元与 6 互素. 由此，我们猜想更一般的结论：

在模 n 的剩余类环中，非零元有逆元的充要条件是$(a, n)=1$.

教科书是通过分析得到上述结论的，教师教学时也可以先猜想出一般结论，然后再给出证明. 在本节最后，我们指出了剩余类乘法运算与整数乘法运算的一个重要区别，即任何两个非零整数的乘积一定不等于零，而两个非零剩余类的乘积可能为零元，从模 6 的剩余类乘法运算表也可以看出这一点. 由此，我们引出零因子的概念.

一个自然的问题是，什么样的剩余类环是无零因子的呢? 可以证明：如果 n 是 1 或素数，那么模 n 的剩余类环无零因子，否则就有零因子. 这是因为：

当 $n=1$ 时，结论显然成立.

当 n 为合数时，设 $n=ab$，其中 $1<a, b<n$. 显然，$[a]\neq[0]$，$[b]\neq[0]$，但是$[a][b]=[ab]=[n]=[0]$. 这表明，模 n 的剩余类环有零因子.

当 n 为素数时，对任意剩余类$[a]$，$[b]$，如果$[a][b]=[ab]=[0]$，则 $ab\equiv 0(\mathrm{mod}\ n)$，$n|ab-0=ab$. 所以，$n|a$，或 $n|b$，从而 $a\equiv 0(\mathrm{mod}\ n)$，或 $b\equiv 0(\mathrm{mod}\ n)$. 于是$[a]=[0]$，或$[b]=[0]$.

3. 费马小定理和欧拉定理

前面指出，当 n 为素数时，模 n 的剩余类环是无零因子的. 事实上，除此之外，我们还能探究出这种剩余类环的另一个重要特征. 教科书第 22 页的“探究”首先考察模 3 的剩余类环，然后进一步考察模 5 的剩余类环和模 7 的剩余类环，最后猜想出一般规律：

设 m 为素数. 在模 m 的剩余类环中，对任意剩余类$[a]$，总有$[a^m]=[a]$，或等价地，$a^m\equiv a(\mathrm{mod}\ m)$.

这就是著名的费马小定理. 通过上述过程引出费马小定理，有两方面的好处：一是降低学生对费马小定理的认知难度，相对于直接给出费马小定理，然后进行分析和证明的教学方式，前者更容易被学生接受；二是在费马小定理的证明过程中，要用到剩余类的知识. 前面的“探究”表明，这两者之间是有联系的.

费马小定理的证明是本节学生学习的一个难点. 教科书上的证明写得比较简洁，具体教学时，教师板书可以写得更细致些. 例如，

(1) 补充说明 a，$2a$，$3a$，…，$(m-1)a$ 模 m 两两不同余的理由：

如果 $ka\equiv la(\mathrm{mod}\ m)$，其中 $k\geqslant 1$，$m-1\geqslant l$，那么根据同余意义下的消去律知，$k\equiv l(\mathrm{mod}\ m)$，从而 $m|k-l$. 而$-(m-1)\leqslant k-l\leqslant m-1$，故 $k-l=0$，所以 $k=l$. 这表明，a，$2a$，$3a$，…，$(m-1)a$ 模 m 两两不同余.

(2) 补充说明 $a\times 2a\times 3a\times\cdots\times(m-1)a\equiv 1\times 2\times 3\times\cdots\times(m-1)(\mathrm{mod}\ m)$成立的理由：

因为 a，$2a$，$3a$，…，$(m-1)a$ 模 m 两两不同余，所以这 $m-1$ 个数分别属于模 m 的除$[0]$以外的 $m-1$ 个不同的剩余类，而 1，2，3，…，$m-1$ 为这 $m-1$ 个不同的剩余类的代表元，于是

$$a\equiv k_1(\mathrm{mod}\ m),\ 2a\equiv k_2(\mathrm{mod}\ m),\ 3a\equiv k_3(\mathrm{mod}\ m),\ \cdots,\ (m-1)a\equiv k_{m-1}(\mathrm{mod}\ m),$$

这里 k_1，k_2，k_3，…，k_{m-1} 为 1，2，3，…，$m-1$ 的一个排列. 因此，

$$\begin{aligned}a\times 2a\times 3a\times\cdots\times(m-1)a &\equiv k_1\times k_2\times k_3\times\cdots\times k_{m-1}\\ &=1\times 2\times 3\times\cdots\times(m-1)(\mathrm{mod}\ m).\end{aligned}$$

在证明完费马小定理之后，我们通过考察 $a=8$，$m=5$ 的情形促进学生对证明过程的理解.

欧拉定理是费马小定理的推广，我们可以用证明费马小定理的方法证明欧拉定理. 教科书上没有略去欧拉定理的证明过程，其目的是通过重复这个证明过程（不是简单的复制），进一步加深学生对这种证明方法的认识. 在证明过程中，有两点需要注意：

(1) 要用到下面的结论：

$$\text{设}(a,\ c)=1,\ (b,\ c)=1,\ \text{则}(ab,\ c)=1.$$

假设$(ab,\ c)=d>1$，则存在素数 $p|d$，于是 $p|c$，且 $p|ab$. 由 $p|ab$ 知，$p|a$，或 $p|b$. 当 $p|a$ 时，$p|(a,\ c)=1$矛盾；当 $p|b$ 时，$p|(b,\ c)=1$ 矛盾. 所以假设不成立，从而$(ab,\ c)=1$.

(2) 要用到 aa_1，aa_2，…，aa_r 模 m 两两不同余的事实，其正确性是容易检验的. 教科书上的证明没有强调这一点，教师在教学时有必要补充说明一下.

欧拉定理的内容涉及到欧拉函数的概念. 欧拉函数 $\varphi(m)$的一般表达式的推导在教科书附录一中给出，我们将在本讲“拓展资源”部分给出它的几个简单应用.

本节最后介绍欧拉定理和费马小定理在简化计算方面的应用. 例 3 是用费马小定理简化求余数的问题，例 4 是用欧拉定理简化较大整数的同余问题. 需要指出的是，例 3 用例 2 的方法也很容易解决，如下：

$$13^{2\,004}=169^{1\,002}=(170-1)^{1\,002}\equiv(-1)^{1\,002}=1(\mathrm{mod}\ 17),$$

因此，$13^{2\,004}$除以 17 的余数为 1.

4. 一次同余方程

(1) 一次同余方程

教科书从解剩余类环中的方程问题出发，引出同余方程和一次同余方程的概念，这样既可以加强新旧知识的联系，又使新问题的产生过程比较自然. 此外，这样处理使学生容易理解为什么同余方程 $ax\equiv b(\mathrm{mod}\ n)$的解形式为 $x\equiv c(\mathrm{mod}\ n)$，而不是 $x=c$.

我们知道，剩余类环中的方程$[a][x]=[b]$可以写成$ax\equiv b(\mathrm{mod}\ n)$的形式，而方程的解$[x]=[c]$也可以写成同余式$x\equiv c(\mathrm{mod}\ n)$的形式. 自然地，我们把$x\equiv c(\mathrm{mod}\ n)$称为同余方程$ax\equiv b(\mathrm{mod}\ n)$的解. 在这种意义上，同余方程的解是一个剩余类，是一个集合，而不是一个整数.

当$c\equiv d(\mathrm{mod}\ n)$时，$[c]=[d]$，这表明$[x]=[c]$与$[x]=[d]$是方程$[a][x]=[b]$的同一个解，相应地，我们把$x\equiv c(\mathrm{mod}\ n)$与$x\equiv d(\mathrm{mod}\ n)$视为同余方程$ax\equiv b(\mathrm{mod}\ n)$的同一个解.

根据上面的分析，当n不是很大时，我们很容易判断一次同余方程$ax\equiv b(\mathrm{mod}\ n)$是否有解，有多少解，并且在有解时写出全部解. 事实上，我们只需用0，1，2，…，$n-1$分别代替同余式$ax\equiv b(\mathrm{mod}\ n)$中的$x$，看这$n$个数哪些使得同余式$ax\equiv b(\mathrm{mod}\ n)$成立. 如果没有，则同余方程$ax\equiv b(\mathrm{mod}\ n)$无解；如果整数$i(0\leqslant i\leqslant n-1)$使得同余式成立，则$x\equiv i(\mathrm{mod}\ n)$是同余方程$ax\equiv b(\mathrm{mod}\ n)$的一个解.

在介绍一次同余方程的一般解法之前，教师可以通过具体的例子让学生认识到一个一次同余方程不一定有解. 例如，同余方程$2x\equiv 1(\mathrm{mod}\ 4)$无解.

教科书在求解一次同余方程$ax\equiv b(\mathrm{mod}\ n)$的过程中，用到了从特殊到一般的思想方法. 具体地，先考察$(a, n)=1$的特殊情形，再考察$(a, n)=d>1$的情形，然后将后者又转化为特殊情形进行求解，最终得到下面的结论：

一次同余方程$ax\equiv b(\mathrm{mod}\ n)$有解，则$(a, n)\mid b$；反过来，当$(a, n)\mid b$时，一次同余方程$ax\equiv b(\mathrm{mod}\ n)$恰有$(a, n)$个解.

学习本段内容时，教师应引导学生把重点放在一次同余方程$ax\equiv b(\mathrm{mod}\ n)$求解过程的理解和掌握上，而不是死记硬背可解条件和解的一般表达式.

教科书最后通过例5加深学生对一次同余方程解法的认识，巩固本小节所学基本知识.

(2) 大衍求一术

我国古代数学家在一次同余方程的解法方面曾经做出过巨大贡献，其中比较有名的是大衍求一术. 介绍大衍求一术的算法步骤和原理，有助于学生了解我国古代数学的巨大成就，增强他们的民族自豪感和自信心.

大衍求一术实际上是求一次同余方程$ax\equiv 1(\mathrm{mod}\ n)$的一种算法程序，其中$a$为小于$n$的正整数，且$(a, n)=1$. 我国宋代大数学家秦九韶继承前人造历算法经验，在其所著《数书九章》中记载了这个算法程序.

教科书首先简述原始记载的算法程序，然后用现代数学的语言重新表述这个算法程序. 前者有助于学生了解历史上大衍求一术的本来面目，后者有助于学生理解和掌握大衍求一术所蕴含的算法思想，同时也为后面给出大衍求一术的算法原理做准备.

在应用大衍求一术求解形如$ax\equiv 1(\mathrm{mod}\ n)$的一次同余方程时，我们可以先对$n$，$a$用辗转相除法，直至余数为1时停止：

$$\begin{aligned}
&n=aq_2+r_2,\ 0<r_2<a;\\
&a=r_2q_3+r_3,\ 0<r_3<r_2;\\
&r_2=r_3q_4+r_4,\ 0<r_4<r_3;\\
&r_3=r_4q_5+r_5,\ 0<r_5<r_4;\\
&\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n,\ r_n=1.
\end{aligned}$$

令$k_0=0$，$k_1=1$，则由递推关系式

$$k_i=k_{i-2}-q_ik_{i-1}\ (i=2, 3, \cdots, n)$$

依次计算出k_2，k_3，…，k_n. 为了证明k_n满足同余式$ak_n\equiv 1(\mathrm{mod}\ n)$，教科书第27页安排了一个“探

究”栏目，目的是让学生明确每个 r_i 可以表示成 $ax+ny$ 的形式，规定 $r_1=a$. 例如，

$r_1=a\times1+n\times0=a\times k_1+n\times0$；

$r_2=a\times(-q_2)+n\times1=a\times(k_0-q_2k_1)+n\times1=a\times k_2+n\times1$；

$r_3=a-r_2q_3=a\times k_1-(a\times k_2+n\times1)q_3=a\times(k_1-q_3k_2)+n\times(-q_3)=a\times k_3+n\times(-q_3)$；

$r_4=r_2-r_3q_4=(a\times k_2+n\times1)-[a\times k_3+n\times(-q_3)]q_4=a\times(k_2-q_4k_3)+n\times(1+q_3q_4)$

$=a\times k_4+n\times(1+q_3q_4)$；

$r_5=r_3-r_4q_5=[a\times k_3+n\times(-q_3)]-[a\times k_4+n\times(1+q_3q_4)]q_5=a\times(k_3-q_5k_4)+n$

$\times[-q_3-(1+q_3q_4)q_5]$

$=a\times k_5+n\times[-q_3-(1+q_3q_4)q_5]$.

从上面的表达式可以看出，

$r_1\equiv ak_1(\bmod n)$，$r_2\equiv ak_2(\bmod n)$，$r_3\equiv ak_3(\bmod n)$，$r_4\equiv ak_4(\bmod n)$，

$r_5\equiv ak_5(\bmod n)$.

如此进行下去，我们最后得到：对任意 i（$i=1$，2，…，n），$r_i\equiv ak_i(\bmod n)$. 而 $r_n=1$，所以 $ak_n\equiv1(\bmod n)$，这就是大衍求一术的算法原理.

教科书最后介绍用大衍求一术解同余方程的例子，加深学生对这种算法的认识.

5. 拉格朗日插值法和孙子定理

本节以一道历史名题“物不知其数”问题为载体，介绍求解一次同余方程组的著名定理——孙子定理.

本节包括两部分内容，第一部分介绍拉格朗日插值公式的建立过程，第二部分推导孙子定理. 这两部分内容之间存在密切的联系，孙子定理先特解而后求通解的思路和建立拉格朗日插值公式是一样的，因此在本节列入建立拉格朗日插值公式的内容有助于学生理解孙子定理，同时加强有关内容的联系.

约 2000 多年以前，我国古代数学著作《孙子算经》中提出了著名的“物不知其数”问题：“今有物不知其数，三三数之余二，五五数之余三，七七数之余二，问物几何?”答曰：“二十三”. 教科书将这个问题归结为求解如下三个一次同余方程组成的方程组：

$$\begin{cases}x\equiv2(\bmod 3),\\ x\equiv3(\bmod 5),\\ x\equiv2(\bmod 7),\end{cases}\qquad(*)$$

我们称之为同余方程组，并给出相应的解的概念. 需要注意的是，教科书上只讨论一种非常特殊的同余方程组. 对其它形式的特殊方程组，解的表述形式会有所变化. 例如：

$$\begin{cases}x\equiv e(\bmod a),\\ x\equiv f(\bmod b),\\ x\equiv g(\bmod c),\end{cases}\qquad(**)$$

其中 a，b，c 不必两两互素. 设 N 为 a，b，c 的最小公倍数，即 $N=[a,b,c]$. 如果 $x=k$ 使得（**）中每个同余式都成立，则称 $x\equiv k(\bmod N)$为同余方程组（**）的一个解.

教科书上关于拉格朗日插值法和孙子定理的介绍是通过具体的例子进行的，并没有介绍拉格朗日插值公式和孙子定理的一般形式的结论，目的是让学生理解这种先特解而后求通解的思想方法.

教科书第 29 页的“思考”栏目要求一个多项式 $f(x)$，使其满足 $f(1)=1$，$f(-1)=3$，$f(2)=3$，即求一个多项式函数 $f(x)$，其图象通过平面上点 $(1,1)$，$(-1,3)$ 和 $(2,3)$. 我们把这种问题称为多项式插值问题，并把 $f(1)=1$，$f(-1)=3$，$f(2)=3$ 称为插值条件.

由于这三个点的横坐标不同，且不在一条直线上，所以一定存在一条抛物线通过这三个点. 于是，我们待定 $f(x)=ax^2+bx+c$，然后将点代入，通过解关于 a，b，c 的三元一次方程组，最终得到 $f(x)$ 的表达式，这种方法具有一般性. 例如，多项式插值问题：

求一个多项式 $f(x)$，使其满足 $f(1)=1$，$f(-1)=3$，$f(2)=3$，$f(-2)=5$.

由于(1，1)，(−1，3)，(2，3)，(−2，3)四点的横坐标彼此不同，我们总可以待定多项式函数 $f(x)=ax^3+bx^2+cx+d$，将这四点代入多项式函数表达式后，通过求解关于 a，b，c，d 的四元一次方程组，最终得到 $f(x)$ 的表达式.

对更一般的多项式插值问题，我们也可以用类似的方法求解，但是这种方法很难得到 $f(x)$ 的一个明显的表达式. 教科书在介绍拉格朗日插值法之前介绍这种待定多项式的方法，其目的是通过前后两种方法的对照，体验拉格朗日插值法的优越性.

教科书在求出 $f(x)=x^2-x+1$ 后，写出了满足“思考”栏目中插值条件的所有多项式：

$$f(x)=x^2-x+1+(x-1)(x+1)(x-2)h(x), \tag{1}$$

其中 $h(x)$ 为任意多项式. 这是因为：一方面，容易检验由 (1) 式给出的多项式 $f(x)$ 满足插值条件；另一方面，如果 $f(x)$ 是满足插值条件的任一多项式，令多项式 $g(x)=f(x)-(x^2-x+1)$，则 $g(1)=0$，于是 $g(x)$ 含有一次因式 $x-1$，再由 $g(-1)=0$，$g(2)=0$ 知，$g(x)$ 又含有一次因式 $x+1$，$x-2$. 因此，$g(x)$ 具有下面的形式：

$$g(x)=f(x)-(x^2-x+1)=(x-1)(x+1)(x-2)h(x),$$

其中 $h(x)$ 为某个多项式. 这表明，满足插插条件的每个多项式均可以表示成 (1) 的形式.

教科书仍以“思考”栏目中的多项式插值问题为例，介绍拉格朗日插值法. 拉格朗日插值法的思想是先求一些特殊而又简单的多项式插值问题的解，将这些解按一定的方式线性组合，便得到所求多项式插值问题的一个解. 用类似的想法，我们很容易得到一般情形的拉格朗日插值公式，详细讨论见本讲“拓展资源”部分.

教科书第 29 页求多项式 $p(x)$ 时，我们可以选取 $p(x)=c(x+1)(x-2)$ (c 为常数). 理由如下：因为 $p(-1)=0$，$p(2)=0$，所以 $p(x)$ 有一次因式 $x+1$，$x-2$，于是 $p(x)$ 可以表示成下面的形式：

$$p(x)=(x+1)(x-2)h(x), \tag{2}$$

其中 $h(x)$ 为多项式. 再由插值条件 $p(1)=1$ 知，

$$1=p(1)=(1+1)(1-2)h(1),$$

所以 $h(1)=-\frac{1}{2}$. 选取 $h(x)=-\frac{1}{2}$，将其代入 (2) 式得

$$p(x)=-\frac{1}{2}(x+1)(x-2). \tag{3}$$

事实上，由上面的分析过程知，(3) 中的 $p(x)$ 是满足插值条件 $p(1)=1$，$p(-1)=0$，$p(2)=0$，次数最低的多项式. 类似地，我们可以计算出多项式 $q(x)$ 和 $r(x)$. 在计算出多项式 $p(x)$，$q(x)$ 和 $r(x)$ 后，作多项式 $f(x)=1\times p(x)+3\times p(x)+3\times r(x)$，容易检验，$f(x)$ 与前面用待定多项式的方法计算出的多项式是一致的，并且是所有满足插值条件 $f(1)=1$，$f(-1)=3$，$f(2)=3$ 的多项式中次数最小的一个.

用建立拉格朗日插值公式的思路可以推导求解一次同余方程组的孙子定理. 教科书以本节开始提出的“物不知其数”问题为例进行说明. 为了求解同余方程组 (*)，我们先求整数 p，q 和 r，它们分别满足：

$$p\equiv 1(\mathrm{mod}\ 3),\ p\equiv 0(\mathrm{mod}\ 5),\ p\equiv 0(\mathrm{mod}\ 7);$$
$$q\equiv 0(\mathrm{mod}\ 3),\ q\equiv 1(\mathrm{mod}\ 5),\ q\equiv 0(\mathrm{mod}\ 7);$$
$$r\equiv 0(\mathrm{mod}\ 3),\ r\equiv 0(\mathrm{mod}\ 5),\ r\equiv 1(\mathrm{mod}\ 7).$$

首先计算整数 p. 由于 $p\equiv 0(\bmod 5)$，$p\equiv 0(\bmod 7)$，所以 $5\mid p$，$7\mid p$. 而 $(5,7)=1$，故 $p=5\times 7\times c$，其中 c 为某个整数. 再由 $p\equiv 1(\bmod 3)$ 知，整数 c 满足 $35c\equiv 1(\bmod 3)$. 由此解得 $c\equiv -1(\bmod 3)$. 选取 $c=2$，则 $p=70$.

类似地，可以计算得 $q=21$，$r=15$. 作整数 $k=2\times 70+3\times 21+2\times 15=233$，则 $x=233$ 使得（*）式中每个同余式都成立，因此 $x\equiv 233\equiv 23(\bmod 105)$ 是同余方程组（*）的解.

一般来说，p，q，r 的选取是不唯一的，但最后得到的同余方程组（*）的解不会发生变化. 例如在计算 p 时，如果选取满足同余式 $c\equiv -1(\bmod 3)$ 的不同的整数 c 就会得到不同的 p. 注意到，满足同余式 $c\equiv -1(\bmod 3)$ 的整数 c 可以表示成 $c=3t-1$ 的形式，其中 t 为整数，那么相应的整数 p 可以表示为 $p=35(3t-1)=105t-35$. 于是，整数

$$k=2\times(105t-35)+3\times 21+2\times 15=210t+23.$$

此时 $x=210t+23$ 使得（*）中每个同余式成立. 因此，$x\equiv 210t+23\equiv 23(\bmod 105)$ 是同余方程组（*）的解，与前面是一致的.

作为前面讨论的总结，教科书第 30 页给出了孙子定理. 教学时，教师应对定理中解的唯一性作补充说明. 具体如下：

如果 $x\equiv m(\bmod abc)$ 与 $x\equiv n(\bmod abc)$ 是同余方程组

$$\begin{cases} x\equiv e(\bmod a), \\ x\equiv f(\bmod b), \\ x\equiv g(\bmod c) \end{cases} \tag{4}$$

的解，则 $x=m$ 与 $x=n$ 使得（4）中每个同余式都成立. 于是

$$m\equiv e(\bmod a),\ n\equiv e(\bmod a).$$

由同余的传递性知 $m\equiv n(\bmod a)$，因此 $a\mid m-n$. 类似可证：$b\mid m-n$，$c\mid m-n$. 而 a，b，c 两两互素，故 $abc\mid m-n$，从而 $m\equiv n(\bmod abc)$. 这表明 $x\equiv m(\bmod abc)$ 与 $x\equiv n(\bmod abc)$ 是同余方程组（4）的同一个解.

关于孙子定理的一般情形将在本讲“拓展资源”部分给出.

6. 弃九验算法

本节从一个思考题开始引入本书所要讨论的内容，容易吸引学生的注意和探究的兴趣. 教科书仅以正整数的乘法为例说明弃九验算法及其原理，对于正整数的加、减和除法的讨论可类似进行. 需要指出的是，减法运算通常转化为加法运算进行讨论，除法运算通常转化为乘法运算进行讨论. 例如，要验算算式

$$3\ 596-2\ 346=1\ 340,\ 226\ 380\div 165=1\ 432$$

是否正确，只需判断算式

$$2\ 346+1\ 340=3\ 596,\ 165\times 1\ 432=226\ 380$$

是否正确即可.

在弃九验算法的原理中，要用到“一个正整数与它的各位数字之和模 9 同余”的结论，这也是教科书第 31 页“探究”栏目中要探究的问题.

我们知道，每个正整数 N 总可以表示成下面的形式：

$$N=\overline{a_n\cdots a_2a_1a_0}=a_n\times 10^n+\cdots+a_2\times 10^2+a_1\times 10+a_0. \tag{5}$$

于是，

$$\begin{aligned} N&=\overline{a_n\cdots a_2a_1a_0}=a_n\times(99\cdots 9+1)+\cdots+a_2\times(99+1)+a_1\times(9+1)+a_0\\ &=9(11\cdots 1a_n+\cdots+11a_2+a_1)+(a_0+a_1+\cdots+a_n). \end{aligned}$$

从上式可以看出，$9 \mid N-(a_n+\cdots+a_2+a_1)$，所以

$$N \equiv a_n+\cdots+a_2+a_1 \pmod 9$$

教科书在推导出弃九验算法的原理之后，再回来处理本节开始“思考”栏目中的问题，加深学生对这种验算正整数计算结果是否正确的方法的认识.

教师教学时，教师需要特别向学生强调的是，弃九验算法只能“检错”，不能“判正”. 也就是说，使用弃九验算法时，得出的结果如果是

$$\overline{ab} \equiv \overline{p} \pmod 9 \quad (\text{或 } \bar{a}+\bar{b} \equiv \overline{p} \pmod 9),$$

也不能判定算式 $ab=p$(或 $a+b=p$)是正确的，教科书上给了一个关于乘法运算的例子. 必须让学生认识到弃九验算法的不足，以免实际应用时犯错.

四、教学设计案例

同余（1课时）

1. 教学任务分析

(1) 理解同余的概念，建立同余和整除之间的关系；

(2) 探究同余的性质，并给出证明；

(3) 能够灵活运用同余的性质简化数论中的问题，如星期几问题、整除问题.

2. 教学重点与难点

重点：

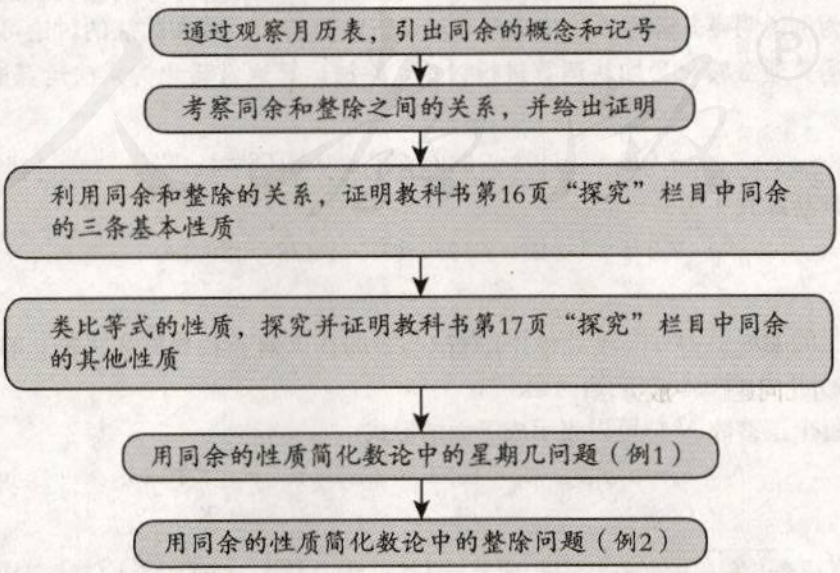
(1) 准确地理解同余的概念，正确地使用同余符号；

(2) 类比等式的性质，探究并证明同余的一些重要性质；

(3) 运用同余的性质解决数论中的一些问题.

难点：灵活运用同余的性质解决数论中的问题.

3. 教学基本流程



4. 教学情境设计

问题 1：观察教科书第 15 页的月历表，在月历表中位于同一列的整数被 7 除后的余数有什么规律？观察其他的月历表，你是否发现同样的规律？

设计意图：通过观察月历表中位于同一列的整数被 7 除后的余数的规律，引出同余的概念和符号.

师生活动：教师提出问题，学生观察月历表中位于同一列的整数被 7 除后的余数的规律，并汇报所发现的规律. 教师总结，并引出同余的概念和符号.

问题 2：由同余的概念知，同余与整除存在密切的关系. 如果 $a\equiv b(\mathrm{mod}\ n)$，那么整数 a，b 和 n 之间存在什么样的整除关系？

设计意图：让学生明确同余和整除之间的内在联系，这对应用同余解决整除问题或用整除解决同余问题是至关重要的，也是后面证明同余性质的理论依据.

师生活动：教师引导学生根据同余的概念推导结论：$a\equiv b(\mathrm{mod}\ n)\Leftrightarrow n\mid a-b$.

问题 3：你能根据同余和整除的关系证明教科书第 16 页“探究”栏目中同余的三条基本性质吗？从同余的这三条性质可以看出，模 n 同余给出了整数之间的一种关系. 你能利用这种关系对整数集进行分类吗？试举例说明.

设计意图：让学生理解同余的三条最基本的性质，知道模 n 同余实际上给出了整数之间的一种关系，并会利用这种关系对整数集合进行分类，为第二节的学习作铺垫.

师生活动：学生尝试用同余和整除的关系证明同余的三条基本性质. 教师引导学生认识同余这种关系，并通过具体例子让学生体验如何用同余关系对整数集进行分类.

问题 4：从教科书第 16 页的“探究”不难发现，同余式 $a\equiv b(\mathrm{mod}\ n)$ 与等式 $a=b$ 有许多类似的性质. 你能类比等式的性质，探究教科书第 17 页“探究”栏目中同余的两条性质吗？

设计意图：让学生通过类比，探究同余的其他性质，这些性质是我们运用同余知识解决数论问题的理论基础.

师生活动：学生独立思考，给出证明过程. 教师纠正学生证明中可能出现的逻辑问题. 让学生感受数学的严谨性.

问题 5：教科书第 17 页“探究”栏目中同余的性质 2 对应于等式中的什么性质？它们的联系与区别是什么？

设计意图：让学生明确性质 2 是同余意义下的消去律，以及它与等式意义下的消去律的联系和区别.

师生活动：学生思考并回答. 教师强调同余意义下消去律成立的前提条件是 $(a, n)=1$，等式意义下消去律成立的前提条件是 $a\neq 0$.

问题 6：运用同余的性质可以简化数论中的许多问题，如星期几问题、整除问题. 你能用同余的性质解决例 1 中的星期几问题吗？

设计意图：让学生了解如何用同余的性质解决数论中的星期几问题，加深学生对所学知识的理解和认识.

师生活动：教师提出问题，并引导学生分析、思考例 1，直至问题解决. 师生共同总结出解决星期几问题的一般方法.

问题 7：你能用同余的性质解决例 2 中的整除问题吗？

设计意图：让学生了解如何用同余的性质解决数论中的一些整除问题，进一步巩固学生所学基本知识.

师生活动：教师引导学生分析、思考例 2，并逐步解决问题. 师生共同总结出用同余解决整除问题的一般方法.

最后，教师引导对本小节的内容进行小结，同时提出需要进一步思考的问题.

五、习题解答

习题（第 18 页）

1. 证明：(1) 因为 $N=\overline{a_n\cdots a_2a_1a_0}=a_n\times(9+1)^n+\cdots+a_2\times(9+1)^2+a_1\times(9+1)+a_0$
$\equiv a_0+a_1+\cdots+a_n\pmod 3$，
所以 $N\equiv 0\pmod 3$ 当且仅当 $a_0+a_1+\cdots+a_n\equiv 0\pmod 3$，也就是说，$3\mid N$ 当且仅当 $3\mid a_0+a_1+\cdots+a_n$.
(2) 因为 $N=\overline{a_n\cdots a_2a_1a_0}=a_n\times(9+1)^n+\cdots+a_2\times(9+1)^2+a_1\times(9+1)+a_0$
$\equiv a_0+a_1+\cdots+a_n\pmod 9$，
所以 $N\equiv 0\pmod 9$ 当且仅当 $a_0+a_1+\cdots+a_n\equiv 0\pmod 9$，也就是说，$9\mid N$ 当且仅当 $9\mid a_0+a_1+\cdots+a_n$.
(3) 因为 $N=\overline{a_n\cdots a_2a_1a_0}=\overline{a_n\cdots a_3}\times 1\,001+(\overline{a_2a_1a_0}-\overline{a_n\cdots a_3})$
$\equiv\overline{a_2a_1a_0}-\overline{a_n\cdots a_3}\pmod 7$，
所以 $N\equiv 0\pmod 7$ 当且仅当 $\overline{a_2a_1a_0}-\overline{a_n\cdots a_3}\equiv 0\pmod 7$，也就是说，$7\mid N$ 当且仅当 $7\mid\overline{a_2a_1a_0}-\overline{a_n\cdots a_3}$.
(4) 因为 $N=a_n\cdots a_2a_1a_0=a_n\times(11-1)^n+\cdots+a_2\times(11-1)^2+a_1\times(11-1)+a_0$
$\equiv a_0-a_1+a_2-a_3+\cdots=(a_0+a_2+\cdots)-(a_1+a_3+\cdots)\pmod{11}$，
所以 $N\equiv 0\pmod{11}$ 当且仅当 $(a_0+a_2+\cdots)-(a_1+a_3+\cdots)\equiv 0\pmod{11}$，
也就是说，$11\mid N$ 当且仅当 $11\mid(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$.

2. 解：由于 $2+2\,008^{2\,008}=2+(287\times 7-1)^{2\,008}\equiv 2+(-1)^{2\,008}=2+1=3\pmod 7$，故过 $2\,008^{2\,008}$ 天后的今天是星期三.

3. 解：对任意自然数 n，对 n 和 3 用带余除法：$n=3q+r$，$r=0$，1 或 2，则
$$2^n+1=2^{3q+r}+1=(2^3)^q\times 2^r+1=(7+1)^q\times 2^r+1$$
$$\equiv 1^q\times 2^r+1=2^r+1=2,\ 3\text{ 或 }5\pmod 7.$$
所以，对任意自然数 n，$2^n+1\not\equiv 0\pmod 7$，即 $7\nmid 2^n+1$.

4. 解：只需求 3^{50} 被 100 除后的余数即可. 由于
$$3^{50}=9^{25}=9\times(10-1)^{24}\equiv 9\times[(10-1)^2]^{12}\equiv 9\times(1-20)^{12}\equiv 9\times(1-40)^6\equiv 9\times(1-80)^3$$
$$\equiv 9\times(1-3\times 80)\equiv 9\times(1-40)=9-360\equiv 9-60=-51\equiv 49\pmod{100},$$
故 3^{50} 的十进制表示中的末两位数字为 49.

5. 证明：注意到对任意整数 a，$a=2k$，或 $2k+1$，则 $a^2\equiv 0$，或 $1\pmod 4$. 假设 $4n+3=a^2+b^2$，其中 a，b 为整数，则
$$4n+3=a^2+b^2\equiv 0,\ 1,\text{ 或 }2\pmod 4.$$
显然，$4n+3\equiv 3\pmod 4$，矛盾. 故 $4n+3$ 不是两个整数的平方和.

习题（第 22 页）

1. 证明：只需证明在模 n 的剩余类环中，对任意 $c\in[a]$，$d\in[b]$，总有
$$[c+d]=[a+b],\ [cd]=[ab].\qquad(*)$$
这是因为，当 $c\in[a]$，$d\in[b]$ 时，$c\equiv a\pmod n$，$d\equiv b\pmod n$，所以
$$c+d\equiv a+b\pmod n,\ cd\equiv ab\pmod n,$$
从而（*）式成立.

2. 证明：假设在模 n 的剩余类环中，$[b]$ 与 $[c]$ 均为 $[a]$ 的逆元，即

$$[a][b]=[b][a]=[1],\ [a][c]=[c][a]=[1],$$

则

$$[b]=[b][1]=[b]([a][c])=([b][a])[c]=[1][c]=[c].$$

这表明，在模 n 的剩余类环中，若$[a]$存在逆元，则它的逆元仅有一个.

3. 充分条件：$n=1$ 或 n 为素数（注：此条件也是必要条件）.

证明：当 $n=1$ 时，结论显然成立.

当 n 为素数时，对模 n 的剩余类中任意非零元$[a]$，由于$[a]\neq[0]$，故 $a\not\equiv 0 \pmod p$，即 $p\nmid a$，再由素数的性质知$(a, p)=1$. 于是存在一对整数 s，t 使得 $as+pt=1$，此时 $p\mid 1-as$，从而有 $as=sa\equiv 1 \pmod p$，即$[a][s]=[s][a]=[1]$. 这表明，$[a]$存在逆元，并且$[s]$为$[a]$的逆元.

习题（第 25 页）

1. 解：由于 19 为素数，故由费马小定理知 $47^{18}\equiv 1 \pmod{19}$. 于是，

$$47^{7\,385}=47^{18\times 410+5}=(47^{18})^{410}\times 47^5\equiv 1^{410}\times 47^5=(19\times 2+9)^5\equiv 9^5$$
$$=(19\times 4+5)^2\times 9\equiv 25\times 9\equiv 6\times 9=54\equiv 16 \pmod{19}.$$

所以，$47^{7\,385}$除以 19 的余数为 16.

2. 解：由于$(18, 25)=1$，且 $\varphi(25)=20$，由欧拉定理知 $18^{20}\equiv 1 \pmod{25}$. 显然，$x\leqslant 20$. 对 20 和 x 用带余除法：$20=xq+r$，其中 $0\leqslant r<x$，则有

$$18^{20}=18^{xq+r}=(18^x)^q\times 18^r\equiv 18^r\equiv 1 \pmod{25}.$$

由 x 是使 $18^x\equiv 1 \pmod{25}$ 成立的最小正整数知 $r=0$，从而 $x\mid 20$. 20 的所有正因数依次为 1，2，4，5，10，20，我们检验发现

$$18^1\equiv 18 \pmod{25},\ 18^2\equiv 24\equiv -1 \pmod{25},\ 18^4\equiv(-1)^2=1 \pmod{25}.$$

因此，最小正整数 x 为 4.

3. 证明：对任意正整数 n，n 要么是 13 的倍数，要么不是 13 的倍数. 当 n 是 13 的倍数时，$13\mid n$，则 $13\mid n^{12}$，即 n^{12}是 13 的倍数. 当 n 不是 13 的倍数时，$13\nmid n$，注意到 13 为素数，所以$(13, n)=1$，由费马小定理知 $n^{12}\equiv 1 \pmod{13}$，即 $13\mid n^{12}-1$，$n^{12}-1=13t$，$n^{12}=13t+1$. 综上所述，正整数 n 的 12 次方要么是 13 的倍数，要么是 13 的倍数加 1.

习题（第 28 页）

解：(1) $(9, 7)=1$，且 $1\mid 5$，故同余方程仅有一个解. 而 $4\times 9=36\equiv 1 \pmod 7$，故 $x\equiv 4\times 5=20\equiv 6 \pmod 7$. 所以，原同余方程的解为 $x\equiv 6 \pmod 7$.

(2) $(32, 8)=8$，但 $8\nmid 12$，故同余方程没有解.

(3) $(28, 116)=4$，且 $4\mid 124$，故同余方程有四个解. 原同余方程可化简为

$$7x\equiv 31\equiv 2 \pmod{29}.$$

由于 $7\times(-4)=-28\equiv 1 \pmod{29}$，故 $x\equiv 2\times(-4)=-8 \pmod{29}$. 所以，原同余方程的四个解为 $x\equiv -8+29\times 0=-8 \pmod{116}$，$x\equiv -8+29\times 1=21 \pmod{116}$，$x\equiv -8+29\times 2=50 \pmod{116}$，$x\equiv -8+29\times 3=69 \pmod{116}$.

(4) $(5, 81)=1$，且 $1\mid 44$，故同余方程仅有一个解. 而 $5\times(-16)=-80\equiv 1 \pmod{81}$，故 $x\equiv 44\times(-16)=-704\equiv 25 \pmod{81}$. 所以，原同余方程的解为 $x\equiv 25 \pmod{81}$.

习题（第 30 页）

1. 解：由拉格朗日插值公式知，

$$f(x)=2\times\frac{x(x-1)}{(-1-0)(-1-1)}+3\times\frac{(x+1)(x-1)}{[0-(-1)](0-1)}+6\times\frac{(x+1)x}{[1-(-1)](1-0)}$$
$$=x(x-1)-3(x+1)(x-1)+3(x+1)x$$
$$=x^2+2x+3.$$

2. 解：(1) 由于4，5，9两两互素，故可用孙子定理. 解同余方程 $5\times 9c_1=45$ $c_1\equiv 1(\mathrm{mod}\ 4)$ 得 $c_1\equiv 1(\mathrm{mod}\ 4)$，再解同余方程 $4\times 9c_2=36$ $c_2\equiv 1(\mathrm{mod}\ 5)$ 得 $c_2\equiv 1(\mathrm{mod}\ 5)$，最后解同余方程 $4\times 5c_3=20c_3\equiv 1(\mathrm{mod}\ 9)$ 得 $c_3\equiv 5(\mathrm{mod}\ 9)$. 于是，选取 $c_1=1$，$c_2=1$，$c_3=5$ 得

$$x\equiv 2\times 5\times 9\times 1+3\times 4\times 9\times 1+4\times 4\times 5\times 5=598\equiv 58(\mathrm{mod}\ 180)$$

是同余方程组的解.

(2) 由于7，9，11两两互素，故同样可用孙子定理. 解同余方程 $9\times 11c_1=99$ $c_1\equiv 1(\mathrm{mod}\ 7)$ 得 $c_1\equiv 1(\mathrm{mod}\ 7)$，再解同余方程 $7\times 11c_2=77c_2\equiv 1(\mathrm{mod}\ 9)$ 得 $c_2\equiv 2(\mathrm{mod}\ 9)$，最后解同余方程 $7\times 9c_3=63c_3\equiv 1(\mathrm{mod}\ 11)$ 得 $c_3\equiv 7(\mathrm{mod}\ 11)$. 于是，选取 $c_1=1$，$c_2=2$，$c_3=7$ 得

$$x\equiv 2\times 9\times 11\times 1+3\times 7\times 11\times 2+7\times 7\times 9\times 7=3\ 747\equiv 282(\mathrm{mod}\ 693)$$

是同余方程组的解.

3. 解：设兵数为 x. 由题意知，韩信点兵问题相当于求解如下同余方程组：

$$\begin{cases}x\equiv 1(\mathrm{mod}\ 5),\\ x\equiv 5(\mathrm{mod}\ 6),\\ x\equiv 4(\mathrm{mod}\ 7),\\ x\equiv 10(\mathrm{mod}\ 11).\end{cases}$$

下面求解上面的同余方程组. 由于5，6，7，11两两互素，可用一般情形的孙子定理.

解同余方程 $6\times 7\times 11c_1\equiv 2c_1\equiv 1(\mathrm{mod}\ 5)$ 得 $c_1\equiv 3(\mathrm{mod}\ 5)$；解同余方程 $5\times 7\times 11c_2\equiv c_2\equiv 1(\mathrm{mod}\ 6)$ 得 $c_2\equiv 1(\mathrm{mod}\ 6)$；解同余方程 $5\times 6\times 11c_3\equiv c_3\equiv 1(\mathrm{mod}\ 7)$ 得 $c_3\equiv 1(\mathrm{mod}\ 7)$，解同余方程 $5\times 6\times 7c_4\equiv c_4\equiv 1(\mathrm{mod}\ 11)$ 得 $c_4\equiv 1(\mathrm{mod}\ 11)$. 于是，选取 $c_1=3$，$c_2=1$，$c_3=1$，$c_4=1$ 得

$$x\equiv 1\times 6\times 7\times 11\times 3+5\times 5\times 7\times 11\times 1+4\times 5\times 6\times 11+10\times 5\times 6\times 7\times 1$$
$$\equiv 2\ 111(\mathrm{mod}\ 2\ 310),$$

即 $2\ 310\mid x-2\ 111$，$x=2\ 111+2\ 310k$，这里 k 取非负整数.

所以，兵数为 $2\ 111+2\ 310k$ 人，其中 k 为非负整数.

习题（第32页）

解：(1) $1\ 524\equiv 1+5+2+4=12\equiv 3(\mathrm{mod}\ 9)$，$3\ 456\equiv 3+4+5+6=18\equiv 0(\mathrm{mod}\ 9)$，

$4\ 880\equiv 4+8+8+0=20\equiv 2(\mathrm{mod}\ 9)$.

由于 $3+0=3\not\equiv 2(\mathrm{mod}\ 9)$，故算式不正确.

(2) 只需验算算式 $2\ 346+1\ 340=2\ 596$ 是否正确.

$2\ 346\equiv 2+3+4+6=15\equiv 6(\mathrm{mod}\ 9)$，$1\ 340\equiv 1+3+4+0=8(\mathrm{mod}\ 9)$，

$2\ 596\equiv 2+5+9+6=22\equiv 4(\mathrm{mod}\ 9)$.

由于 $6+8=14\not\equiv 4(\mathrm{mod}\ 9)$，故算式不正确.

(3) $4\ 328\equiv 4+3+2+8=17\equiv 8(\mathrm{mod}\ 9)$，$3\ 249\equiv 3+2+4+9=18\equiv 0(\mathrm{mod}\ 9)$，

$14\ 246\ 432\equiv 1+4+2+4+6+4+3+2=26\equiv 8(\mathrm{mod}\ 9)$.

由于 $8\times 0=0\not\equiv 8(\mathrm{mod}\ 9)$，故算式不正确.

(4) 只需验算算式 $165\times 1432=226380$ 是否正确.

$165\equiv 1+6+5=12\equiv 3(\mathrm{mod}\ 9)$，$1432\equiv 1+4+3+2=10\equiv 1(\mathrm{mod}\ 9)$，

$226\ 380\equiv 2+2+6+3+8+0=21\equiv 3(\mathrm{mod}\ 9)$.

而 $3\times1\equiv3(\mathrm{mod}\ 9)$，故用弃九验算法无法判断算式是否正确. 事实上，直接计算发现，该算式是错误的.

六、拓展资源

1. 拉格朗日插值公式的一般情形

考察多项式插值问题：求多项式 $f(x)$，使其满足 $f(x_1)=y_1$，$f(x_2)=y_2$，…，$f(x_n)=y_n$，这里 x_1，y_1，x_2，y_2，…，x_n，y_n 为给定的数，且 x_1，x_2，…，x_n 互不相同.

类似于教科书中 $n=3$ 的情形，我们先求一些特殊的多项式：

(1) 求多项式 $L_1(x)$，使 $L_1(x_1)=1$，$L_1(x_2)=0$，…，$L_1(x_n)=0$；

(2) 求多项式 $L_2(x)$，使 $L_2(x_1)=0$，$L_2(x_2)=1$，…，$L_2(x_n)=0$；

……

(n) 求多项式 $L_n(x)$，使 $L_n(x_1)=0$，$L_n(x_2)=0$，…，$L_n(x_n)=1$.

注意到 $L_1(x_2)=0$，…，$L_1(x_n)=0$，所以多项式 $L_1(x)$ 含有一次因式 $x-x_2$，$x-x_3$，…，$x-x_n$，由于 x_2，…，x_n 互不相同，所以 $L_1(x)$ 具有下面的形式

$$L_1(x)=h(x)(x-x_2)(x-x_3)(x-x_n),$$

这里 $h(x)$ 为多项式. 再将插值条件 $L_1(x_1)=1$ 代入上式得

$$1=h(x_1)(x_1-x_2)(x_1-x_3)(x_1-x_n),$$

于是

$$h(x_1)=\frac{1}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)}.$$

如果选取

$$h(x)=\frac{1}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)},$$

则有

$$L_1(x)=\frac{(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)}.$$

用类似的方法，可依次计算得

$$L_2(x)=\frac{(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_n)},$$

……

$$L_n(x)=\frac{(x-x_1)(x-x_2)\cdots(x-x_{n-1})}{(x_n-x_1)(x_n-x_2)\cdots(x_n-x_{n-1})}.$$

最后，我们作多项式

$$\begin{aligned}f(x)&=y_1L_1(x)+y_2L_2(x)+\cdots+y_nL_n(x)\\&=\frac{y_1(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)}+\frac{y_2(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_n)}\\&\quad+\cdots+\frac{y_n(x-x_1)(x-x_2)\cdots(x-x_{n-1})}{(x_n-x_1)(x_n-x_2)\cdots(x_n-x_{n-1})},\end{aligned}\tag{*}$$

容易检验 $f(x)$ 是原多项式插值问题的一个解.

公式（*）就是拉格朗日插值公式的一般情形.

2. 孙子定理的一般情形

与教科书 $n=3$ 的情形一样，前面建立拉格朗日插值公式的思路可用来求解同余方程组. 考察如下形式的同余方程组：

$$\begin{cases} x\equiv d_1 \pmod{m_1}, \\ x\equiv d_2 \pmod{m_2}, \\ \cdots\cdots\cdots\cdots \\ x\equiv d_n \pmod{m_n}, \end{cases} \qquad (**)$$

其中 m_1，m_2，…，m_n 两两互素.

为求解同余方程组（**），我们先求一些特殊的整数：

(1) 求整数 p_1，使 $p_1\equiv 1 \pmod{m_1}$，$p_1\equiv 0 \pmod{m_2}$，…，$p_1\equiv 0 \pmod{m_n}$；

(2) 求整数 p_2，使 $p_2\equiv 0 \pmod{m_1}$，$p_1\equiv 1 \pmod{m_2}$，…，$p_1\equiv 0 \pmod{m_n}$；

……

(n) 求整数 p_n，使 $p_n\equiv 0 \pmod{m_1}$，$p_n\equiv 0 \pmod{m_2}$，…，$p_n\equiv 1 \pmod{m_n}$.

由于 $p_1\equiv 0 \pmod{m_2}$，…，$p_1\equiv 0 \pmod{m_n}$，故 $m_2 \mid p_1$，…，$m_n \mid p_1$，而 m_2，…，m_n 两两互素，由教科书第 13 页习题 3 的结论知，$m_2m_3\cdots m_n \mid p_1$. 于是，整数 p_1 具有下面的形式：

$$p_1 = m_2m_3\cdots m_n c_1, \qquad (***)$$

其中 c_1 为整数. 再由 $p_1\equiv 1 \pmod{m_1}$ 知，c_1 满足同余式

$$m_2m_3\cdots m_nc_1\equiv 1 \pmod{m_1}.$$

我们可以通过求解一次同余方程 $m_2m_3\cdots m_nx\equiv 1 \pmod{m_1}$ 得到整数 c_1. 需要指出的是，整数 c_1 的选取是不惟一的.

类似地，我们可依次计算出整数

$$p_2 = m_1m_3\cdots m_nc_2, \ \cdots, \ p_n = m_1m_2\cdots m_{n-1}c_n,$$

其中整数 c_2，…，c_n 分别满足同余式

$$m_2m_3\cdots m_nc_2\equiv 1 \pmod{m_2}, \ \cdots, \ m_1m_2\cdots m_{n-1}c_n\equiv 1 \pmod{m_n}.$$

在求出整数 p_1，p_2，…，p_n 后，作整数

$$k = d_1p_1 + d_2p_2 + \cdots + d_np_n,$$

则容易检验 k 满足（**）中每个同余式. 通常，我们把 $x\equiv k \pmod{m_1m_2\cdots m_n}$ 叫做同余方程组（**）的一个解. 并且，在模 $m_1m_2\cdots m_n$ 的意义下，这个解是惟一的.

综上所述，我们可得到一般情形的孙子定理：

设 m_1，m_2，…，m_n 为两两互素的正整数，d_1，d_2，…，d_n 为任意整数，又设 $M = m_1m_2\cdots m_n$，$M_i = M/m_i (i=1, 2, \cdots, n)$，则同余方程组（**）有惟一解：

$$x\equiv d_1M_1c_1 + d_2M_2c_2 + \cdots + d_nM_nc_n \pmod{M},$$

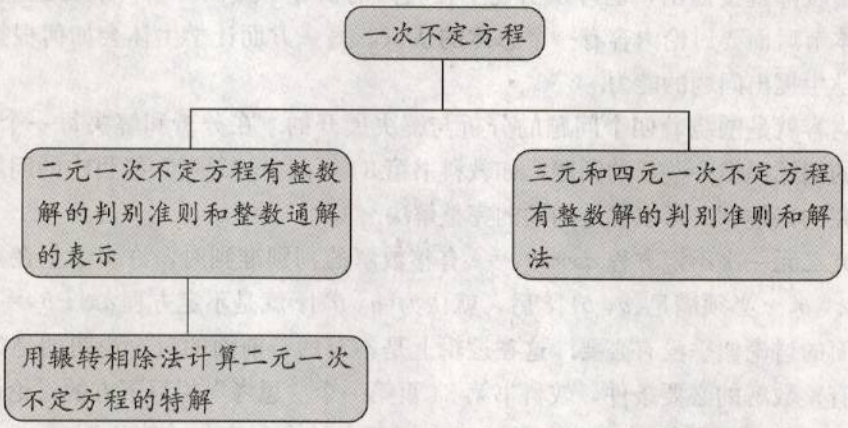
其中 c_1，c_2，…，c_n 分别是满足同余式

$$M_1c_1\equiv 1 \pmod{m_1}, \ M_2c_2\equiv 1 \pmod{m_2}, \ \cdots, \ M_nc_n\equiv 1 \pmod{m_n}$$

的整数.

第三讲　一次不定方程

一、本讲知识结构



二、教学重点与难点

重点：

1. 理解二元一次不定方程有整数解的判别准则和有整数解时整数通解的表示；
2. 会用辗转相除法计算二元一次不定方程的一个特解；
3. 理解三元和四元一次不定方程有整数解的判别准则；
4. 会解三元和四元一次不定方程；
5. 培养学生提出问题、分析问题和解决问题的能力.

难点：

将三元或四元一次不定方程转化为二元一次不定方程进行求解.

三、编写意图与教学建议

不定方程的内容非常丰富，本讲主要介绍如何解一次不定方程，并了解我国古代数学家在不定方程的研究方面取得的一些成就. 通过学习，培养学生提出问题、分析问题和解决问题的能力.

教科书首先在引言部分简要介绍了不定方程的一些历史背景知识，其中包括我国古代和古希腊数学家研究不定方程的事例. 然后，教科书通过三节介绍一次不定方程的一些基本知识，如二元一次不定方程有整数解的判别准则和整数通解的表示，用辗转相除法计算二元一次不定方程的一个特解，以及三元和四元一次不定方程有整数解的判别准则和解法等.

1. 二元一次不定方程

二元一次不定方程是最简单的不定方程. 教科书在介绍完二元一次不定方程的一般形式后，紧接着讨论这类不定方程是否有整数解的问题. 通过具体的例子，使学生认识到二元一次不定方程$ax+by=c$有

时有整数解，有时没有整数解，为后面问题的提出做准备.

在前面分析的基础上，教科书提出了研究二元一次不定方程时需要回答的四个问题：

(1) 二元一次不定方程 $ax+by=c$ 何时有整数解?

(2) 有整数解时是否有无穷多个整数解?

(3) 这些整数解是否有统一的表达式?

(4) 有整数解时如何求出所有的整数解?

这些问题可由教师直接提出，也可以由学生在教师的引导下提出. 教科书在这里提出这些问题，一方面让学生对本节后面要讨论内容有一个总体的认识，另一方面让学生体会如何根据一些现象提出问题，从而培养学生提出问题的能力.

本节后面的内容就是围绕着四个问题的分析与解决展开的. 在分析和解决每一个问题的过程中，又围绕所要解决的问题提出一些新的问题，如教科书第 34 页两个“思考”栏目中的问题. 这些问题既可以激发学生探究的兴趣，又可以促进问题的完整解决.

例如，在探究二元一次不定方程 $ax+by=c$ 有整数解的判别准则时，许多学生在得到不定方程有整数解时，整数 a，b，c 必须满足 $(a,b)|c$ 后，就认为 $(a,b)|c$ 就是不定方程 $ax+by=c$ 有整数解的判别准则，认为后面的讨论似乎没有必要. 这在逻辑上是不对的，前面的讨论说明的是 $(a,b)|c$ 是不定方程 $ax+by=c$ 有整数解的必要条件，教科书第 34 页第一个“思考”栏目下方的讨论说明 $(a,b)|c$ 也是不定方程 $ax+by=c$ 有整数解的充分条件. 只有把两者结合起来，才能说明 $(a,b)|c$ 是不定方程 $ax+by=c$ 有整数解的判别准则. 从内容结构上讲，第一个“思考”栏目中的问题在教科书中起着承上启下的作用.

对于有整数解的不定方程 $ax+by=c$，我们总是先将其化简为 x，y 的系数互素的不定方程的形式，因此总可假定 $(a,b)=1$. 在后面的讨论中，我们要用到这个假定，教学时教师必须向学生强调这一点，否则容易出错.

在已知 $x=x_0$，$y=y_0$ 是不定方程 $ax+by=c$，$(a,b)=1$ 的整数解的前提下，我们可以得到不定方程的无穷多个整数解：

$$\begin{cases} x=x_0+bt, \\ y=y_0-at \end{cases} \qquad (*)$$

其中 t 为任意整数. 这就回答了前面提出的第二个问题. 但 (*) 式是否给出了不定方程 $ax+by=c$，$(a,b)=1$ 的所有整数解是需要进一步讨论的，教科书上第二个“思考”栏目中的问题也就是我们将要讨论得问题，在内容结构上这个“思考”栏目也是起着承上启下的作用. 在证明了不定方程 $ax+by=c$，$(a,b)=1$ 的所有整数解均可以表示成 (*) 式的形式后，前面提出最后两个问题也就解决了.

需要指出的是，在本段讨论中条件 $(a,b)=1$ 是非常重要的. 我们发现，即使 $(a,b)\neq 1$，对任意整数 t，(*) 式给出的 x，y 也是不定方程 $ax+by=c$ 的整数解. 但是，此时不定方程 $ax+by=c$ 的某些解不能表示成 (*) 式的形式. 例如，$x=-2$，$y=-1$ 是不定方程 $4x-10y=2$ 的一个整数解，并且对任意整数 t，

$$\begin{cases} x=-2-10t, \\ y=-1-4t \end{cases} \qquad (**)$$

都是不定方程 $4x-10y=2$ 的整数解. 我们发现，$x=-7$，$y=-3$ 也是不定方程 $4x-10y=2$ 的整数解，但它不能表示成 (**) 式的形式，因为不存在整数 t，使得 $-7=-2-10t$.

另外，如果选取不同的特解 $x=x_0$，$y=y_0$ 和参数记号，(*) 中的表达式一般来说是不同的，但是它所表达的整数解的集合是完全一样的.

从 (*) 式可以看出，要求出不定方程 $ax+by=c$，$(a,b)=1$ 的所有整数解，我们只需先求出它

的一个特解即可. 对一些简单的二元一次不定方程，我们可以直接通过观察或实验得到它的一个特解. 对某些较复杂的二元一次不定方程，需要借助其他的方法，这也正是下一节需要探讨的内容.

教科书最后应用前面的结论，求解两个具体的一次不定方程，增强学生对二元一次不定方程有整数解的判别准则和有整数解时整数通解的认识，以及应用它们解决具体问题的能力.

2. 二元一次不定方程的特解

前面已经指出，对某些较复杂的二元一次不定方程 $ax+by=c$，$(a, b)=1$，我们很难通过直接的观察或者实验得到它的一个特解，往往需要借助其他的方法. 教师可以通过具体的例子增强学生对这个问题的感性认识. 例如，教师可以让学生观察不定方程

$$103x+231y=1$$

的一个特解. 因此寻求一个行之有效的求二元一次不定方程的特解的方法是十分必要的.

教科书介绍的是用辗转相除法计算 $ax+by=c$，$(a, b)=1$ 的特解的方法.

不失一般性，我们总可以假定 $b>0$，否则将原不定方程变形为 $(-a)x+(-b)y=-c$. 这样的处理使我们后面的讨论可以借用大衍求一术的算法步骤（选取 $n=b$）. 具体如下：

当 $b=1$ 时，我们可以直接观察 $ax+by=c$ 的一个特解 $x_0=1$，$y_0=c-a$.

当 $b>1$ 时，与大衍求一术的算法步骤类似，我们对 a，b 用辗转相除法，假设第 n 步后余数为 1，这样得到一系列商 q_1，q_2，…，q_n. 然后，由递推关系式

$$k_0=0,\ k_1=0,\ k_i=k_{i-2}-q\,k_{i-1}(i=2,\ \cdots,\ n)$$

依次计算出 k_2，…，k_n. 同样地，可以证明 $ak_n\equiv 1(\mathrm{mod}\ b)$，即 $b\mid 1-ak_n$. 选取

$$\begin{cases} x_0=k_nc, \\ y_0=\dfrac{c(1-ak_n)}{b}, \end{cases}$$

容易检验 $x=x_0$，$y=y_0$ 就是不定方程 $ax+by=c$，$(a, b)=1$ 的一个特解.

教科书上给出了上面算法的程序框图，学生理解和接受起来可能有些困难，教师可根据学校和学生的实际情况进行安排，也可略去不讲. 如果学校有条件且学生接受过计算机编程方面的训练，教师可以让学生上机实现. 对于不定方程 $23x-76y=3$，下面的计算机程序（Matlab）可供参考：

```
a=-23;
b=76;
c=-3;
u=a;
v=b;
i=0;
j=1;
k=j;
r=mod(u, v);
while r~=1
    u=v;
    v=r;
    r=mod(u, v);
    q=div(u, v);
    j=i-q*j;
    i=k;
```

```
    k=j;
end
x=c*k
y=div(c-a*x, b)
```

教科书在本节最后安排了一个用辗转相除法计算二元一次不定方程特解的例子，目的是进一步加深学生对这种算法的认识，并练习使用这种算法.

3. 多元一次不定方程

本节以三元和四元一次不定方程为例说明二元以上多元一次不定方程的解法，内容包括推导这两类不定方程有整数解的判别准则，以及将它们转化为二元一次不定方程进行求解. 需要指出的是，四元以上的多元一次不定方程的可解准则的推导和解法是完全类似的.

教科书在介绍三元一次不定方程的一般形式后，紧接着类似于二元一次不定方程的情形，推导三元一次不定方程 $ax+by+cz=d$ 有整数解的判别准则. 首先，我们推导 $ax+by+cz=d$ 有整数解时，整数 a，b，c，d 的特征：$(a, b, c)|d$. 这表明，$(a, b, c)|d$ 是不定方程 $ax+by+cz=d$ 有整数解的必要条件. 教科书第 38 页设置了一个“思考”栏目，目的是提示学生进一步探究 $(a, b, c)|d$ 是不是不定方程 $ax+by+cz=d$ 有整数解的充分条件.

在 $(a, b, c) \mid d$ 成立的前提下，我们利用最大公因数的性质和二元一次不定方程有整数解的条件，得到了三元一次不定方程 $ax+by+cz=d$ 的一组整数解，从而证明了 $(a, b, c) \mid d$ 也是不定方程 $ax+by+cz=d$ 有整数解的充分条件. 需要注意的是，这种处理方式还蕴涵了三元一次不定方程的解法，即将三元一次不定方程转化为两个二元一次不定方程进行求解.

事实上，如果仅是为了证明 $(a, b, c)|d$ 是不定方程 $ax+by+cz=d$ 有整数解的充分条件，我们还可以直接应用最大公因数的如下性质：

设整数 a，b，c 不同时为零，则存在整数 p，q，r，使得 $ap+bq+cr=(a, b, c)$. (1)

结论 (1) 的证明：令 $(a, b)=m$，则存在整数 u，v，使得 $au+bv=m$. 而 $(m, c)=(a, b, c)$，故存在整数 s，t，使得 $ms+ct=(a, b, c)$. 于是，

$$(au+bv)s+ct=aus+bvs+ct=(a, b, c).$$

选取整数 $p=us$，$q=vs$，$r=t$ 即可.

如果 $(a, b, c)|d$，不妨设 $d=(a, b, c)d'$，则由结论 (1) 知 $x=pd'$，$y=qd'$，$z=rd'$ 就是不定方程 $ax+by+cz=d$ 的一组整数解.

在得到三元一次不定方程有整数解的判别准则后，教科书只是简单地叙述了三元一次不定方程的解法. 另外，对一般的三元一次不定方程，教科书没有像二元一次不定方程那样写出整数通解的表示，这是因为它的整数通解叙述起来比较麻烦. 但是，对具体的三元一次方程来说，按教科书所述的求解方法容易得到它的整数通解.

为了加深对三元一次不定方程有整数解的可解准则和解法的认识，教科书上安排了一个求三元一次不定方程的整数解的例子（见教科书第 39 页的例 4）.

由于四元一次不定方程 $ax+by+cz+dw=e$ 有整数解的判别准则的推导过程与三元一次不定方程 $ax+by+cz=d$ 有整数解的判别准则的推导过程是完全类似的，所以教科书将其留给学生探究. 探究过程描述如下：

设四元一次不定方程 $ax+by+cz+dw=e$ 有整数解 $x=x_0$，$y=y_0$，$z=z_0$，$w=w_0$. 因为

$$(a, b, c, d)|a,\ (a, b, c, d)|b,\ (a, b, c, d)|c,\ (a, b, c, d)|d,$$

则 $(a, b, c, d)|ax_0+by_0+cz_0+dw_0=e$.

这表明，$(a, b, c, d)|e$ 是四元一次不定方程 $ax+by+cz+dw=e$ 有整数解的必要条件.

下面，我们再说明 $(a, b, c, d)|e$ 也是四元一次不定方程 $ax+by+cz+dw=e$ 有整数解的充分条件.

设 $(a, b, c, d)|e$，且记 $m=(a, b)$，$n=(m, c)$. 由于 $(n, d)=(a, b, c, d)|e$，故二元一次不定方程

$$nv+dw=e$$

有整数解 $v=v_0$，$w=w_0$. 又由于 $(m, c)=n|nv_0$，故二元一次不定方程

$$mu+cz=nv_0$$

有整数解 $u=u_0$，$z=z_0$. 再由 $(a, b)|mu_0$，二元一次不定方程

$$ax+by=mu_0$$

有整数解 $x=x_0$，$y=y_0$. 容易检验 $x=x_0$，$y=y_0$，$z=z_0$，$w=w_0$ 就是四元一次不定方程 $ax+by+cz+dw=e$ 的一组整数解.

综上所述，$(a, b, c, d)|e$ 是四元一次不定方程 $ax+by+cz+dw=e$ 有整数解的充要条件.

与三元一次不定方程的情形类似，上面的推导过程蕴含了四元一次不定方程的解法，即将其转化为三个二元一次不定方程进行求解. 对此，教科书上作了比较详细的描述.

教科书最后通过一个例子（见教科书第 39 页的例 5）向学生展示四元一次不定方程的解法. 教学时，教师可从本节习题的第 1 题（3）（4）中选取一个作为学生课堂练习用.

四、教学设计案例

二元一次不定方程（1 课时）

1. 教学任务分析

（1）探究二元一次不定方程有整数解的判别准则；

（2）探究二元一次不定方程有整数解时整数通解的表示；

（3）求解简单的二元一次不定方程及“百钱买百鸡”问题.

2. 教学重点与难点

重点：

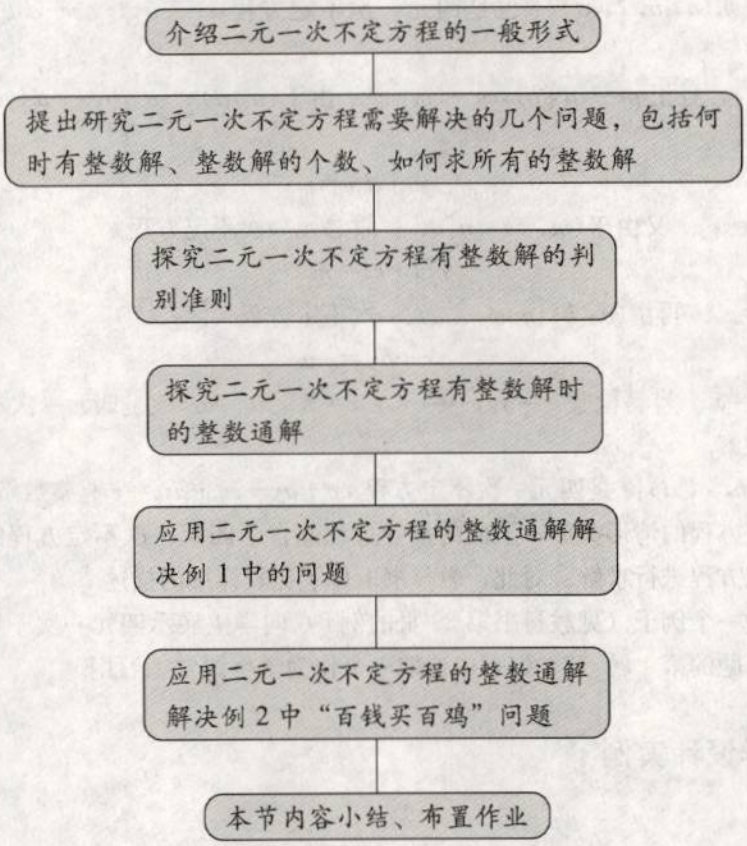
（1）理解二元一次不定方程有整数解的判别准则及其探究过程；

（2）理解二元一次不定方程有整数解时整数通解的探究过程；

（3）应用二元一次不定方程的整数通解求解简单的一次不定方程.

难点：探究二元一次不定方程有整数解的判定准则和整数通解的表示.

3. 教学基本流程



4. 教学情境设计

问题1：二元一次不定方程的一般形式为 $ax+by=c$，其中 a，b，c 为整数，且 a，b 不等于零. 那么，给定一个二元一次不定方程，它一定有整数解吗？试举例说明.

设计意图：让学生明确有些二元一次不定方程有整数解，而有些二元一次不定方程没有整数解，为后面问题的提出做准备.

师生活动：教师介绍二元一次不定方程的一般形式，并提出问题. 学生思考、回答老师提出的问题.

问题2：从上面的分析可以看出，二元一次不定方程不一定有整数解. 那么，研究二元一次不定方程需要解决哪些问题呢？

设计意图：让学生体会如何根据一些现象或事实提出问题，同时对本节后面的内容有一个总体的认识.

师生活动：教师提出问题，并引导学生思考. 学生分组讨论、交流后回答. 最后，由师生共同总结出：研究二元一次不定方程 $ax+by=c$，需要解决它何时有整数解？有整数解时是否有无穷多个整数解？这些整数解是否有统一的表达式？有整数解时如何求出所有的整数解？

问题3：下面我们分别解决上面提出的问题. 先考察二元一次不定方程 $ax+by=c$ 有整数解时，整数 a，b，c 应具有什么样的特征.

设计意图：让学生结合整除的性质，推导不定方程 $ax+by=c$ 有整数解时必有 $(a,b)|c$.

师生活动：学生尝试用整除的性质推导不定方程 $ax+by=c$ 有整数解的一个必要条件：$(a,b)|c$. 教师对学生的推导过程进行引导.

问题4：当$(a,b)|c$时，不定方程$ax+by=c$一定有整数解吗？（教科书第34页第1个“思考”栏目中的问题）

设计意图：让学生明确$(a,b)|c$既是不定方程$ax+by=c$有整数解的必要条件，又是充分条件，由此得到不定方程$ax+by=c$有整数解的一个判别准则．同时，培养学生分析问题、解决问题的能力．

师生活动：学生独立思考、回答，并尝试自己给出理由．教师纠正学生可能出现的逻辑错误．最后，由师生共同总结出教科书第34页框中的结论，即二元一次不定方程有整数解的判别准则．

问题5：前面已经解决了二元一次不定方程何时有整数解的问题．那么，二元一次不定方程有整数解时是否有无穷多个整数解呢？

设计意图：让学生明确每一个有整数解的二元一次不定方程总可以化为不定方程$ax+by=c$，$(a,b)=1$的形式，并且会根据它的一个整数解构造出无穷多个整数解．

师生活动：教师引导学生由不定方程$ax+by=c$，$(a,b)=1$的一个整数解$x=x_0$，$y=y_0$构造出它的无穷多个整数解：

$$\begin{cases}x=x_0+bt,\\y=y_0-at,\end{cases}\qquad(***)$$

其中t为任意整数．

问题6：不定方程$ax+by=c$，$(a,b)=1$的每一个整数解都可以表示成（$***$）式的形式吗？（教科书第34页第2个“思考”栏目中的问题）

设计意图：推导不定方程$ax+by=c$，$(a,b)=1$的整数解的统一表达式，从而得到它的全部整数解．

师生活动：教师提出问题后，引导学生分析、思考．学生运用整除的性质证明不定方程$ax+by=c$，$(a,b)=1$的每个整数解可以表示成（$***$）式的形式．最后，师生共同总结出教科书第35页框中的结论，即二元一次不定方程有整数解时整数通解的表示．

问题7：应用前面的结论，你能求解教科书上例1中的不定方程吗？

设计意图：让学生应用前面得到的结论，求解简单的二元一次不定方程，巩固所学知识．

师生活动：教师提出问题，学生独立解决，教师纠正可能出现的错误．

问题8：你能求解本讲引言中提出的“百钱买百鸡”问题吗？（教科书上的例2）

设计意图：让学生灵活运用二元一次不定方程的有关结论，解决一些历史名题，如“百钱买百鸡”问题，提高学生学习的兴趣．

师生活动：教师引导学生对“百钱买百鸡”问题进行分析，将其转化为求二元一次不定方程的非负整数解的问题．学生应用前面的结论解决问题．

最后，教师与学生一起对本节的内容进行小结，教师布置作业．

五、习题解答

习题（第36页）

1. 解：(1) 因为$(5,4)=1$，而$1|11$，所以不定方程有整数解，观察到不定方程$5x+4y=1$有一个特解$x=1$，$y=-1$．那么，$x=11$，$y=-11$就是原不定方程的一个特解．于是，原不定方程的整数通解为

$$\begin{cases}x=11+4t,\\y=-11-5t,\end{cases}$$

其中 t 为任意整数.

(2) 因为$(25, -13)=1$，而 $1 \mid 7$，所以不定方程有整数解. 观察到不定方程 $25x-13y=1$ 有一个特解 $x=-1$，$y=-2$. 那么，$x=-7$，$y=-14$ 就是原不定方程的一个特解. 于是，原不定方程的整数通解为

$$\begin{cases} x=-7-13t, \\ y=-14-25t, \end{cases}$$

其中 t 为任意整数.

2. 解：设大马、中马和小马的个数分别为 x，y，z，由题意得到下面的不定方程组：

$$\begin{cases} 3x+2y+\dfrac{1}{2}z=100, \\ x+y+z=100. \end{cases}$$

将不定方程中第一个方程的 2 倍减去第二个不定方程，得 $5x+3y=100$. 观察发现，不定方程 $5x+3y=1$有一个特解 $x=-1$，$y=2$. 那么 $x=-100$，$y=200$ 是不定方程 $5x+3y=100$ 的一个特解. 于是，不定方程 $5x+3y=100$ 的整数通解为

$$\begin{cases} x=-100+3t, \\ y=200-5t, \end{cases}$$

其中 t 为任意的整数. 注意到，$0 \leqslant x \leqslant 100$，$0 \leqslant y \leqslant 100$，则有

$$33\frac{1}{3} \leqslant t \leqslant 66\frac{2}{3}, \quad 20 \leqslant t \leqslant 40,$$

从而 $t=34, 35, 36, 37, 38, 39, 40$. 再将 x，y 的值代入方程 $x+y+z=100$，可求得原不定方程有七组非负整数解：

$$\begin{cases} x=2, \\ y=30, \\ z=68; \end{cases} \quad \begin{cases} x=5, \\ y=25, \\ z=70; \end{cases} \quad \begin{cases} x=8, \\ y=20, \\ z=72; \end{cases} \quad \begin{cases} x=11, \\ y=15, \\ z=74; \end{cases}$$

$$\begin{cases} x=14, \\ y=10, \\ z=76; \end{cases} \quad \begin{cases} x=17, \\ y=5, \\ z=78; \end{cases} \quad \begin{cases} x=20, \\ y=0, \\ z=80. \end{cases}$$

习题（第 38 页）

1. 解：(1) 因为$(103, 231)=1$，且 $1 \mid 21$，所以不定方程有整数解. 对 103，231 用辗转相除法，得 $103=231\times0+103$，$231=103\times2+25$，$103=25\times4+3$，$25=3\times8+1$，因此 $q_1=0$，$q_2=2$，$q_3=4$，$q_4=8$. 再由递推关系式依次计算得 $k_2=(-2)\times1+0=-2$，$k_3=(-4)\times(-2)+1=9$，$k_4=(-2)+(-8)\times9=-74$. 那么

$$\begin{cases} x_0=(-74)\times21=-1\,554, \\ y_0=\dfrac{21(1-103\times(-74))}{231}=693 \end{cases}$$

就是不定方程 $103x+231y=21$ 的一个特解. 于是，原不定方程的整数通解为

$$\begin{cases} x=-1\,554+231t, \\ y=693-103t, \end{cases}$$

其中 t 为任意的整数.

(2) 因为$(23, -76)=1$，且 $1 \mid 3$，所以不定方程有整数解. 对 23，-76 用辗转相除法，得 $23=(-76)\times0+23$，$-76=23\times(-4)+16$，$23=16\times1+7$，$16=7\times2+2$，$7=2\times3+1$，因此

$q_1=0$，$q_2=-4$，$q_3=1$，$q_4=2$，$q_5=3$. 再由递推关系式依次计算得 $k_2=-(-4)\times1+0=4$，$k_3=(-1)\times4+1=-3$，$k_4=4+(-2)\times(-3)=10$，$k_5=(-3)+(-3)\times10=-33$. 那么

$$\begin{cases}x_0=(-33)\times3=-99,\\ y_0=\dfrac{3(1-23\times(-33))}{(-76)}=-30\end{cases}$$

就是不定方程 $23x-76y=3$ 的一个特解. 于是，原不定方程的整数通解为

$$\begin{cases}x=-99-76t,\\ y=-30+23t,\end{cases}$$

其中 t 为任意的整数.

2. 解：首先求不定方程 $71x+12y=2\,004$ 的整数解. 因为$(71, 12)=1$，且 $1\mid 2\,004$，所以不定方程有整数解. 对 71，12 用辗转相除法，得 $71=12\times5+11$，$12=11\times1+1$. 因此 $q_1=5$，$q_2=1$. 再由递推关系式计算得 $k_2=(-1)\times1+0=-1$. 那么

$$\begin{cases}x_0=(-1)\times2\,004=-2\,004,\\ y_0=\dfrac{2\,004(1-71\times(-1))}{12}=12\,024\end{cases}$$

是不定方程 $71x+12y=2\,004$ 的一个特解. 于是，不定方程的整数通解为

$$\begin{cases}x=-2\,004+12t,\\ y=12\,024-71t,\end{cases}\qquad(*)$$

其中 t 为任意的整数.

下面求不定方程 $71x+12y=2\,004$ 的正整数解. 由于 x，y 为正整数，故整数 t 的变化范围为

$$t>167,\ t<169\frac{25}{71},$$

从而 $t=168$，169. 将 $t=168$，169 代入（*）式中可得原不定方程有两组正整数解：

$$\begin{cases}x=12,\\ y=96;\end{cases}\qquad\begin{cases}x=24,\\ y=25.\end{cases}$$

习题（第 40 页）

1. 解：(1) 因为$(5, -13)=1$，$(5, -13, 6)=(1, 6)=1\mid 10$，所以不定方程有整数解. 作不定方程 $5x-13y=t$ 和 $t+6z=10$. 分别解得这两个不定方程的整数通解为

$$\begin{cases}x=-5t-13k,\\ y=-2t-5k;\end{cases}\qquad\begin{cases}t=-50+6l,\\ z=10-l,\end{cases}$$

其中 k，l 为任意整数. 联立上面的两个通解表示式消去 t，便得到原不定方程的全部整数解

$$\begin{cases}x=250-30l-13k,\\ y=100-12l-5k,\\ z=10-l,\end{cases}$$

其中 k，l 为任意整数.

(2) 因为$(4, -10)=2$，$(4, -10, 21)=(2, 21)=1\mid 1$，所以不定方程有整数解. 作不定方程 $4x-10y=2t$ 和 $2t+21z=1$. 分别解得这两个不定方程的整数通解为

$$\begin{cases}x=-2t-5k,\\ y=-t-2k;\end{cases}\qquad\begin{cases}t=-10+21l,\\ z=1-2l,\end{cases}\qquad(*)$$

其中 k，l 为任意整数. 联立上面的两个通解表示式消去 t，便得到原不定方程的全部整数解

$$\begin{cases} x=20-42l-5k, \\ y=10-21l-2k, \\ z=1-2l, \end{cases}$$

其中 k，l 为任意整数.

(3) 因为$(3, 2)=1$，$(1, 6)=1$，$(3, 2, 6, -5)=(1, 6)=1\mid -4$，所以不定方程存在整数解. 作不定方程

$$3x+2y=u, \qquad u+6z=v, \qquad v-5w=-4,$$

分别求得上面三个二元一次不定方程的整数通解为

$$\begin{cases} x=u+2t_1, \\ y=-u-3t_1; \end{cases} \qquad \begin{cases} u=-5v+6t_2, \\ z=v-t_2; \end{cases} \qquad \begin{cases} v=1-5t_3, \\ w=1-t_3, \end{cases}$$

其中 t_1，t_2，t_3 为任意整数. 联合上述三个通解表达式，消去 u，v 得

$$\begin{cases} x=-5+25t_3+6t_2+2t_1, \\ y=5-25t_3-6t_2-3t_1, \\ z=1-5t_3-t_2, \\ w=1-t_3, \end{cases}$$

其中 t_1，t_2，t_3 为任意整数.

(4) 因为$(12, 8)=4$，$(4, -4)=4$，$(12, 8, -4, 14)=(4, 14)=2\mid 20$，所以不定方程存在整数解. 作不定方程 $12x+8y=4u$，$4u-4z=4v$，$4v+14w=20$，即

$$3x+2y=u, \qquad u-z=v, \qquad 2v+7w=10,$$

分别求得上面三个二元一次不定方程的整数通解为

$$\begin{cases} x=u+2t_1, \\ y=-u-3t_1; \end{cases} \qquad \begin{cases} u=v-t_2, \\ z=-t_2; \end{cases} \qquad \begin{cases} v=-2+7t_3, \\ w=2-2t_3, \end{cases}$$

其中 t_1，t_2，t_3 为任意整数. 联立上述三个通解表达式，消去 u，v 得

$$\begin{cases} x=-2+7t_3-t_2+2t_1, \\ y=2-7t_3+t_2-3t_1, \\ z=-t_2, \\ w=2-2t_3, \end{cases}$$

其中 t_1，t_2，t_3 为任意整数.

2. 解：设物数为 x，则 x 满足下面的不定方程：

$$x=3u+2, \qquad x=5v+3, \qquad x=7w+2.$$

解第一个不定方程得 $x=2-3k$，$u=-k$；将 $x=2-3k$ 代入第二个不定方程得

$$5v+3k=-1.$$

解不定方程得 $v=1+3l$，$k=-2-5l$. 于是，$x=2-3(-2-5l)=8+15l$. 再将 $x=8+15l$ 代入第三个不定方程得

$$7w-15l=6.$$

解不定方程得 $w=3-15t$，$l=1-7t$. 于是，$x=8+15\times(1-7t)=23-105t$，其中 t 为非负整数.

六、拓展资源

商高不定方程

公元前1100多年，我国古代数学家商高就提出了直角三角形的“勾广三，股修四，径隅五”的著名论断. 后人把直角三角形三边的这个特征叫做勾股定理. 商高的这个论断实际上给出了二元二次不定方程

$$x^2+y^2=z^2 \tag{1}$$

的一组正整数解 $x=3$，$y=4$，$z=5$. 我们把不定方程（1）叫做商高不定方程，把它的一组正整数解叫做勾股数.

公元263年，刘徽注的《九章算术》中除了上述勾股数外，又记载了一些勾股数：(5，12，13)，(8，15，17)，(7，24，25)，(20，21，29).

公元前500年，古希腊数学家毕达哥拉斯（Pythagoras）也证明了商高的结论，因此勾股定理也叫做毕达哥拉斯定理，商高不定方程也叫做毕达哥拉斯方程.

这里，我们简要介绍勾股数的一种统一表示. 假定$(x，y，z)$是一组勾股数，我们注意到如下事实：

(a) 当$(x，y)=d>1$时，$d^2\mid x^2$，$d^2\mid y^2$，故$d^2\mid x^2+y^2=z^2$，从而$d\mid z$. 那么，x，y，z是另一组勾股数的d倍. 例如，勾股数(6，8，10)是勾股数(3，4，5)的2倍.

(b) x，y不能同时为奇数. 若不然，令$x=2k+1$，$y=2l+1$，则

$$z^2=4(k^2+l^2)+4(k+l)+2.$$

故$2\mid z$，从而$4\mid z^2$，矛盾. 故x，y一奇一偶.

(c) $(y，x，z)$也是一组勾股数，即一组勾股数中x，y互换后仍是勾股数.

设$(x，y，z)$为勾股数，如果x为偶数，且$(x，y)=1$，那么把$(x，y，z)$叫做基本勾股数. 由前面的分析知，如果找出了所有的基本勾股数，那么通过交换基本勾股数中x，y的位置或将基本勾股数乘以正整数倍就可以得到所有的勾股数.

关于基本勾股数，我们有下面的统一表示.

定理 所有基本勾股数均可表示为

$$\begin{cases} x=2ab, \\ y=a^2-b^2, \\ z=a^2+b^2, \end{cases} \tag{2}$$

其中$(a，b)=1$，$a>b>0$，a，b一奇一偶.

证明：要证明（2）式给出$(x，y，z)$是基本勾股数，只需证明它是不定方程（1）的正整数解，满足$(x，y)=1$，且$2\mid x$. 注意到.

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

故由（2）式给出的$(x，y，z)$是不定方程（1）的正整数解，其中$2\mid x$是显然的.

现在证明$(x，y)=1$. 设$(x，y)=d$. 则$d\mid 2ab$，$d\mid a^2-b^2$，从而$d^2\mid 4a^2b^2$，$d^2\mid (a^2-b^2)^2$，于是$d^2\mid (a^2-b^2)^2+4a^2b^2=(a^2+b^2)^2$，$d\mid a^2+b^2$. 由整除的性质，$d\mid (a^2-b^2)+(a^2+b^2)=2a^2$，$d\mid (a^2+b^2)-(a^2-b^2)=2b^2$，$d\mid (2a^2，2b^2)$. 再由$(a，b)=1$知$(a^2，b^2)=1$. 因此，$d=1$，或$d=2$. 若$d=2$，则$y$为偶数，即$a^2-b^2$为偶数，这与$a$，$b$一奇一偶相矛盾. 故$d=1$，即$(x，y)=1$.

余下证明每个基本勾股数总可以表示成（2）式的形式. 设$(x，y，z)$为任一基本勾股数，则它是

不定方程（1）的整数解，满足$(x, y)=1$，$2|x$. 由于y，z均为奇数，故

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2}, \tag{3}$$

其中$\frac{z+y}{2}$，$\frac{z-y}{2}$为整数.

设

$$d=\left(\frac{z+y}{2}, \frac{z-y}{2}\right),$$

则$d|\frac{z+y}{2}+\frac{z-y}{2}=z$，$d|\frac{z+y}{2}-\frac{z-y}{2}=y$，从而$d\mid x$. 由于$(x, y)=1$，故$d=1$. 再由（3）式知，$\frac{z+y}{2}$与$\frac{z-y}{2}$均为完全平方数. 于是存在正整数$a$，$b$使得

$$\frac{z+y}{2}=a^2,\ \frac{z-y}{2}=b^2,\ \frac{x}{2}=ab,$$

其中$(a, b)=1$. 即有$x=2ab$，$y=a^2-b^2$，$z=a^2+b^2$，a，$b>0$，$(a, b)=1$. 注意到$y>0$，且y为奇数，则$a>b$，且a，b一奇一偶.

综上所述，所有的基本勾股数x，y，z均可以表达成（2）式的形式.

例 求证：在边长为正整数的直角三角形中，

（1）必有一条直角边的长是3的倍数；

（2）必有一条直角边的长是4的倍数；

（3）必有一条边的长是5的倍数.

证明：设直角三角形的三边长分别为x，y，z，则$x^2+y^2=z^2$. 只需证明(x, y, z)为基本勾股数时结论成立即可. 由定理1，设

$$x=2ab,\quad y=a^2-b^2,\quad z=a^2+b^2,$$

其中$(a, b)=1$，$a>b>0$，a，b中一奇一偶.

（1）若$3|a$，或$3|b$，则$3|2ab=x$；若3既不整除a也不整除b，则$a=3k\pm1$，$b=3l\pm1$，从而有

$$y=a^2-b^2=(3k\pm1)^2-(3l\pm1)^2=3(3k^2+3l^2\pm2k\pm2l),$$

故$3|y$.

（2）由于a，b一奇一偶，故$4|2ab=x$.

（3）若5不整除x，也不整除y，下证$5|z$. 由于x是偶数，故x^2的个位数为4或6；由于y是奇数且5不整除y，则y^2的个位数为1或9. 由此得$x^2+y^2=z^2$的个位数只可能为5，3，7. 显然，一个完全平方数的个位数不可能为3，7. 故z^2的个位数只能为5，从而$5|z$.

从上面的例子还可以看出，在边长为正整数的直角三角形中，三边长的乘积一定能被60整除.

III 自我检测题

一、选择题（每小题只有一个正确选项）.

1. 能同时被9和11整除的整数是（　　）

（A）6 758 991　　（B）6 340 332　　（C）7 584 192　　（D）1 599 180

2. 2 035除以某个整数，商为75，则除数为（　　）

(A) 25　　(B) 26　　(C) 27　　(D) 28

3. 只有两个正因数的正整数是（　　）

(A) 667　　(B) 431　　(C) 221　　(D) 649

4. 下列叙述中不正确的是（　　）

(A) 当 a，b 不全为零时，a，b 的公因数一定整除(a, b)

(B) 若存在整数 s，t 使得 $as+bt=1$，则$(a, b)=1$

(C) 若 $a|bc$，则 $a|b$，或 $a|c$

(D) 当 a，b 为非零整数时，$[a, b]$一定整除 ab

5. 今天是星期一，问 3^{50} 天后的今天是（　　）

(A) 星期二　　(B) 星期三　　(C) 星期四　　(D) 星期五

6. 在模 n 的剩余类环中，叙述正确的是（　　）

(A) 每个非零元均有逆元

(B) 总存在一个非零元没有逆元

(C) 有的非零元没有负元

(D) 当 n 为素数时，模 n 的剩余类环无零因子

7. 使同余式 $7^x \equiv 1 \pmod{18}$成立的整数 x 是（　　）

(A) 26　　(B) 22　　(C) 30　　(D) 28

8. 下列算式错误的是（　　）

(A) 4 327+7 883=12 210

(B) 76 541−34 455=42 086

(C) 4 567×3 452=15 645 284

(D) 66 384 835÷9 845=6 743

二、填空题.

9. 120～150 中的素数为_____

10. $(276, 345)=$_____，$[276, 345]=$_____

11. 所有能表示成 $12x+21y$ 的整数中，最小的正整数为_____

12. 2^{100} 被 19 除后的余数为_____

13. 在模 10 的剩余类环中，存在逆元的非零元为_____

14. 一次同余方程 $21x \equiv 9 \pmod{15}$的解为_____

15. 若多项式 $f(x)$的次数小于 3，且满足 $f(1)=-1$，$f(-1)=1$，$f(2)=1$，则 $f(x)=$_____

16. 不定方程 $3x+4y=30$ 的非负整数解为_____

三、解方程.

17. 解同余方程组
$$\begin{cases} x \equiv 4 \pmod 9, \\ x \equiv 3 \pmod 4, \\ x \equiv 1 \pmod 5. \end{cases}$$

18. 求四元一次不定方程 $4x+8y+3z+5w=2$ 的全部整数解.

四、证明题.

19. 设$(a, b)=1$，证明：对任意正整数 n，$(a^n, b^n)=1$.

参考答案

一、选择题.

1. C. 2. C. 3. B. 4. C. 5. B. 6. D. 7. C. 8. C.

二、填空题.

9. 127，131，137，139，149

10. 69；1 380

11. 3

12. 17

13. [1]，[3]，[7]，[9]

14. $x\equiv4(\mathrm{mod}\ 15)$，$x\equiv9(\mathrm{mod}\ 15)$，$x\equiv14(\mathrm{mod}\ 15)$

15. x^2-x-1

16. (10，0)，(6，3)，(2，6)

三、解方程.

17. 由于 9，4，5 两两互素，故可以用孙子定理. 解同余方程 $4\times5c_1=20c_1\equiv1(\mathrm{mod}\ 9)$得 $c_1\equiv5(\mathrm{mod}\ 9)$；再解同余方程 $9\times5c_2=45c_2\equiv1(\mathrm{mod}\ 4)$得 $c_2\equiv1(\mathrm{mod}\ 4)$；最后解同余方程 $9\times4c_3=36c_3\equiv1(\mathrm{mod}\ 5)$得 $c_3\equiv1(\mathrm{mod}\ 9)$. 于是，选取 $c_1=5$，$c_2=1$，$c_3=1$，得

$$x\equiv4\times4\times5\times5+3\times9\times5\times1+1\times9\times4\times1=571\equiv31(\mathrm{mod}\ 180).$$

18. 因为$(4，8)=4$，$(4，3)=1$，$(4，8，3，5)=(1，5)=1\mid2$，所以不定方程存在整数解. 作不定方程

$$4x+8y=4u\ (\text{即}\ x+2y=u)，4u+3z=v，v+5w=2.$$

分别求得上面三个二元一次不定方程的整数通解为

$$\begin{cases}x=-u+2t_1,\\ y=u-t_1;\end{cases}\quad\begin{cases}u=v+3t_2,\\ z=-v-4t_2;\end{cases}\quad\begin{cases}v=-3+5t_3,\\ w=1-t_3;\end{cases}$$

其中 t_1，t_2，t_3 为任意整数. 联合上述三个通解表达式，消去 u，v 得原不定方程的整数通解

$$\begin{cases}x=3-5t_3-3t_2+2t_1,\\ y=-3+5t_3+3t_2-t_1,\\ z=3-5t_3-4t_2,\\ w=1-t_3,\end{cases}$$

其中 t_1，t_2，t_3 为任意整数.

四、证明题.

19. 证明：设 $(a^n，b^n)=d$，下面只需证明 $d=1$ 即可.

反证法：假设 $d>1$，则存在素数 p，使得 $p\mid d$. 由于 $d\mid a^n$，故 $p\mid a^n$，而 p 是素数，所以 $p\mid a$. 同样地，由于 $d\mid b^n$，故 $p\mid b^n$，而 p 是素数，所以 $p\mid b$. 于是，$p\mid(a，b)=1$，矛盾. 所以，假设不成立，即 $d=1$.