四川理工学院课程实施大纲

课程名称：初等数论

授课班级：应数 2013 级 1,2 班

任课教师：卢天秀

工作部门：理学院

联系方式：13408138464

四川理工学院 制

2016 年 1 月

《初等数论》课程实施大纲

基本信息

课程代码：

课程名称：初等数论

学　　分：3

总 学 时：45

学　　期：2015-2016 下期

上课时间：1-12 周，周一上午 3、4 节，周三上午 1、2 节。

上课地点：N1-422，N1-422,

答疑时间和方式：每周二下午 9,10 节当面答疑；随时可以电话、短信、邮件、QQ 答疑。

答疑地点：厚德楼 325

授课班级：应数 2013 级 1,2 班

任课教师：卢天秀

学　　院：理学院

邮　　箱：lubeeltx@163.com

联系电话：13408138464

目　录

教学理念..... 1

课程介绍..... 3

1、课程的性质.....3

2、课程在学科专业结构中的地位、作用.....3

3、学习本课程的必要性.....4

4、课程教学要求.....4

教师简介..... 5

先修课程..... 6

课程目标..... 6

课程内容..... 7

1、课程的内容概要.....7

2、教学重点、难点.....9

3、学时安排.....10

课程实施..... 11

第一章 整数的可除性.....11

一　数的整除性.....10

二　带余除法.....13

三　最大公约数.....14

四　最小公倍数.....16

五　辗转相除法.....18

六　算术基本定理.....19

七　函数[x]与{x}.....21
八　素数.....22
第二章　不定方程..... 26
一　二元一次不定方程的定义和解法.....26
二　勾股数.....28
三　几个特殊不定方程的解法.....31
第三章　同余..... 34
一　同余的基本性质.....34
二　完全剩余系.....37
三　简化剩余系.....38
四　Euler 定理..... 40
第四章　同余式..... 43
一　同余式的基本概念.....43
二　孙子定理.....46
三　模的　同余方程.....47
四　素数模的同余方程.....49
第五章　连分数..... 52
一　连分数的定义及基本性质.....52
二　实数的连分数表示.....54
三　循环连分数.....55
课程要求..... 57
1、学生自学要求.....57

2、课外阅读要求.....57
3、课堂讨论要求.....57
课堂规范..... 58
1、课堂纪律.....58
2、课堂礼仪.....96
课程考核..... 60
1、出勤（迟到、早退等）、作业、报告等的要求..... 60
2、成绩的构成与评分规则说明.....60
3、考试形式及说明.....60
学术诚信..... 60
课程资源..... 61
1、教材与参考书.....61
2、专业学术著作.....61
3、专业刊物.....62
4、网络课程资源.....62
5、课外阅读资源.....62
教学合约..... 63

教学理念

古有“一日为师，终身为父”、“师者，传道、授业、解惑也”的说法，今有“春蚕到死丝方尽，蜡炬成灰泪始干”的名句，“身为世范，为人师表”的谨言，可见教师在学生成长和发展中的不可取代的重要作用。因此，教师在日常的教学活动中，就要时时关注学生的需要与发展。

1、以人为本。重视教育对象，尊重教育对象，爱护教育对象，赏识教育对象，提升和发展人的精神文化品质。公平对待每一个学生，不以个人的私利和好恶为标准。现代教育的特征就是发展人的主体性，教师不能一直充当“主角”，而让学生仅仅充当的是“配角”，剥夺了他们自主学习的权利。通过学习和教育达到自身的和谐发展，是人类认识自然和社会、不断完善和发展自我的必由之路。

2、全面发展。人的全面发展是社会发展的根本问题，也是教育的根本目的和价值取向。人的全面发展理论是马克思主义理论的重要组成部分。在教学过程中，教师应注重学生知识结构的完整性和全面性，在学习专业知识的同时，提高思想道德素质和文化素质。知识、技能，过程、方法与情感、态度、价值观三维目标的整合。即，相对于人的发展这一总目标，任一维度的目标都不能脱离整体而单独优质服务，缺失任一维度都无法实现真正意义上的发展。

3、素质教育。更加注重教育的过程，将传授知识和培养创造性思维结合，通过点拨、启发、引导和训练，挖掘学生的潜力，提高主观能动性。培养学生的自学能力、实践能力、创新能力。鼓励学生积极反思、大胆批

判和实践运用。通过对现实世界的关注，使学生得到情感体验、人格提升、个性张扬，同时使教师的职业生命活力得以焕发，师生生命在交往互动、共同经历中不断生成的信念系统。在教育日益专业化的今天，大学教育必须更新教育理念，大力加强素质教育，才能实现对人的改造和自身的重建，培育健全的人格和品质，促进人的全面和谐的发展。

4、因材施教。最早应源于我国古代的教育家，思想家孔子提出的育人要“深其深，浅其浅，益其益，尊其尊”，即“因材施教，因人而异”的主张；原苏联教育家维果茨基的“最近发展区”理论则认为：每个学生都存在着两种发展水平，一是现有水平，二是潜在水平，它们的区域被称为“最近发展区”教学，只有从这两种水平的个性差异出发，把最近发展区转化为现有发展水平，并不断创造出更高水平的最近发展区，才能促进学生的发展；美国学者卡罗尔也提出：“如果提供足够的时间，再具备合适的学习材料和教学环境，那么，几乎所有的学生都有可能达到即定的目标。”不同的学生个体也完全可能由于知识和思维方法等方面的差异，而具有不同的思维过程。因此，在教学中要正确对待学生中客观存在的差异，不过分追求统一性，一致性。教师可以一边组织大多数同学进行针对性的练习，巩固性的练习，一边让学有余力，探究欲望强烈的学生深入探究。

课程介绍

1、 课程的性质

“初等数论”课程是数学学科专业的一门专业必修课程。它是以讨论整数性质为中心的一门学科，数学专业的学生学习初等数论的基础知识可以加深对数的性质的了解与认识，便于理解和学习与其相关的一些课程。数论是研究整数性质的一门很古老的数学分支，其初等部分是以整数的整除性为中心的，包括整除性、不定方程、同余式、连分数、素数（即整数）分布以及数论函数等内容，统称初等数论（elementary number theory）。

数论的研究方法和观点，对其他学科产生了越来越大的影响，而且随着科学技术的不断进步，特别是计算机的发展与推广，初等数论的思想、理论和方法的应用日趋广泛。

2、 课程在学科专业结构中的地位、作用

初等数论的大部份内容早在古希腊欧几里德的《几何原本》中就已出现。欧几里得证明了素数有无穷多个，他还给出求两个自然数的最大公约数的方法， 即所谓欧几里得算法。我国古代在数论方面亦有杰出之贡献，现在一般数论书中的“中国剩余定理”正是我国古代《孙子算经》中的下卷第 26 题，我国称之为“孙子定理”。

近代初等数论的发展得益于费马、欧拉、拉格朗日、勒让德和高斯等人的工作。1801 年，高斯的《算术探究》是数论的划时代杰作。高斯还提出：“数学是科学之王，数论是数学之王”。可见高斯对数论的高度评价。

由于自 20 世纪以来引进了抽象数学和高等分析的巧妙工具，数论得到进一步的发展，从而开阔了新的研究领域，出现了代数数论、解析数论、几何数论等新分支。而且近年来初等数论在计算机科学、组合数学、密码学、代数编码、计算方法等领域内更得到了广泛的应用，无疑同时间促进着数论的发展。

3、 学习本课程的必要性

《初等数论》的内容和中小学数学联系比较紧密，对中小学数学中整数理论和方程理论进行了总结和提升，它是现代数学的重要基础。学习初等数论可以指导中学数学教学与实践，能在高观点下看清中学数学知识的来龙去脉，对提高高校教师和中小学教师的数学素养和教学质量有着重要的意义，还可以培养学生的科学思维、逻辑推理、运算能力以及辩证唯物论观点。

初等数论的理论和方法已广泛应用于现代密码学、算子理论、代数编码、最优设计、信息科学等诸多领域。例如，同余理论就和算子理论、抽象代数、抽象群理论、几何学及组合数学有着非常紧密的关系。

4、 课程教学要求

讲授本课程要贯彻“夯实基础，培养能力，提高科研水平”的教育方针的基本方针，依据“有用、有效、先进”的指导原则，重点放在培养学生的概括能力、推理能力、计算能力、探究能力上。

通过本课程的学习，让学生能够系统地理解和掌握初等数论的基本概念、理论和方法。提高学生的数学素养。学会运用初等数论的方法和技巧

分析解决数学理论学习和应用数学学科中遇到的有关问题。具体的说，要让学生理解整数理论的相关概念、质因数分解定理，会用筛法求素数；理解整数同余的概念及同余的基本性质，熟练运用同余的基本性质；理解剩余类、完全剩余系的概念，熟练掌握判断剩余系的方法；了解 Fermat 小定理，熟练运用之；理解中国剩余定理，掌握中国剩余定理的简单应用，掌握求解简单同余式方程组的方法；理解欧拉函数的定义及性质，了解欧拉定理，掌握循环小数的判定方法；掌握二元一次不定方程解的形式、二元一次不定方程有整数解的条件，熟练掌握利用辗转相除法求二元一次不定方程的方法，知道不定方程 $x^2+y^2=z^2$ 的整数解的形式；掌握连分数、有限、无限连分数的概念，理解它们之间的关系，渐近分数及其之间的递推关系式，理解有限、无限连分数与有理数、无理数之间的关系。

教师简介

卢天秀，四川理工学院副教授，博士研究生。1998 年在重庆师范大学数学与计算机系本科毕业；2010 年电子科技大学数学科学学院硕士毕业，研究方向为拓扑学及其应用；2013 年电子科技大学数学科学学院博士毕业，研究方向为混沌理论及其应用。从事教学工作 18 年来，担任过《数学分析》、《高等代数》、《概率论与数理统计》、《近世代数》、《初等数论》、《离散数学》《模糊数学》、《组合数学》、《拓扑学》、《线性代数》、《高等数学》、《高代选讲》等课程的教学。

先修课程

学习《初等数论》这门学科，需要有一些中学数学知识和一些基本的多项式理论、函数理论，若先修《高等代数》中的多项式部分，会对初等数论中定义的内涵外延，定理的条件结论和证明理解更加深入。

课程目标

讲授本课程要贯彻“夯实基础，培养能力，提高科研水平”的教育方针的基本方针，依据“有用、有效、先进”的指导原则，重点放在培养学生的概括能力、推理能力、计算能力、探究能力上。

1、让学生了解初等数论建立的背景和历史，系统掌握初等数论的基本概念与基本理论。主要是不定方程、同余和连分数理论。

2、历史上遗留下来没有解决的大多数数论难题其问题本身容易搞懂，容易引起人们的兴趣，但是解决它们却非常困难。鼓励学生思考、研究这些问题。

在教学方法上要做到：

1、加强对知识重点与难点的讲解，组织学生进行课堂讨论，促使学生对重点及难点的牢固掌握；

2、加强对学生自学能力的指导与培养；

3、培养学生发现问题，分析问题，解决问题的能力。

课程内容

1、 课程的内容概要

第一章 整数的可除性（8 学时）

1、整除性、公因数、公倍数

两个整数整除的概念、剩余定理；最大公因子的概念、性质及求最大公因子的方法；最小公倍数的概念、性质及最小公倍数的求法。

2、素数与整数的素因子分解

素数与合数的概念、素数的性质、整数关于素数的分解定理、素数的求法（筛法）。

3、取整函数和取小函数及其性质

取整函数和取小函数的定义和性质，利用取整函数求$n!$的标准分解式。

第二章 不定方程（6 学时）

1、二元一次不定方程

二元一次不定方程的形式，二元一次不定方程解的形式，二元一次不定方程有整数解的条件，利用辗转相除法求二元一次不定方程的解。

2、多元一次不定方程

通过二元一次不定方程的求解

3、勾股数

不定方程$x^2+y^2=z^2$的整数解的形式，Fermat 大定理的简单介绍。

第三章 同余（12 学时）

1、同余的概念及性质

整数同余的概念、同余的基本性质，利用同余简单验证整数乘积运算的结果。

2、剩余类、完全剩余系

剩余类、完全剩余系的概念，判断剩余系的方法。

3、费马小定理

费马小定理及其应用，求余数的方法。

4、欧拉函数、欧拉定理

欧拉函数的定义，欧拉定理，循环小数的判定条件。

第四章　同余式（12 学时）

1、一次同余式

同余式的概念，一次同余式的解法

2、一次同余式组

中国剩余定理的内容，中国剩余定理的应用，求解同余式方程组。

3、高次同余式

高次同余式的通用解法和便捷解法（利用一次同余式组）

第五章　连分数（8 学时）

1、连分数、渐近分数

连分数、渐近分数的含义，它们之间的递推关系式

2、有限、无限连分数

有限、无限连分数的概念，以及它们与有理数、无理数之间的关系

2、 教学重点、难点

重点

1、整除、公因子、素数的概念及性质，裴蜀恒等式，求最大公因子的方法，整数的素数分解定理；

2、二元一次不定方程解的形式，二元一次不定方程有整数解的条件，利用辗转相除法求二元一次不定方程的解；

3、剩余系的判定，欧拉函数的定义及性质，中国剩余定理，同余性质的运用；

4、连分数、渐近分数及其之间的递推关系；有限、无限连分数与有理数、无理数之间的关系。

难点

1、整数的素数分解定理的理解与运用函数[x]、{x}的概念及其应用；

2、不定方程$x^2+y^2=z^2$的整数解的形式；

3、剩余系的判定，中国剩余定理，费马小定理应用；

4、连分数、渐近分数及其之间的递推关系。

3、学时安排

教学内容	课时数	合计
1.1 整除的概念，带余除法 1.2 最大公因数与辗转相除法 1.3 整除的进一步性质及最小公倍数 1.4 质数，算数基本定理 1.5 函数[x],{x}及其在数论中的一个应用	10 学时	44 学时
2.1 二元一次不定方程 2.2 多元一次不定方程 2.3 勾股数	8 学时	
3.1 同余的概念及其基本性质 3.2 剩余类及完全剩余系 3.3 简化剩余系与欧拉函数 3.4 欧拉定理，费马定理及其对循环小数的应用	10 学时	
4.1 基本概念及一次同余式 4.2 孙子定理 4.3 高次同余式的解数与解法 4.4 质数模的同余式	8 学时	
7.1 连分数的基本性质 7.2 把实数表成连分数 7.3 循环连分数	8 学时	

课程实施

第一章 整数的可除性

教学日期：2016. 2.29，2016.3.2，2016.3.7，2016.3.9，2016.3.14

教学方法：讲授+提问+讨论；板书+PPT

教学重点：整除性理论是初等数论的基础。本章主要介绍整除性理论中的概念和相关性质。取整函数、取小函数的定义和应用。

难点：第 3 节，整除的进一步性质中定理 1 的内容及其证明（即辗转相处发中各余数项与不完全商之间的关系）；n!的标准分解式中质因数 p 的指数的求法。

教学内容

本章基本概念有：整除，倍数，约数（因数或除数），平凡约数，非平凡约数。偶数，奇数。素数（质数）、合数、商（不完全商）、余数、公约数、最大公约数、公倍数、最小公倍数、互素、辗转相除法、标准分解式、取整函数，取小函数。

一、数的整除性（60 分钟）

定理 1 下面的结论成立：

(ⅰ) $a\mid b \Leftrightarrow \pm a\mid \pm b$；

(ⅱ) $a\mid b$，$b\mid c \Rightarrow a\mid c$；

(iii) $b \mid a_i$，$i = 1, 2, \cdots, k \Longrightarrow b \mid a_1x_1 + a_2x_2 + \cdots + a_kx_k$，此处 x_i（$i = 1, 2, \cdots, k$）是任意的整数；

(iv) $b \mid a \Longrightarrow bc \mid ac$，此处 c 是任意的非零整数；

(v) $b \mid a$，$a \neq 0 \Longrightarrow |b| \leq |a|$；$b \mid a$ 且 $|a| < |b| \Longrightarrow a = 0$。

定理 2 任何大于 1 的整数 a 都至少有一个素约数。

推论 任何大于 1 的合数 a 必有一个不超过 $\sqrt{a}$ 的素约数。

例 1 设 r 是正奇数，证明：对任意的正整数 n，有

$$n + 2 \nmid 1^r + 2^r + \cdots + n^r。$$

例 2 设 $A = \{ d_1, d_2, \cdots, d_k \}$ 是 n 的所有约数的集合，则

$$B = \{\frac{n}{d_1}, \frac{n}{d_2}, \cdots, \frac{n}{d_k}\}$$

也是 n 的所有约数的集合。

例 3 以 $d(n)$ 表示 n 的正约数的个数，例如：$d(1) = 1$，$d(2) = 2$，$d(3) = 2$，$d(4) = 3$，$\cdots$。问：

$$d(1) + d(2) + \cdots + d(1997)$$

是否为偶数？

例 4 设凸 $2n$ 边形 M 的顶点是 $A_1, A_2, \cdots, A_{2n}$，点 O 在 M 的内部，用 $1, 2, \cdots, 2n$ 将 M 的 $2n$ 条边分别编号，又将 $OA_1, OA_2, \cdots, OA_{2n}$ 也同样进行编号，若把这些编号作为相应的线段的长度，证明：无论怎么编号，都不能使得三角形 $OA_1A_2, OA_2A_3, \cdots, OA_{2n}A_1$ 的周长都相等。

例 5 设整数 $k \geq 1$，证明：

(i) 若 $2^k \leq n < 2^{k+1}$，$1 \leq a \leq n$，$a \neq 2^k$，则 $2^k \nmid a$；

(ii) 若 $3^k \leq 2n - 1 < 3^{k+1}$，$1 \leq b \leq n$，$2b - 1 \neq 3^k$，则 $3^k \nmid 2b - 1$。

例 6　证明：存在无穷多个正整数 a，使得

$$n^4 + a（n = 1, 2, 3, \cdots）$$

都是合数。

例 7　设 $a_1, a_2, \cdots, a_n$ 是整数，且

$$a_1 + a_2 + \cdots + a_n = 0，\ a_1 a_2 \cdots a_n = n，$$

则 $4 \mid n$。

例 8　若 n 是奇数，则 $8 \mid n^2 - 1$。

例 8 的结论虽然简单，却是很有用的。例如，使用例 3 中的记号，我们可以提出下面的问题：

问题　$d(1)^2 + d(2)^2 + \cdots + d(1997)^2$ 被 4 除的余数是多少？

例 9　证明：方程

$$a_1^{\,2} + a_2^{\,2} + a_3^{\,2} = 1999 \tag{1}$$

无整数解。

二、带余除法（60 分钟）

定理 1(带余数除法)　设 a 与 b 是两个整数，$b \neq 0$，则存在唯一的两个整数 q 和 r，使得

$$a = bq + r，\ 0 \leq r < |b|。 \tag{1}$$

由定理 1 可知，对于给定的整数 b，可以按照被 b 除的余数将所有的整数分成 b 类。在同一类中的数被 b 除的余数相同。这就使得许多关于全体整数的问题可以归化为对有限个整数类的研究。

以后在本书中，除特别声明外，在谈到带余数除法时总是假定 b 是正整数。

例 1　设 a，b，x，y 是整数，k 和 m 是正整数，并且

$$a = a_1 m + r_1，\ 0 \le r_1 < m，$$

$$b = b_1 m + r_2，\ 0 \le r_2 < m，$$

则 $ax + by$ 和 ab 被 m 除的余数分别与 $r_1 x + r_2 y$ 和 $r_1 r_2$ 被 m 除的余数相同。特别地，a^k 与 $r_1^{\,k}$ 被 m 除的余数相同。

例 2　设 $a_1, a_2, \cdots, a_n$ 为不全为零的整数，以 y_0 表示集合

$$A = \{\, y；\ y = a_1 x_1 + \cdots + a_n x_n，\ x_i \in \mathbf{Z}，\ 1 \le i \le n \,\}$$

中的最小正数，则对于任何 $y \in A$，$y_0 \mid y$；特别地，$y_0 \mid a_i$，$1 \le i \le n$。

例 3　任意给出的五个整数中，必有三个数之和被 3 整除。

例 4　设 $a_0, a_1, \cdots, a_n \in \mathbf{Z}$，$f(x) = a_n x^n + \cdots + a_1 x + a_0$ ，已知 $f(0)$与 $f(1)$都不是 3 的倍数，证明：若方程 $f(x) = 0$ 有整数解，则

$$3 \mid f(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^n a_n \ 。$$

例 5　证明：对于任意的整数 n，$f(n) = 3n^5 + 5n^3 + 7n$ 被 15 整除。

例 6　设 n 是奇数，则 $16 \mid n^4 + 4n^2 + 11$。

例 7　证明：若 a 被 9 除的余数是 3，4，5 或 6，则方程 $x^3 + y^3 = a$ 没有整数解。

三、最大公约数（40 分钟）

定理 1　下面的等式成立：

(ⅰ)　$(a_1, a_2, \cdots, a_k) = (|a_1|, |a_2|, \cdots, |a_k|)$；

(ⅱ)　$(a, 1) = 1$，$(a, 0) = |a|$，$(a, a) = |a|$；

(ⅲ)　$(a, b) = (b, a)$；

(ⅳ)　若 p 是素数，a 是整数，则$(p, a) = 1$ 或 $p \mid a$；

(ⅴ) 若 $a = bq + r$，则$(a, b) = (b, r)$。

由定理 1 可知，在讨论$(a_1, a_2, \cdots, a_n)$时，不妨假设 $a_1, a_2, \cdots, a_n$ 是正整数，以后我们就维持这一假设。

定理 2 设 $a_1, a_2, \cdots, a_k \in \mathbf{Z}$，记

$$A = \{ y;\ y = \sum_{i=1}^{k} a_i x_i\ ,\ x_i \in \mathbf{Z},\ 1 \le i \le k \}。$$

如果 y_0 是集合 A 中最小的正数，则 $y_0 = (a_1, a_2, \cdots, a_k)$。

推论 1 设 d 是 $a_1, a_2, \cdots, a_k$ 的一个公约数，则 $d \mid (a_1, a_2, \cdots, a_k)$。

这个推论对最大公约数的性质做了更深的刻划：最大公约数不但是公约数中的最大的，而且是所有公约数的倍数。

推论 2 $(ma_1, ma_2, \cdots, ma_k) = |m|(a_1, a_2, \cdots, a_k)$。

推论 3 记$\delta = (a_1, a_2, \cdots, a_k)$，则

$$(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \cdots, \frac{a_k}{\delta}) = 1,$$

特别地，$(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$。

定理 3 $(a_1, a_2, \cdots, a_k) = 1$ 的充要条件是存在整数 $x_1, x_2, \cdots, x_k$，使得

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1。 \qquad (1)$$

定理 4 对于任意的整数 a，b，c，下面的结论成立：

(ⅰ) 由 $b \mid ac$ 及$(a, b) = 1$ 可以推出 $b \mid c$；

(ⅱ) 由 $b \mid c$，$a \mid c$ 及$(a, b) = 1$ 可以推出 $ab \mid c$。

推论 1 若 p 是素数，则下述结论成立：

(ⅰ) $p \mid ab \Longrightarrow p \mid a$ 或 $p \mid b$；

(ⅱ) $p \mid a^2 \Longrightarrow p \mid a$。

推论 2 若 $(a, b) = 1$，则$(a, bc) = (a, c)$。

推论 3　若 $(a, b_i) = 1$，$1 \le i \le n$，则$(a, b_1b_2\cdots b_n) = 1$。

定理 5　对于任意的 n 个整数 $a_1, a_2, \cdots, a_n$，记

$$(a_1, a_2) = d_2，(d_2, a_3) = d_3，\cdots，(d_{n-2}, a_{n-1}) = d_{n-1}，(d_{n-1}, a_n) = d_n，$$

则

$$d_n = (a_1, a_2, \cdots, a_n)。$$

例 1　证明：若 n 是正整数，则$\frac{21n+4}{14n+3}$是既约分数。

注：一般地，若$(x, y) = 1$，那么，对于任意的整数 a，b，有

$$(x, y) = (x - ay, y) = (x - ay, y - b(x - ay)) = (x - ay, (ab + 1)y - bx)，$$

因此，$\frac{x-ay}{(ab+1)y-bx}$是既约分数。

例 2　证明：$121 \nmid n^2 + 2n + 12$，$n \in \mathbf{Z}$。

注：这个例题的一般形式是：

设 p 是素数，a，b 是整数，则

$$p^k \nmid (an + b)^k + p^{k-1}c，$$

其中 c 是不被 p 整除的任意整数，k 是任意的大于 1 的整数。

例 3　设 a，b 是整数，且

$$9 \mid a^2 + ab + b^2，\tag{4}$$

则 $3 \mid (a, b)$。

例 4　设 a 和 b 是正整数，$b > 2$，则 $2^b - 1 \nmid 2^a + 1$。

四、最小公倍数（40 分钟）

定理 1　下面的等式成立：

（ⅰ）　$[a, 1] = |a|$，$[a, a] = |a|$；

（ⅱ）　$[a, b] = [b, a]$；

(iii) $[a_1, a_2, \cdots, a_k] = [|a_1|, |a_2| \cdots, |a_k|]$；

(iv) 若 $a \mid b$，则$[a, b] = |b|$。

由定理 1 中的结论(iii)可知，在讨论 $a_1, a_2, \cdots, a_k$ 的最小公倍数时，不妨假定它们都是正整数。在本节中总是维持这一假定。

最小公倍数和最大公约数之间有一个很重要的关系，即下面的定理。

定理 2 对任意的正整数 a，b，有

$$[a, b] = \frac{ab}{(a, b)}。$$

推论 1 两个整数的任何公倍数可以被它们的最小公倍数整除。

推论 2 设 m，a，b 是正整数，则$[ma, mb] = m[a, b]$。

定理 3 对于任意的 n 个整数 $a_1, a_2, \cdots, a_n$，记

$$[a_1, a_2] = m_2，\ [m_2, a_3] = m_3，\ \cdots，\ [m_{n-2}, a_{n-1}] = m_{n-1}，\ [m_{n-1}, a_n] = m_n，$$

则

$$[a_1, a_2, \cdots, a_n] = m_n。$$

推论 若 m 是整数 $a_1, a_2, \cdots, a_n$ 的公倍数，则$[a_1, a_2, \cdots, a_n] \mid m$ 。

定理 4 整数 $a_1, a_2, \cdots, a_n$ 两两互素，即

$$(a_i, a_j) = 1，\ 1 \le i, j \le n，\ i \ne j$$

的充要条件是

$$[a_1, a_2, \cdots, a_n] = a_1 a_2 \cdots a_n 。 \tag{3}$$

例 1 设 a，b，c 是正整数，证明：$[a, b, c](ab, bc, ca) = abc$ 。

例 2 对于任意的整数 $a_1, a_2, \cdots, a_n$ 及整数 k，$1 \le k \le n$，证明：

$$[a_1, a_2, \cdots, a_n] = [[a_1, \cdots, a_k],[a_{k+1}, \cdots, a_n]]$$

例 3 设 a，b，c 是正整数，证明：

$$[a, b, c][ab, bc, ca] = [a, b][b, c][c, a]。$$

五、辗转相除法（50 分钟）

引理 1　用下面的方式定义 Fibonacci 数列$\{F_n\}$：

$$F_1 = F_2 = 1，\ F_n = F_{n-1} + F_{n-2}，\ n \geq 3，$$

那么对于任意的整数 $n \geq 3$，有

$$F_n > \alpha^{n-2}, \tag{2}$$

其中$\alpha = \frac{1+\sqrt{5}}{2}$。

定理 1(Lame)　设 $a, b \in \mathbf{N}$，$a > b$，使用在式(1)中的记号，则

$$n < 5\log_{10} b。$$

定理 2　使用式(1)中的记号，记

$$P_0 = 1，\ P_1 = q_1，\ P_k = q_k P_{k-1} + P_{k-2}，\ k \geq 2，$$

$$Q_0 = 0，\ Q_1 = 1，\ Q_k = q_k Q_{k-1} + Q_{k-2}，\ k \geq 2，$$

则

$$aQ_k - bP_k = (-1)^{k-1} r_k，\ k = 1, 2, \cdots, n\ 。 \tag{3}$$

定理 3　使用式(1)中的记号，有 $r_n = (a, b)$。

例 1　设 a 和 b 是正整数，那么只使用被 2 除的除法运算和减法运算就可以计算出(a, b)。

解　下面的四个基本事实给出了证明：

(ⅰ)　若 $a \mid b$，则$(a, b) = a$；

(ⅱ)　若 $a = 2^{\alpha} a_1$，$2 \nmid a_1$，$b = 2^{\beta} b_1$，$2 \nmid b_1$，$\alpha \geq \beta \geq 1$，则

$$(a, b) = 2^{\beta}(2^{\alpha-\beta} a_1, b_1)；$$

(ⅲ)　若 $2 \nmid a$，$b = 2^{\beta} b_1$，$2 \nmid b_1$，则$(a, b) = (a, b_1)$；

(ⅳ) 若$2\nmid a$，$2\nmid b$，则$(a,b)=(|\frac{a-b}{2}|,b)$。

在实际计算过程中，若再灵活运用最大公约数的性质（例如第三节定理 4 的推论），则可使得求最大公约数的过程更为简单。

例 2 用辗转相除法求(125, 17)，以及 x，y，使得

$$125x + 17y = (125, 17)。$$

例 3 求(12345, 678)。

例 4 在 m 个盒子中放若干个硬币，然后以下述方式往这些盒子里继续放硬币：每一次在 n（$n<m$）个盒子中各放一个硬币。证明：若$(m, n) = 1$，那么无论开始时每个盒子中有多少硬币，经过若干次放硬币后，总可使所有盒子含有同样数量的硬币。

六、算术基本定理（50 分钟）

引理 1 任何大于 1 的正整数 n 可以写成素数之积，即

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

其中 p_i（$1 \le i \le m$）是素数。

定理 1(算术基本定理) 任何大于 1 的整数 n 可以唯一地表示成

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{2}$$

其中 $p_1, p_2, \cdots, p_k$ 是素数，$p_1 < p_2 < \cdots < p_k$，$\alpha_1, \alpha_2, \cdots, \alpha_k$ 是正整数。

推论 1 使用式(2)中的记号，有

(ⅰ) n 的正因数 d 必有形式

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}，\ \gamma_i \in \mathbf{Z}，\ 0 \le \gamma_i \le \alpha_i，\ 1 \le i \le k;$$

(ⅱ) n 的正倍数 m 必有形式

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} M，\ M \in \mathbf{N}，\ \beta_i \in \mathbf{N}，\ \beta_i \ge \alpha_i，\ 1 \le i \le k。$$

推论 2　设正整数 a 与 b 的标准分解式是

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\gamma_1} \cdots q_l^{\gamma_l},\ b = p_1^{\beta_1} \cdots p_k^{\beta_k} r_1^{\delta_1} \cdots r_s^{\delta_s},$$

其中 p_i（$1 \le i \le k$），q_i（$1 \le i \le l$）与 r_i（$1 \le i \le s$）是两两不相同的素数，α_i，β_i（$1 \le i \le k$），γ_i（$1 \le i \le l$）与δ_i（$1 \le i \le s$）都是非负整数，则

$$(a, b) = p_1^{\lambda_1} \cdots p_k^{\lambda_k},\quad \lambda_i = \min\{\alpha_i, \delta_i\},\ 1 \le i \le k,$$

$$[a, b] = p_1^{\mu_1} \cdots p_k^{\mu_k} q_1^{\beta_1} \cdots q_l^{\beta_l} r_1^{\gamma_1} \cdots r_s^{\gamma_s},\ \mu_i = \max\{\alpha_i, \delta_i\},\ 1 \le i \le k。$$

为了方便，推论 2 常叙述为下面的形式：

推论 2′　设正整数 a 与 b 的标准分解式是

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ b = p_1^{\beta_1} p_2^{\beta_1} \cdots p_k^{\beta_k},$$

其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，α_i，β_i（$1 \le i \le k$）都是非负整数，则

$$(a,b) = p_1^{\lambda_1} p_2^{\lambda_1} \cdots p_k^{\lambda_k},\quad \lambda_i = \min\{\alpha_i, \beta_i\},\quad 1 \le i \le k,$$
$$[a,b] = p_1^{\mu_1} p_2^{\mu_1} \cdots p_k^{\mu_k},\quad \mu_i = \max\{\alpha_i, \beta_i\},\quad 1 \le i \le k。$$

推论 3　设 a，b，c，n 是正整数，

$$ab = c^n,\ (a, b) = 1, \tag{5}$$

则存在正整数 u，v，使得

$$a = u^n,\ b = v^n,\ c = uv,\ (u, v) = 1。$$

例 1　写出 51480 的标准分解式。

例 2　设 a，b，c 是整数，证明：

（ⅰ）　$(a, b)[a, b] = ab$;

（ⅱ）　$(a, [b, c]) = [(a, b), (a, c)]$。

注：利用定理 1 可以容易地处理许多像例 2 这样的问题。

例 3　证明：$N = 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$（$n \ge 2$）不是整数。

七、函数$[x]$与$\{x\}$（90 分钟）

定理 1　设 x 与 y 是实数，则

(ⅰ)　$x \le y \Longrightarrow [x] \le [y]$；

(ⅱ)　若 m 是整数，则$[m+x] = m + [x]$；

(ⅲ)　若 $0 \le x < 1$，则$[x] = 0$；

(ⅳ)　$[x+y] = \begin{cases} [x]+[y] & \text{若 } \{x\}+\{y\}<1 \\ [x]+[y]+1 & \text{若 } \{x\}+\{y\}\ge 1 \end{cases}$；

(ⅴ)　$[-x] = \begin{cases} -[x] & \text{若 } x \in \mathbf{Z} \\ -[x]-1 & \text{若 } x \notin \mathbf{Z} \end{cases}$；

(ⅵ)　$\{-x\} = \begin{cases} 0 & \text{若 } x \in \mathbf{Z} \\ 1-\{x\} & \text{若 } x \notin \mathbf{Z} \end{cases}$。

定理 2　设 a 与 b 是正整数，则在 1, 2, …, a 中能被 b 整除的整数有$[\frac{a}{b}]$个。

定理 3　设 n 是正整数，$n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 是 $n!$的标准分解式，则

$$\alpha_i = \sum_{r=1}^{\infty} [\frac{n}{p_i^r}]。\tag{1}$$

推论　设 n 是正整数，则

$$n! = \prod_{p \le n} p^{\sum_{r=1}^{\infty}[\frac{n}{p^r}]},$$

其中$\prod_{p\le n}$ 表示对不超过 n 的所有素数 p 求积。

定理 4　设 n 是正整数，$1 \le k \le n-1$，则

$$\mathrm{C}_n^k = \frac{n!}{k!(n-k)!} \in \mathbf{N}。\tag{3}$$

若 n 是素数，则 $n \mid \mathrm{C}_n^k$，$1 \le k \le n-1$。

例 1　求最大的正整数 k，使得 $10^k \mid 199!$。

例 2　设 x 与 y 是实数，则

$$[2x]+[2y]\geq[x]+[x+y]+[y]。\tag{4}$$

例 3　设 n 是正整数，则

$$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+2}]。\tag{7}$$

例 4　设 x 是正数，n 是正整数，则

$$[x]+[x+\frac{1}{n}]+[x+\frac{2}{n}]+\cdots+[x+\frac{n-1}{n}]=[nx]。$$

例 5　求$[(\sqrt{3}+\sqrt{2})^{1992}]$的个位数。

注：一般地，如果 A，$B\in\mathbf{N}$，$A^2>B$，$A-\sqrt{B}<1$，则由

$$(A+\sqrt{B})^k+(A-\sqrt{B})^k=2(A^k+\mathrm{C}_k^2A^{k-2}B+\cdots)$$

可以求出$[(A+\sqrt{B})^k]$。

例 6　设 x 和 y 是正无理数，$\frac{1}{x}+\frac{1}{y}=1$，证明：数列

$$[x],[2x],\cdots,[kx],\cdots\ 与\ [y],[2y],\cdots,[my],\cdots\tag{11}$$

联合构成了整个正整数集合，而且，两个数列中的数互不相同。

八、素数（60 分钟）

我们已经证明了：每个正整数可以表示成素数幂的乘积。这就引出了一个问题：素数是否有无穷多个？如果有无穷多个，那么，作为无穷大量，素数个数具有怎样的性状？这是数论研究中的一个中心课题。本节要对这一问题作初步的研究。

定义 1　对于正实数 x，以$\pi(x)$表示不超过 x 的素数个数。

例如，$\pi(15)=6$，$\pi(10.4)=4$，$\pi(50)=15$。

例 1　写出不超过 100 的所有的素数。

解　将不超过 100 的正整数排列如下：

~~1~~　2　3　~~4~~　5　~~6~~　7　~~8~~　~~9~~　~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~

41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~

~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~

61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~

71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ 79 ~~80~~

~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~

~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

按以下步骤进行：

(ⅰ) 删去 1，剩下的后面的第一个数是 2，2 是素数；

(ⅱ) 删去 2 后面的被 2 整除的数，剩下的 2 后面的第一个数是 3，3 是素数；

(ⅲ) 再删去 3 后面的被 3 整除的数，剩下的 3 后面的第一个数是 5，5 是素数；

(ⅳ) 再删去 5 后面的被 5 整除的数，剩下的 5 后面的第一个数是 7，7 是素数；

……

照以上步骤可以依次得到素数 2, 3, 5, 7, 11, …。

由本章第一部分定理 2 推论可知，不超过 100 的合数必有一个不超过 10 的素约数，因此在删去 7 后面被 7 整除的数以后，就得到了不超过 100 的全部素数。

在例 1 中所使用的寻找素数的方法，称为 Eratosthenes 筛法。它可以用来求出不超过任何固定整数的所有素数。在理论上这是可行的；但在实际应用中，这种列出素数的方法需要大量的计算时间，是不可取的。

定理 1　素数有无限多个。

注 1：形如 $2^{2^n}+1$（n = 0, 1, 2, …）的数称为 Fermat 数。Fermat 曾经猜测它们都是素数。这是错误的，因为尽管 F_0，F_1，F_2，F_3，F_4 都是素数，$F_5 = 2^{2^5}+1 = 641\cdot 6700417$ 却是合数。

注 2：将全体素数按大小顺序排列为

$$p_1 = 2，\ p_2 = 3，\ p_3 = 5，\ p_4，\ \cdots，\ p_n，\ \cdots，$$

那么由第一个证明方法可以看出

$$p_{n+1} \le p_1 p_2 \cdots p_n + 1，\ n \ge 1。$$

定理 2　对于 $n \ge 1$，

(ⅰ)　$\pi(n) \ge \frac{1}{2}\log_2 n$；

(ⅱ)　$p_n \le 2^{2n}$。

注：定理 2 对于无穷大量$\pi(x)$的下界估计是相当粗糙的。下面的定理是已经知道的（由于其证明较繁，故本书中不予证明）。

定理 3(素数定理)　我们有

$$\pi(x) \sim \frac{x}{\log x}，（x \to \infty），$$

此处 log$x$ 是以 e 为底的 x 的对数。

推论　以 p_n 表示第 n 个素数，则

$$p_n \sim n\log n（n \to \infty）。$$

例 2　若 $a > 1$，$a^n - 1$ 是素数，则 $a = 2$，并且 n 是素数。

注：若 n 是素数，则称 $2^n - 1$ 是 Mersenne 数。

例 3　形如 $4n + 3$ 的素数有无限多个。

例 4　设 $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ 是整系数多项式，那么，存在无穷多个正整数 n，使得 $f(n)$是合数。

思考题+讨论

1、将最大公约数的定义、求法和性质与高等代数中多项式的最大公因式的定义、求法和性质作比较，相同点和不同点是什么？

2、根据整数 n 的标准分解式，如何求 n 的正因数个数？举例说明。

作业安排及课后反思

P4 第 2、3、4 题，P9 第 2、3 题，P14 第 1、3 题，P119 第 1、2、5 题，P23 第 1、2、3 题.

课前准备情况及其他相关特殊要求

课前准备了 PPT 电子教案及本课程实施大纲。本课程无其他特殊要求。

参考资料

[1] 潘承桐, 潘承彪. 简明数论. 北京：北京大学出版社，2000. 第一章

[2] 柯召, 孙琦. 数论讲义. 北京：高等教育出版社, 2003. 第一讲

第二章 不定方程

教学日期： 2016.3.16，2016.3.21，2016.3.23，2016.3.28

教学方法：讲授+提问+讨论；板书+PPT

教学重点：本章讨论二元一次不定方程、多元一次不定方程以及一个特殊的多元二次不定方程（勾股数）的解法。本章考虑整系数代数方程（因为不是整系数的方程可以化为整系数方程）的整数解的通式，并且只寻求它的整数解，求非整数解的方法没有涉及。

难点：求二元一次不定方程的整数解的通式；利用二元一次不定方程解多元一次不定方程。

教学内容

一、二元一次不定方程的定义和解法（100 分钟）

设 $a_1, a_2, \cdots, a_n$ 是非零整数，b 是整数，称关于未知数 $x_1, x_2, \cdots, x_n$ 的方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{1}$$

是 n 元一次不定方程。

若存在整数 $x_1^0, x_2^0, \cdots, x_n^0$ 满足方程(1)，则称$(x_1^0, x_2^0, \cdots, x_n^0)$是方程(1)的解，或说 $x_1 = x_1^0$，$x_2 = x_2^0$，$\cdots$，$x_n = x_n^0$ 是方程(1)的解。

定理 1 方程(1)有解的充要条件是

$$(a_1, a_2, \cdots, a_n) \mid b。 \tag{2}$$

定理 2 设 a，b，c 是整数，方程

$$ax + by = c \tag{3}$$

若有解 (x_0, y_0)，则它的一切解具有

$$\begin{cases} x = x_0 + b_1 t \\ y = y_0 - a_1 t \end{cases}, \quad t \in \mathbf{Z} \tag{4}$$

的形式，其中 $a_1 = \dfrac{a}{(a, b)}$，$b_1 = \dfrac{b}{(a, b)}$。

定理 1 和定理 2 说明了解方程(3)的步骤：

(ⅰ) 判断方程是否有解，即 $(a, b) \mid c$ 是否成立；

(ⅱ) 利用辗转相除法求出 x_0，y_0，使得 $ax_0 + by_0 = (a, b)$；

(ⅲ) 写出方程(3)的解 $\begin{cases} x = x_0 c_1 + b_1 t \\ y = y_0 c_1 - a_1 t \end{cases}, t \in \mathbf{Z}$，其中 $(a,b)c_1 = c$，$a_1 = \dfrac{a}{(a, b)}$，

$b_1 = \dfrac{b}{(a, b)}$。

定理 3 设 $a_1, a_2, \cdots, a_n, b$ 是整数，再设 $(a_1, a_2, \cdots, a_{n-1}) = d_{n-1}$，$(a_1, a_2, \cdots, a_n) = d_n$，则$(x_1', x_2', \cdots, x_n')$是方程(1)的解的充分必要条件是存在整数 t，使得$(x_1', x_2', \cdots, x_n', t)$是方程组

$$\begin{cases} a_1 x_1 + a_2 x_2 + \cdots + a_{n-1} x_{n-1} = d_{n-1} t \\ d_{n-1} t + a_n x_n = b \end{cases} \tag{5}$$

的解。

定理 3 说明了求解 n 元一次不定方程的方法：先解方程组(5)中的第二个方程，再解方程组(5)中的第一个方程，于是，解 n 元一次不定方程就化为解 $n-1$ 元一次不定方程。重复这个过程，最终归结为求解二元一次不定方程。由第一章第三节定理 5，记

$(a_1, a_2) = d_2$，$(d_2, a_3) = d_3$，$\cdots$，$(d_{n-2}, a_{n-1}) = d_{n-1}$，$(d_{n-1}$，$a_n) = d_n$，

逐个地解方程

$$d_{n-1} t_{n-1} + a_n x_n = b,$$

$$d_{n-2}t_{n-2} + a_{n-1}x_{n-1} = d_{n-1}t_{n-1},$$

$$\cdots\cdots$$

$$d_2t_2 + a_3x_3 = d_3t_3,$$

$$a_1x_1 + a_2x_2 = d_2t_2,$$

并且消去中间变量 $t_2, t_3, \cdots, t_{n-1}$，就可以得到方程(1)的解。

例 1　求不定方程 $3x + 6y = 15$ 的解。

例 2　求不定方程 $3x + 6y + 12z = 15$ 的解。

例 3　设 a 与 b 是正整数，$(a, b) = 1$，则任何大于 $ab - a - b$ 的整数 n 都可以表示成 $n = ax + by$ 的形式，其中 x 与 y 是非负整数，但是 $n = ab - a - b$ 不能表示成这种形式。

例 4　设 a，b，c 是整数，$(a, b) = 1$，则在直线 $ax + by = c$ 上，任何一个长度大于 $\sqrt{a^2 + b^2}$ 的线段上至少有一个点的坐标都是整数。

例 5　将 $\frac{19}{30}$ 写成三个分数之和，它们的分母分别是 2，3 和 5。

例 6　甲物每斤 5 元，乙物每斤 3 元，丙物每三斤 1 元，现在用 100 元买这三样东西共 100 斤，问各买几斤?

例 7　求不定方程 $x + 2y + 3z = 7$ 的所有正整数解。

二、勾股数（90 分钟）

讨论二次方程

$$x^2 + y^2 = z^2 。 \qquad (1)$$

容易看出，$(x, y, z) = (0, 0, 0)$，$(0, \pm a, \pm a)$以及$(\pm a, 0, \pm a)$都是方程(1)的解。若(x, y, z)是方程(1)的解，则对于任何整数 k，(kx, ky, kz)也是方程(1)的解。此外，若$(x, y) = k$，则 $k \mid z$，$(x, y, z) = k$。因此，我们只需研究方程(1)的满足下

述条件的解：

$$x > 0，\ y > 0，\ z > 0，\ (x, y) = 1。 \tag{2}$$

定理 1　若(x, y, z)是方程(1)的满足条件(2)的解，则下面的结论成立：

(ⅰ)　x 与 y 有不同的奇偶性；

(ⅱ)　x 与 y 中有且仅有一个数被 3 整除；

(iii)　x，y，z 中有且仅有一个数被 5 整除。

引理　不定方程 $xy = z^2$ 的满足条件

$$xy = z^2，\ x > 0，\ y > 0，\ z > 0，\ (x, y) = 1 \tag{6}$$

的一切正整数解，可以写成下面的形式

$$x = a^2，\ y = b^2，\ z = ab，\ (a, b) = 1，\ a > 0，\ b > 0。 \tag{7}$$

定理 2　方程(1)的满足式(2)和 $2 \mid x$ 的一切正整数解具有下面的形式：

$$x = 2ab，\ y = a^2 - b^2，\ z = a^2 + b^2， \tag{8}$$

其中 $a > b > 0$，$(a, b) = 1$，a 与 b 有不同的奇偶性。

推论　单位圆周上座标都是有理数的点（称为有理点），可以写成

$$\left(\pm\frac{2ab}{a^2+b^2}, \pm\frac{a^2-b^2}{a^2+b^2}\right) 或 \left(\pm\frac{a^2-b^2}{a^2+b^2}, \pm\frac{2ab}{a^2+b^2}\right)$$

的形式，其中 a 与 b 是不全为零的整数。

定理 3　不定方程

$$x^4 + y^4 = z^2 \tag{10}$$

没有满足 $xyz \neq 0$ 的整数解。

推论　方程 $x^4 + y^4 = z^4$ 没有满足 $xyz \neq 0$ 的整数解。

定理 3 中使用的证明方法称为无穷递降法。常用于判定方程的可解性。

例　证明方程

$$x^2+y^2=x^2y^2 \tag{18}$$

没有满足 $xy\neq 0$ 的整数解。

三、几个特殊不定方程的解法（90 分钟）

不定方程是一个内容丰富的课题，许多不定方程的解法有其特殊性。本节要介绍几个这样的方程。

1、因数分析法

任何非零整数的因数个数是有限的，因此，可以对不定方程的解在有限范围内用枚举法确定。

例 6　求方程 $x^2y+2x^2-3y-7=0$ 的整数解。

解　原方程即

$$(x^2-3)(y+2)=1。$$

因此

$$\begin{cases}x^2-3=1\\ y+2=1\end{cases}\text{或}\begin{cases}x^2-3=-1\\ y+2=-1\end{cases},$$

解这两个联立方程组，得到所求的解是

$$\begin{cases}x_1=2\\ y_1=-1\end{cases}\text{或}\begin{cases}x_2=-2\\ y_2=-1\end{cases}。$$

例 7　求方程 $x^3+y^3=1072$ 的正整数解。

解　容易看出，对于任何正整数 a，$(x,y)=(1,a)$，$(a,1)$及(a,a)都不是方程的解。所以，只需考虑 $x\geq 2$，$y\geq 2$，$x\neq y$ 的情况。于是

$$x^2-xy+y^2>xy>x+y, \tag{8}$$

$$(x+y)^2>x^2-xy+y^2。 \tag{9}$$

原方程即

$$(x+y)(x^2-xy+y^2)=2^4\cdot 67。$$

由此及式(8)与式(9)得到

$$\begin{cases}x+y=2^4\\x^2-xy+y^2=67\end{cases},$$

解这两个联立方程组，得到所求的解是

$$\begin{cases}x_1=7\\y_1=9\end{cases}\text{或}\begin{cases}x_2=9\\y_2=7\end{cases}。$$

2、不等式分析法

利用量的整数性或不等关系，确定出方程解的范围。

例 8　求方程

$$3x^2+7xy-2x-5y-35=0$$

的正整数解。

解　对于正整数 x，y，由原方程得到

$$y=\frac{-3x^2+2x+35}{7x-5}。\tag{10}$$

因此，若 $x\geq 1$，$y\geq 1$，则应有

$$\begin{cases}x\geq 1\\-3x^2+2x+35\geq 7x-5\end{cases},$$

解这个不等式组，得到 $1\leq x\leq 2$。

分别取 $x=1$ 和 $x=2$，由式(10)得到 $y=17$ 和 $y=3$。所以所求的解是$(x, y)=(1, 17)$，$(2, 3)$。

例 9　求方程 $5(xy+yz+zx)=4xyz$ 的正整数解。

解　原方程即

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{4}{5}。\tag{11}$$

设 $x \le y \le z$，则由

$$\frac{1}{x} < \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \le \frac{3}{x}$$

及式(11)，得到

$$\frac{1}{x} < \frac{4}{5} \le \frac{3}{x}，\ 1 < x < 4，\ x = 2 \text{ 或 } 3。$$

(ⅰ) 若 $x = 2$，则式(11)成为

$$\frac{1}{y} + \frac{1}{z} = \frac{3}{10}。$$

由此及

$$\frac{1}{y} < \frac{1}{y} + \frac{1}{z} \le \frac{2}{y}$$

得到

$$\frac{1}{y} < \frac{3}{10} \le \frac{2}{y}，\ 3 < y < 7，\ y = 4，5 \text{ 或 } 6。$$

将 $x = 2$ 以及 $y = 4$，5 或 6 分别代入式(11)，得到所求的解

$$(x, y, z) = (2, 4, 20)，(2, 5, 10)。$$

(ⅱ) 若 $x = 3$，同样的方法可以推出，方程(11)无解。

综合以上，注意到(11)式对于 x，y，z 的对称性，得到方程的 12 个正整数解

$$(x, y, z) = (2, 4, 20)，(2, 5, 10)，(2, 20, 4)，(2, 10, 5)，$$
$$(4, 2, 20)，(5, 2, 10)，(20, 2, 4)，(10, 2, 5)，$$
$$(20, 4, 2)，(10, 5, 2)，(4, 20, 2)，(5, 10, 2)。$$

课堂思考题+讨论

1、证明取整函数取小函数的第（Ⅴ）条性质。

2、$x^4 + y^4 = z^2$，$x^4 + y^4 = z^4$ 有没有整数解？

作业安排及课后反思

P31 第 1、2、3、4 题，P34 第 1、2 题，P36 第 2、3 题

课前准备情况及其他相关特殊要求

课前准备了 PPT 电子教案及本课程实施大纲。本课程无其他特殊要求。

参考资料

[1] 潘承桐, 潘承彪. 简明数论. 北京：北京大学出版社，2000. 第三章

[2] 柯召, 孙琦. 数论讲义. 北京：高等教育出版社, 2003. 第二讲

第三章 同　余

教学日期：2016.3.30，2016.4.4，2016.4.6，2016.4.11，2016.4.13

教学方法：讲授+提问+讨论；板书+PPT

教学重点：整数同余的概念及同余的基本性质，运用同余的基本性质，会利用同余简单验证整数乘积运算的结果。剩余类、完全剩余系的概念，判断剩余系的方法。Fermat 小定理及应用。

难点：同余理论的应用、求欧拉函数的值、欧拉定理和费马定理及其在循环小数中的运用。

教学内容

一、同余的基本性质（120 分钟）

定义 1　给定正整数 m，如果整数 a 与 b 之差被 m 整除，则称 a 与 b 对于模 m 同余，或称 a 与 b 同余，模 m，记为

$$a \equiv b \pmod{m},$$

此时也称 b 是 a 对模 m 的同余。

如果整数 a 与 b 之差不能被 m 整除，则称 a 与 b 对于模 m 不同余，或称 a 与 b 不同余，模 m，记为 $a \not\equiv b \pmod{m}$。

定理 1　下面的三个叙述是等价的：

(ⅰ)　$a \equiv b \pmod{m}$；

(ⅱ)　存在整数 q，使得 $a = b + qm$；

(ⅲ)　存在整数 q_1，q_2，使得 $a = q_1 m + r$，$b = q_2 m + r$，$0 \le r < m$。

定理 2　同余具有下面的性质：

(ⅰ)　$a \equiv a \pmod{m}$；

(ⅱ)　$a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$；

(ⅲ)　$a \equiv b$，$b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$。

定理 3　设 a，b，c，d 是整数，并且

$$a \equiv b \pmod{m}，\ c \equiv d \pmod{m}，\tag{1}$$

则

(ⅰ)　$a + c \equiv b + d \pmod{m}$；

(ⅱ)　$ac \equiv bd \pmod{m}$。

定理 4　设 a_i，b_i（$0 \le i \le n$）以及 x，y 都是整数，并且

$$x \equiv y \pmod{m}，\ a_i \equiv b_i \pmod{m}，\ 0 \le i \le n，$$

则

$$\sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} b_i y^i \pmod{m}。\tag{2}$$

定理 5　下面的结论成立：

(ⅰ)　$a \equiv b \pmod{m}$，$d \mid m$，$d > 0 \Longrightarrow a \equiv b \pmod{d}$；

(ⅱ)　$a \equiv b \pmod{m}$，$k > 0$，$k \in \mathbf{N} \Longrightarrow ak \equiv bk \pmod{mk}$；

(ⅲ)　$a \equiv b \pmod{m_i}$，$1 \le i \le k \Longrightarrow a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$；

(ⅳ)　$a \equiv b \pmod{m} \Longrightarrow (a, m) = (b, m)$；

(ⅴ)　$ac \equiv bc \pmod{m}$，$(c, m) = 1 \Longrightarrow a \equiv b \pmod{m}$。

例 1　设 $N = \overline{a_n a_{n-1} \cdots a_0}$ 是整数 N 的十进制表示，即

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \ ,$$

则

(ⅰ) $3 \mid N \Leftrightarrow 3 \mid \sum_{i=0}^{n} a_i$；

(ⅱ) $9 \mid N \Leftrightarrow 9 \mid \sum_{i=0}^{n} a_i$；

(ⅲ) $11 \mid N \Leftrightarrow 11 \mid \sum_{i=0}^{n} (-1)^i a_i$；

(ⅳ) $13 \mid N \Leftrightarrow 13 \mid \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$。

注：一般地，在考虑使 $N = \overline{a_{n-1} a_{n-2} \cdots a_1 a_0}$ 被 m 除的余数时，首先是求出正整数 k，使得

$$10^k \equiv -1 \text{ 或 } 1 \pmod{m},$$

再将 $N = \overline{a_{n-1} a_{n-2} \cdots a_1 a_0}$ 写成

$$N = \overline{a_{k-1} a_{k-2} \cdots a_1 a_0} \cdot 10^0 + \overline{a_{2k-1} a_{2h-2} \cdots a_k} \cdot 10^k + \cdots$$

的形式，再利用式(2)。

例 2　求 $N = \overline{a_{n-1} a_{n-2} \cdots a_1 a_0}$ 被 7 整除的条件，并说明 1123456789 能否被 7 整除。

例 3　说明 $2^{2^5} + 1$ 是否被 641 整除。

注：一般地，计算 $a^b \pmod{m}$ 常是一件比较繁复的工作。但是，如果利用 Euler 定理或 Fermat 定理（见第四节）就可以适当简化。

例 4　求 $(257^{33} + 46)^{26}$ 被 50 除的余数。

例 5　求 $n = 7^{7^7}$ 的个位数。

注：一般地，若求 a^{b^c} 对模 m 的同余，可分以下步骤进行：

(ⅰ) 求出整数 k，使 $a^k \equiv 1 \pmod{m}$；

(ⅱ) 求出正整数 r，$r < k$，使得 $b^c \equiv r \pmod{k}$；

(ⅲ) $a^{b^c} \equiv a^r \pmod{m}$。

例 6　证明：若 n 是正整数，则 $13 \mid 4^{2n+1} + 3^{n+2}$。

例 7　证明：若 $2 \nmid a$，n 是正整数，则

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}。\tag{4}$$

例 8　设 p 是素数，a 是整数，则由 $a^2 \equiv 1 \pmod{p}$可以推出

$$a \equiv 1 \text{ 或 } a \equiv -1 \pmod{p}。$$

例 9　设 n 的十进制表示是$\overline{13xy45z}$，若 $792 \mid n$，求 x，y，z。

二、完全剩余系（100 分钟）

定理 1　整数集合 A 是模 m 的完全剩余系的充要条件是

(ⅰ)　A 中含有 m 个整数；

(ⅱ)　A 中任何两个整数对模 m 不同余。

定理 2　设 $m \geq 1$，a，b 是整数，$(a, m) = 1$，$\{x_1, x_2, \cdots, x_m\}$是模 m 的一个完全剩余系，则$\{ax_1 + b, ax_2 + b, \cdots, ax_m + b\}$也是模 m 的一个完全剩余系。

定理 3　设 $m_1, m_2 \in \mathbf{N}$，$A \in \mathbf{Z}$，$(A, m_1) = 1$，又设

$$X = \{x_1, x_2, \cdots, x_{m_1}\},\quad Y = \{y_1, y_2, \cdots, y_{m_2}\},$$

分别是模 m_1 与模 m_2 的完全剩余系，则

$$R = \{\, Ax + m_1 y;\ x \in X,\ y \in Y \,\}$$

是模 $m_1 m_2$ 的一个完全剩余系。

推论　若 $m_1, m_2 \in \mathbf{N}$，$(m_1, m_2) = 1$，则当 x_1 与 x_2 分别通过模 m_1 与模 m_2 的完全剩余系时，$m_2 x_1 + m_1 x_2$ 通过模 $m_1 m_2$ 的完全剩余系。

定理 4　设 $m_i \in \mathbf{N}$（$1 \leq i \leq n$），则当 x_i 通过模 m_i（$1 \leq i \leq n$）的完全剩余系时，

$$x = x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_{n-1} x_n$$

通过模 $m_1 m_2 \cdots m_n$ 的完全剩余系。

定理 5　设 $m_i \in \mathbf{N}$，$A_i \in \mathbf{Z}$（$1 \le i \le n$），并且满足下面的条件：

（ⅰ）　$(m_i, m_j) = 1$，$1 \le i, j \le n$，$i \ne j$；

（ⅱ）　$(A_i, m_i) = 1$，$1 \le i \le n$；

（ⅲ）　$m_i \mid A_j$ ，$1 \le i, j \le n$，$i \ne j$ 。

则当 x_i（$1 \le i \le n$）通过模 m_i 的完全剩余系 X_i 时，

$$y = A_1x_1 + A_2x_2 + \cdots + A_nx_n$$

通过模 $m_1m_2\cdots m_n$ 的完全剩余系。

例 1　设 $A = \{x_1, x_2, \cdots, x_m\}$是模 m 的一个完全剩余系，以$\{x\}$表示 x 的小数部分，证明：若$(a, m) = 1$，则

$$\sum_{i=1}^{m}\{\frac{ax_i + b}{m}\} = \frac{1}{2}(m-1)。$$

例 2　设 $p \ge 5$ 是素数，$a \in \{ 2, 3, \cdots, p-2 \}$，则在数列

$$a，2a，3a，\cdots，(p-1)a，pa \tag{4}$$

中有且仅有一个数 b，满足

$$b \equiv 1 \pmod{p}。 \tag{5}$$

此外，若 $b = ka$，则 $k \ne a$，$k \in \{2, 3, \cdots, p-2\}$。

例 3(Wilson 定理)　设 p 是素数，则

$$(p-1)! \equiv -1 \pmod{p}。$$

例 4　设 $m > 0$ 是偶数，$\{a_1, a_2, \cdots, a_m\}$与$\{b_1, b_2, \cdots, b_m\}$都是模 m 的完全剩余系，证明：$\{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$不是模 m 的完全剩余系。

三、简化剩余系（100 分钟）

定理 1　整数集合 A 是模 m 的简化剩余系的充要条件是

（ⅰ）　A 中含有$\varphi(m)$个整数；

(ⅱ) A 中的任何两个整数对模 m 不同余；

(ⅲ) A 中的每个整数都与 m 互素。

定理 2 设 a 是整数，$(a, m) = 1$，$B = \{x_1, x_2, \cdots, x_{\varphi(m)}\}$是模 m 的简化剩余系，则集合 $A = \{ax_1, ax_2, \cdots, ax_{\varphi(m)}\}$也是模 m 的简化剩余系。

注：在定理 2 的条件下，若 b 是整数，集合

$$\{ax_1 + b, ax_2 + b,, \cdots, ax_{\varphi(m)} + b\}$$

不一定是模 m 的简化剩余系。例如，取 $m = 4$，$a = 1$，$b = 1$，以及模 4 的简化剩余系{1, 3}。

定理 3 设 $m_1, m_2 \in \mathbf{N}$，$(m_1, m_2) = 1$，又设

$$X = \{x_1, x_2, \cdots, x_{\varphi(m_1)}\} \text{ 与 } Y = \{y_1, y_2, \cdots, y_{\varphi(m_2)}\}$$

分别是模 m_1 与 m_2 的简化剩余系，则

$$A = \{ m_1y + m_2x；\ x \in X，\ y \in Y \}$$

是模 m_1m_2 的简化剩余系。

定理 4 设 $m, n \in \mathbf{N}$，$(m, n) = 1$，则$\varphi(mn) = \varphi(m)\varphi(n)$。

证明 这是定理 3 的直接推论。证毕。

定理 5 设 n 是正整数，$p_1, p_2, \cdots, p_k$ 是它的全部素因数，则

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\cdots(1 - \frac{1}{p_k}) = n\prod_{p|n}(1 - \frac{1}{p})。$$

由定理 5 可知，$\varphi(n) = 1$ 的充要条件是 $n = 1$ 或 2。

例 1 设整数 $n \geq 2$，证明：

$$\sum_{\substack{1 \leq i \leq n \\ (i,n)=1}} i = \frac{1}{2}n\varphi(n),$$

即在数列 1, 2, ⋯, n 中，与 n 互素的整数之和是$\frac{1}{2}n\varphi(n)$。

例 2 设 n 是正整数，则

$$\sum_{d|n}\varphi(d)=n,$$

此处$\sum_{d|n}$是对 n 的所有正约数求和。

例 3　设 $n\in\mathbf{N}$，证明：

(ⅰ)　若 n 是奇数，则$\varphi(4n)=2\varphi(n)$;

(ⅱ)　$\varphi(n)=\frac{1}{2}n$的充要条件是 $n=2^k$，$k\in\mathbf{N}$;

(ⅲ)　$\varphi(n)=\frac{1}{3}n$的充要条件是 $n=2^k3^l$，$k, l\in\mathbf{N}$;

(ⅳ)　若 $6\mid n$，则$\varphi(n)\le\frac{1}{3}n$;

(ⅴ)　若 $n-1$ 与 $n+1$ 都是素数，$n>4$，则$\varphi(n)\le\frac{1}{3}n$。

例 4 证明：若 $m, n\in\mathbf{N}$，则$\varphi(mn)=(m, n)\varphi([m, n])$;

四、Euler 定理（100 分钟）

定理 1(Euler)　设 m 是正整数，$(a, m)=1$，则

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m)。$$

定理 2(Fermat)　设 p 是素数，则对于任意的整数 a，有

$$a^{p}\equiv a\ (\mathrm{mod}\ p)。$$

例 1　设 n 是正整数，则 $5\nmid 1^n+2^n+3^n+4^n$ 的充要条件是 $4\mid n$。

例 2　设$\{x_1, x_2, \cdots, x_{\varphi(m)}\}$是模 m 的简化剩余系，则

$$(x_1x_2\cdots x_{\varphi(m)})^2\equiv 1\ (\mathrm{mod}\ m)。$$

例 3　设$(a, m)=1$，d_0 是使

$$a^{d}\equiv 1\ (\mathrm{mod}\ m)$$

成立的最小正整数，则

(ⅰ)　$d_0\mid\varphi(m)$;

(ⅱ)　对于任意的 i，j，$0\le i, j\le d_0-1$，$i\ne j$，有

$$a^i \not\equiv a^j \pmod{m}。\tag{3}$$

例 4　设 a，b，c，m 是正整数，$m > 1$，$(b, m) = 1$，并且

$$b^a \equiv 1 \pmod{m}，\ b^c \equiv 1 \pmod{m}，\tag{4}$$

记 $d = (a, c)$，则 $b^d \equiv 1 \pmod{m}$。

例 5　设 p 是素数，$p \mid b^n - 1$，$n \in \mathbf{N}$，则下面的两个结论中至少有一个成立：

(ⅰ)　$p \mid b^d - 1$ 对于 n 的某个因数 $d < n$ 成立；

(ⅱ)　$p \equiv 1 \pmod{n}$。

若 $2 \nmid n$，$p > 2$，则(ⅱ)中的 mod n 可以改为 mod $2n$。

注：例 5 提供了一个求素因数的方法，就是说，整数 $b^n - 1$ 的素因数 p，是 $b^d - 1$（当 $d \mid n$ 时）的素因数，或者是形如 $kn + 1$ 的数（当 $2 \nmid n$，$p > 2$ 时，是形如 $2kn + 1$ 的数)。

例 6　将 $2^{11} - 1 = 2047$ 分解因数。

例 7　将 $2^{35} - 1 = 34359738367$ 分解因数。

例 8　设 n 是正整数，记 $F_n = 2^{2^n} + 1$，则 $2^{F_n} \equiv 2 \pmod{F_n}$。

注 1：我们已经知道，F_5 是合数，因此，例 8 说明，一般地，Fermat 定理的逆定理不成立。即若有整数 a，$(a, n) = 1$，使得

$$a^{n-1} \equiv 1 \pmod{n},\tag{6}$$

并不能保证 n 是素数。习题 3 说明，即使所有的与 n 互素的整数都满足式(6)，也不能保证 n 是素数。

注 2：设 n 是合数，若存在整数 a，$(a, n) = 1$，使得式(6)成立，则称 n 是关于基数 a 的伪素数。

例 9 对于任意的正整数 $a \geq 3$，存在无穷多个关于基数 a 的伪素数。

课堂练习

1、证明 P49 定理 2 的性质庚和壬。

2、（i）证明整数 $-H,\ldots -1,-0,1,\ldots,H(H=\frac{3^{n+1}-1}{3-1})$ 中每一个整数有而且只有一种方法表示成 $3^n x_n+3^{n-1}x_{n-1}+\ldots 3x+x_0\ldots\ldots\ldots\ldots$ ❶ 的形状，其中 $x_i=-1,0,1(i=0,1,\ldots n)$；反之，❶中每一数都 $\geq -H$ 且 $\leq H$。

（ii）说明应用 $n+1$ 个特别的砝码，在天平上可以量出 1 到 H 中的任意一个斤数。

作业安排及课后反思

P53 第 2、3、4、5、6 题，P57 第 1、2 题，P60 第 3、4 题，P64 第 1、2 题

课前准备情况及其他相关特殊要求

课前准备了 PPT 电子教案及本课程实施大纲。本课程无其他特殊要求。

参考资料

[1] 潘承桐，潘承彪. 简明数论. 北京：北京大学出版社，2000. 第二章

[2] 柯召，孙琦. 数论讲义. 北京：高等教育出版社, 2003. 第三讲

第四章 同余式

教学日期：2016.4.18，2016.4.20，2016.4.25，2016.4.27

教学方法：讲授+提问+讨论；板书+PPT

教学重点：同余式的定义和通用解法，中国剩余定理（孙子定理）的内容及证明，掌握中国剩余定理的简单应用，掌握求解简单同余式方程组的方法。高次同余式组的解法。

难点：高次同余式组的解法。

教学内容

一、同余式的基本概念（90 分钟）

定义 1 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是整系数多项式，称

$$f(x)\equiv 0 \pmod m \tag{1}$$

是关于未知数 x 的模 m 的同余方程，简称为模 m 的同余方程。

若 $a_n\not\equiv 0 \pmod m$，则称为 n 次同余方程。

定义 2 设 x_0 是整数，当 $x=x_0$ 时式(1)成立，则称 x_0 是同余方程(1)的解。凡对于模 m 同余的解，被视为同一个解。同余方程(1)的解数是指它的关于模 m 互不同余的所有解的个数，也即在模 m 的一个完全剩余系中的解的个数。

由定义 2，同余方程(1)的解数不超过 m。

定理 1 下面的结论成立：

(ⅰ) 设 $b(x)$是整系数多项式，则同余方程(1)与

$$f(x) + b(x) \equiv b(x) \pmod{m}$$

等价；

(ⅱ) 设 b 是整数，$(b, m) = 1$，则同余方程(1)与

$$bf(x) \equiv 0 \pmod{m}$$

等价；

(ⅲ) 设 m 是素数，$f(x) = g(x)h(x)$，$g(x)$与 $h(x)$都是整系数多项式，又设 x_0 是同余方程(1)的解，则 x_0 必是同余方程

$$g(x) \equiv 0 \pmod{m} \text{ 或 } h(x) \equiv 0 \pmod{m}$$

的解。

下面，我们来研究一次同余方程的解。

定理 2 设 a，b 是整数，$a \not\equiv 0 \pmod{m}$。则同余方程

$$ax \equiv b \pmod{m} \tag{2}$$

有解的充要条件是$(a, m) \mid b$。若有解，则恰有 $d = (a, m)$个解。

在定理的证明中，同时给出了解方程(2)的方法，但是，对于具体的方程(2)，常常可采用不同的方法去解。

例 1 设$(a, m) = 1$，又设存在整数 y，使得 $a \mid b + ym$，则

$$x \equiv \frac{b + ym}{a} \pmod{m}$$

是方程(2)的解。

注：例 1 说明，求方程(2)的解可以转化为求方程

$$my \equiv -b \pmod{a} \tag{5}$$

的解，这有两个便利之处：第一，将一个对于大模 m 的同余方程转化为一个对于小模 a 的同余方程，因此有可能通过对模 a 的完全剩余系进行逐个

验证，以求出方程(5)和(2)的解；第二，设 $m \equiv r \pmod{a}$，$r < a$，则又可继续转化成一个对于更小的模 r 的同余方程。

例 2　解同余方程

$$325x \equiv 20 \pmod{161} \tag{6}$$

例 3　设 $a > 0$，且$(a, m) = 1$，a_1 是 m 对模 a 的最小非负剩余，则同余方程

$$a_1 x \equiv -b[\frac{m}{a}] \pmod{m} \tag{7}$$

等价于同余方程(2)。

注：用本例的方法，可以将同余方程(2)转化成未知数的系数更小一些的同余方程，从而易于求解。

例 4　解同余方程 $6x \equiv 7 \pmod{23}$。

例 5　设$(a, m) = 1$，并且有整数$\delta > 0$ 使得

$$a^{\delta} \equiv 1 \pmod{m},$$

则同余方程(2)的解是

$$x \equiv ba^{\delta - 1} \pmod{m}。$$

注：由例 5 及 Euler 定理可知，若$(a, m) = 1$，则

$$x \equiv ba^{\varphi(m) - 1} \pmod{m}$$

总是同余方程(2)的解。

例 6　解同余方程

$$81x^3 + 24x^2 + 5x + 23 \equiv 0 \pmod{7}。$$

注：本例使用的是最基本的解同余方程的方法，一般说来，它的计算量太大，不实用。

例 7　解同余方程组

$$\begin{cases} 3x+5y \equiv 1 (\mathrm{mod}\, 7) \\ 2x-3y \equiv 2 (\mathrm{mod}\, 7) \end{cases}。 \tag{8}$$

例 8　设 a_1，a_2 是整数，m_1，m_2 是正整数，证明：同余方程组

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \end{cases} \tag{9}$$

有解的充要条件是

$$a_1 \equiv a_2 \ (\mathrm{mod}\ (m_1, m_2))。 \tag{10}$$

若有解，则对模$[m_1, m_2]$是唯一的，即若 x_1 与 x_2 都是同余方程组(9)的解，则

$$x_1 \equiv x_2 \ (\mathrm{mod}\ [m_1, m_2])。 \tag{11}$$

二、孙子定理（80 分钟）

本节要讨论同余方程组

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \quad \cdots\cdots \\ x \equiv a_k (\mathrm{mod}\, m_k) \end{cases}。 \tag{1}$$

在第一节的例题中，我们已讨论了 $k = 2$ 的情形。下面考察一般情形。

定理 1 (孙子定理)　设 $m_1, m_2, \cdots, m_k$ 是正整数，

$$(m_i, m_j) = 1，\ 1 \le i, j \le k，\ i \ne j。 \tag{2}$$

记

$$m = m_1 m_2 \cdots m_k \ ，\ M_i = \frac{m}{m_i} ，\ 1 \le i \le k,$$

则存在整数 M_i'（$1 \le i \le k$），使得

$$M_i M_i' \equiv 1 \ (\mathrm{mod}\ m_i), \tag{3}$$

$$M_i M_i' \equiv 0 \ (\mathrm{mod}\ m_i)，\ 1 \le j \le k，\ i \ne j, \tag{4}$$

并且

$$x_0 \equiv \sum_{i=1}^{k} a_i M_i M_i' \pmod{m} \tag{5}$$

是同余方程组(1)对模 m 的唯一解，即若有 x 使方程组(1)成立，则

$$x \equiv x_0 \pmod{m}。 \tag{6}$$

定理 2　在定理 1 的条件下，若式(1)中的 $a_1, a_2, \cdots, a_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系，则式(5)中的 x_0 通过模 $m_1 m_2 \cdots m_k$ 的完全剩余系。

定理 3　同余方程组(1)有解的充要条件是

$$a_i \equiv a_j \pmod{(m_i, m_j)}，\ 1 \le i, j \le n。 \tag{7}$$

定理 4　设 $m = m_1 m_2 \cdots m_k$ ，其中 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，$f(x)$是整系数多项式，以 T 与 T_i（$1 \le i \le k$）分别表示同余方程

$$f(x) \equiv 0 \pmod{m} \tag{10}$$

与

$$f(x) \equiv 0 \pmod{m_i} \tag{11}$$

的解的个数，则 $T = T_1 T_2 \cdots T_k$ 。

由定理 4 及算术基本定理，解一般模的同余方程可以转化为解模为素数幂的同余方程。

例 1　求整数 n，它被 3，5，7 除的余数分别是 1，2，3。

例 2　解同余方程

$$5x^2 + 6x + 49 \equiv 0 \pmod{60}。 \tag{15}$$

三、模 p^{α} 的同余方程（90 分钟）

容易看出，若 x_0 是同余方程

$$f(x) \equiv 0 \pmod{p^{\alpha}} \tag{1}$$

的解，则它必是方程

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \tag{2}$$

的解，因此，必有与 x_0 相应的方程(2)的某个解 x_1，使

$$x_0 \equiv x_1 \pmod{p^{\alpha-1}}，\ x_0 = x_1 + p^{\alpha-1}t_0，$$

此处，t_0 是某个适当的整数。

这提示我们：可以从方程(2)的解中去求方程(1)的解。于是，现在的问题是，对于方程(2)的每个解 x_1，是否必有方程(1)的解 x_0 与之对应？若有，如何去确定它？

定理　设 p 是素数，$\alpha \geq 2$ 是整数，$f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是整系数多项式，又设 x_1 是同余方程(2)的一个解。以 $f'(x)$表示 $f(x)$的导函数。

(ⅰ)　若 $f'(x_1) \not\equiv 0 \pmod{p}$，则存在整数 t，使得

$$x = x_1 + p^{\alpha-1}t \tag{3}$$

是同余方程(1)的解。

(ⅱ)　若 $f'(x_1) \equiv 0 \pmod{p}$，并且 $f(x_1) \equiv 0 \pmod{p^{\alpha}}$，则对于 $t = 0$，1, 2, …, $p - 1$，式(3)中的 x 都是方程(1)的解。

推论　使用定理的记号，

(ⅰ)　若 $x \equiv a \pmod{p}$是同余方程(6)的解，并且 $f'(a) \not\equiv 0 \pmod{p}$，则存在 x_α，$x_\alpha \equiv a \pmod{p}$，使得 $x \equiv x_\alpha \pmod{p^{\alpha}}$是同余方程(1)的解。

(ⅱ)　若 $f'(x) \equiv 0 \pmod{p}$与同余方程(6)没有公共解，则对于任意的整数 $\alpha \geq 1$，同余方程(1)与(6)的解数相同。

例 1　解同余方程

$$x^3 + 3x - 14 \equiv 0 \pmod{45}。$$

例 2　解同余方程

$$2x^2 + 13x - 34 \equiv 0 \pmod{5^3}。\tag{11}$$

例 3　解同余方程

$$x^2 \equiv 1 \pmod{2^k}，\ k \in \mathbf{N}。\tag{17}$$

例 4　解同余方程 $x^2 \equiv 2 \pmod{7^3}$。

注：例 4 中的方法是利用数的 b 进制表示，这一方法可以处理模 b^k 的同余方程，而不必要求 b 是素数。

四、素数模的同余方程（90 分钟）

以下，设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是整系数多项式，p 是素数，$p \nmid a_n$。

定理 1　设 $k \le n$，若同余方程

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}\tag{1}$$

有 k 个不同的解 $x_1, x_1, \cdots, x_k$，则对于任意的整数 x，有

$$f(x) \equiv (x - x_1)(x - x_2)\cdots(x - x_k) f_k(x) \pmod{p},$$

其中 $f_k(x)$是一个次数为 $n - k$ 的整系数多项式，并且它的 x^{n-k} 项的系数是 a_n。

推论　若 p 是素数，则对于任何整数 x，有

$$x^{p-1} - 1 \equiv (x - 1)(x - 2)\cdots(x - p + 1) \pmod{p}。$$

定理 2　同余方程(1)的解数$\le n$。

推论　若同余方程 $b_n x^n + \cdots + b_0 \equiv 0 \pmod{p}$的解数大于 n，则

$$p \mid b_i，\ 0 \le i \le n。\tag{7}$$

定理 3　同余方程(1)或者有 p 个解，或者存在次数不超过 $p - 1$ 的整系数多项式 $r(x)$，使得同余方程(1)与 $r(x) \equiv 0 \pmod{p}$等价。

定理 4　设 $n \le p$，则同余方程

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \equiv 0 \pmod{p} \qquad (10)$$

有 n 个解的充要条件是存在整数多项式 $q(x)$和 $r(x)$，$r(x)$的次数< n，使得

$$x^p - x = f(x)q(x) + p \cdot r(x)。 \qquad (11)$$

注：若 $p \nmid a_n$，由辗转相除法可求出 a_n'，$p \nmid a_n'$使得 $a_n a_n' \equiv 1 \pmod{p}$，于是，同余方程(1)与同余方程

$$a_n' f(x) = x^n + a_n' a_{n-1}x^{n-1} + \cdots + a_n' a_1 x + a_n' a_0 \pmod{p}$$

等价。因此，定理 4 是有普遍性的。

定理 5　若 p 是素数，$n \mid p-1$，$p \nmid a$ 则

$$x^n \equiv a \pmod{p} \qquad (14)$$

有解的充要条件是

$$a^{\frac{p-1}{n}} \equiv 1 \pmod{p}。 \qquad (15)$$

若有解，则解数为 n。

例 1　判定同余方程 $2x^3 + 3x + 1 \equiv 0 \pmod{7}$是否有三个解。

例 2　解同余方程

$$3x^{14} + 4x^{10} + 6x - 18 \equiv 0 \pmod{5}。$$

思考题+讨论（10 分钟）

判定

(ⅰ)　$2x3 - x2 + 3x - 1 \equiv 0 \pmod{5}$是否有三个解？

(ⅱ)　$x6 + 2x5 - 4x2 + 3 \equiv 0 \pmod{5}$是否有六个解？

作业安排及课后反思

P75 习题 1、2、3、4 题，P79 第 1、2 题，P87 第 1、2 题

课前准备情况及其他相关特殊要求

课前准备了 PPT 电子教案及本课程实施大纲。本课程无其他特殊要求。

参考资料

[1] 潘承桐, 潘承彪. 简明数论. 北京：北京大学出版社，2000. 第四章

[2] 柯召, 孙琦. 数论讲义. 北京：高等教育出版社, 2003. 第四章

第五章 连分数

教学日期：2016.5.2，2016.5.4，2016.5.9，2016.5.11

教学方法：讲授+提问+讨论；板书+PPT

教学重点：连分数、有限、无限连分数的概念，理解它们之间的关系；连分数、渐近分数及其之间的递推关系式，有限、无限连分数与有理数、无理数之间的关系。

难点：连分数、渐近分数之间的递推关系式，有限、无限连分数与有理数、无理数之间的关系。

教学内容

一、连分数的定义及基本性质（120 分钟）

定义 1 设$\alpha_1, \alpha_2, \cdots, \alpha_n$是不为零的实数，当分数

$$\alpha_1+\cfrac{1}{\alpha_2+\cfrac{1}{\alpha_3+\cfrac{1}{\ddots+\cfrac{1}{\alpha_n}}}}$$

有意义时，称为有限连分数，简记为$\alpha_1+\cfrac{1}{\alpha_2+}\cfrac{1}{\alpha_3+}\cdots\cfrac{1}{+\alpha_n}$，或$\langle \alpha_1, \alpha_2, \cdots, \alpha_n \rangle$。

定义 2 设$\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots$ 是不为零的无限的实数列，记$\frac{p_n}{q_n}=\langle \alpha_1, \alpha_2, \cdots, \alpha_n \rangle$。若$\frac{p_n}{q_n}$（$n \geq 1$）都有意义并且$\lim\limits_{n\to\infty}\frac{p_n}{q_n}=A\neq\infty$，则称$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$是无限连分数，并称连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$等于 A，或称它的值是 A。也称它是 A 的连分数，或者称它表示 A，记为

$$A=\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle=\alpha_1+\cfrac{1}{\alpha_2+}\cfrac{1}{\alpha_3+}\cdots\cfrac{1}{+\alpha_n+}\cdots。$$

称 $\frac{p_n}{q_n}$（$n \geq 1$）是连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$的第 n 个渐近分数。

定理 1　连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$的第 k 个渐近分数为 $\frac{p_k}{q_k}$，则

$$\begin{array}{lll} p_1 = \alpha_1, & p_2 = \alpha_2\alpha_1 + 1, & p_k = \alpha_k p_{k-1} + p_{k-2}, \quad (k \geq 3) \\ q_1 = 1, & q_2 = \alpha_2, & q_k = \alpha_k q_{k-1} + q_{k-2}, \quad (k \geq 3) \end{array} \tag{1}$$

推论　在定理 1 中，若$\alpha_i \geq 1$（$i \geq 1$），则 $q_n \geq n - 1$（$n \geq 2$）。

定理 2　设 $\frac{p_k}{q_k}$ 是连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$的渐近分数，则

（ⅰ）　$p_k q_{k-1} - p_{k-1} q_k = (-1)^k$，（$k \geq 2$）；

（ⅱ）　$p_k q_{k-2} - p_{k-2} q_k = (-1)^{k-1} \alpha_k$，（$k \geq 3$）；

定义 3　设 a_1 是整数，$a_2, a_3, \cdots, a_n, \cdots$ 是正整数，则称连分数

$$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$$

是简单连分数。

以后，在本章中，除特别声明外，在谈到连分数时，都是指简单连分数。

定理 3　设$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$是简单连分数，$\frac{p_k}{q_k}$（$k \geq 1$）是它的渐近分数，则

（ⅰ）　$\frac{p_{2(k-1)}}{q_{2(k-1)}} > \frac{p_{2k}}{q_{2k}}$，$\frac{p_{2k-1}}{q_{2k-1}} > \frac{p_{2k-3}}{q_{2k-3}}$，$\frac{p_{2k}}{q_{2k}} > \frac{p_{2k-1}}{q_{2k-1}}$；

（ⅱ）　对任意的正整数 k，p_k 与 q_k 互素。

定理 4　任何简单连分数都表示一个实数。

例 1　设 a 与 b 是正整数，$b > 1$，$\langle a_1, a_2, \cdots, a_n \rangle$是 $\frac{a}{b}$ 的有限简单连分数，证明

$$aq_{n-1} - bp_{n-1} = (-1)^n (a, b),$$

其中(a, b)是 a 与 b 的最大公约数。

注：例 1 给出了求不定方程 $ax + by = c$ 的特解的一个方法。

例 2　求不定方程

$$13x + 17y = 5 \tag{4}$$

的解。

例 3　设$\frac{p_n}{q_n}$是$\langle a_1, a_2, \cdots, a_n, \cdots \rangle$的第 n 个渐近分数，则

$$\frac{q_n}{q_{n-1}} = \langle a_n, a_{n-1}, \cdots, a_2 \rangle \quad (n \geq 2)。 \tag{5}$$

例 4　求连分数$\langle 0, 1, 2, 1, 2, \cdots \rangle$的值。

二、实数的连分数表示（120 分钟）

定理 1　任一有理数α可以表示成有限简单连分数。

定理 2　任一无理数可以表示成无限简单连分数。

推论　设α是实无理数，那么，对于任意的正整数 n，存在δ_n与η_n，$0 < \delta_n, \eta_n < 1$，使得

$$\alpha = \frac{p_n}{q_n} + \frac{(-1)^{n-1}\delta_n}{q_n q_{n+1}} = \frac{p_n}{q_n} + \frac{(-1)^{n-1}\eta_n}{{q_n}^2}。$$

定理 3　无理数的连分数表示是唯一的。

定理 4　设 a 与 b 是整数，$\langle a_1, a_2, \cdots, a_n \rangle$与$\langle b_1, b_2, \cdots, b_m \rangle$是$\frac{a}{b}$的两个简单连分数表示，

(ⅰ)　若 $a_n > 1$，$b_m > 1$，则 $n = m$，$a_i = b_i$（$1 \leq i \leq n$）；

(ⅱ)　若 a_n 是大于 1 的整数，则有理数$\frac{a}{b}$仅有两种表示成简单连分数的方法，即$\langle a_1, a_2, \cdots, a_n \rangle = \langle a_1, a_2, \cdots, a_n - 1, 1 \rangle$。

定理 5　设$\frac{p_n}{q_n}$（$n = 1, 2, \cdots$）是实数α的连分数的渐近分数，则对于任意的正整数 $q \leq q_n$ 及整数 p，有

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{p}{q}\right| 。 \tag{6}$$

定理 5 说明，在分母不超过 q_n 的分数中，$\frac{p_n}{q_n}$ 是α的最佳有理逼近。这是渐近分数的一个非常重要的性质。

定理 6(Hurwitz)　设α是无理数，那么，在它的连分数的任何两个相邻渐近分数中，至少有一个满足不等式

$$|\alpha-\frac{p}{q}|<\frac{1}{2q^2}。\tag{8}$$

推论　对于任意的无理数α，存在无穷多个有理数$\frac{p}{q}$满足

$$|\alpha-\frac{p}{q}|<\frac{1}{2q^2}。$$

例 1　写出$\sqrt{8}$的连分数

例 2　求$\sqrt{8}$的误差不超过10^{-4}的有理近似值。

三、循环连分数（120 分钟）

定义 1　设$\langle a_1, a_2, \cdots, a_n, \cdots\rangle$是无限简单连分数。如果存在正整数 s 与 t，使得

$$a_{s+i}=a_{s+kt+i},\ \ i=1, 2, \cdots, t;\ \ k=0, 1, 2, \cdots,$$

则称$\langle a_1, a_2, \cdots, a_n, \cdots\rangle$是循环连分数,并记为

$$\langle a_1, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t}\rangle。$$

如果 $s=0$，则称它是纯循环连分数。

定理 1　任何循环连分数表示一个不可约整系数二次方程的实根。

定理 2　设$\alpha=\langle \dot{a}_1, \cdots, \dot{a}_t\rangle$是纯循环连分数，则它所满足的二次方程的另一个根在–1 与 0 之间。

定理 3　设α是二次不可约整系数方程

$$Ax^2+Bx+C=0\tag{3}$$

的实根，则α的简单连分数是循环连分数。

例 1　设 a，b，c 是正整数，$b = ac$，求连分数

$$x = b + \frac{1}{a + b + \frac{1}{a + \cdots}} = \langle \dot{b}, \dot{a} \rangle$$

的值。

例 2　求 $\alpha = \langle \dot{1}, 2, \dot{3} \rangle$ 之值。

作业安排及课后反思

P153 习题 1、2 题，P159 第 1、2 题，P87 第 1、2 题

课前准备情况及其他相关特殊要求

课前准备了 PPT 电子教案及本课程实施大纲。本课程无其他特殊要求。

参考资料

[1] 潘承桐, 潘承彪. 简明数论. 北京：北京大学出版社，2000. 第七章

[2] 柯召, 孙琦. 数论讲义. 北京：高等教育出版社, 2003. 第六讲

课程要求

1、学生自学要求

学生应在上课前对即将学习的章节进行预习，需要学生课堂演讲的内容应倒背如流，保证课堂演讲脱稿进行。已学章节的复习由学生在课余自行安排时间，课堂上不安排复习。除了教材上的内容外，要求学生阅读一些相关著作，如下述课外阅读要求中所列著作或其他。

2、课外阅读要求

[1] 盖伊(加拿大). 数论中未解决的问题, 北京：机械工业出版社, 2007

[2] Felix Klein. Elementary Mathematics from an Advanced Standpoint（高观点下的初等数学，第 1—6 章）. 上海：复旦大学出版社，2008

[3] 孙琦, 曹珍富. 初等数论经典例题. 哈尔滨：哈尔滨工业大学出版社，2012

3、课堂讨论要求

讨论目的要明确。教师应提出与当堂课程内容有关的、合理而有价值的讨论题目，激发学生思考，避免提出学生知识结构不能达到的问题。

分组合理分工明确。可自由组合，也可按观点的异同进行分组。可先分组讨论再全班讨论。学生应积极参与。

教师应是组织者和指导者。教师应适当控制讨论局面，使得性格内向的学生也有发言机会，但教师不宜发言过多，左右学生的思维。

课堂规范

课堂纪律

课堂纪律是教学活动正常有效进行的一个保证，是教师教好课，学生学好课的前提。

1、教师需在上课前 10-15 分钟到达上课教室，做好课前准备，比如检查有无粉笔黑板刷，开多媒体，检查多媒体能否正常使用。学生需在上课前 5-10 分钟到达上课教室。迟到的学生从教室后门进入教室，不能影响老师和其他学生上课，并在下课后主动向老师说明迟到原因。

2、课堂上教师不能抽烟喝酒，不能吃东西，不能接打电话，手机调为震动或静音。非特别紧急的情况下不能上厕所。

3、课堂上学生不能睡觉，不能抽烟喝酒，不能吃东西，不能交头接耳，不能做与本课程无关的事（如做作业，听音乐），不能接打电话，不能玩手机，手机调为震动或静音。需要上厕所举手示意，教师同意后方可出教室。

4、教师上课使用普通话。学生发言或提问要举手，经老师同意并起立用普通话表达。

5、上课期间，无关人员一律不得进出教室，或在课堂内逗留。

6、下课铃声响起后，老师和学生方可出教室。不得提前下课。

课堂礼仪

礼仪是人类为维系社会正常生活而要求人们共同遵守的最起码的道德规范，它是人们在长期共同生活和相互交往中逐渐形成，并且以风俗、习

惯和传统等方式固定下来。对一个人来说，礼仪是一个人的思想道德水平、文化修养、交际能力的外在表现，对一个社会来说，礼仪是一个国家社会文明程度。道德风尚和生活习惯的反映。

本课程要求教师和学生遵循的礼仪规范主要有：

1、教师和学生均需着装整齐得体，不能穿拖鞋，吊带背心进入教室。

2、爱护教室内的公物、设备（如桌椅，灯具，多媒体设施）。损坏公物、设备要照价赔偿。不能随意搬动教室理的公共设施，不随地吐痰，不乱扔废弃物。

3、教师和学生在上课过程中均应注意语言文明，相互尊重。教师不能辱骂学生，更不能对学生进行体罚。学生不能随意打断顶撞老师，有问题或意见不一致应举手，经教师同意后相互沟通协调。

4、上课期间和课间均不得在教室或过道内打闹、喧哗，影响其他班级的教学或其他同学的正常自习。

5、教师上完课应关闭多媒体和多媒体机柜。如果课程为上午（下午、晚上）最后一节课，最后离开教室的老师或学生应关闭教室的所有灯光。

课程考核

1、出勤（迟到、早退等）、作业、报告等的要求

（1）一学期教师至少随机抽 1/2 的课时点名，对迟到旷课的学生作书面记载。严禁不假不到，病假事假需相应的请假条（所在学院负责老师签字）。旷课一次扣平时成绩 3 分,迟到或早退一次扣平时成绩 2 分.

（2）学生按时保质保量完成作业，由组长收发作业。作业全批全改，用 A+、A、B、C、D 五个等级，分别表示 100 分（全对且书写工整），90-99（全对或极少数错误）、80-89（错 1 道题以上）、70-79（错 2-3 题）和 60-69（错一半以上或未完成）。

2、成绩的构成与评分规则说明

平时成绩 30% （其中考勤 10%，作业 10%，期中考试 10%）+ 考核成绩 70%

3、考试形式及说明

考试形式：闭卷考试

说明：旷课次数达点名次数 1/3、未参加期中考试或作业一次都没有交的同学不能参加期末考核。

学术诚信

本课程的考核过程中，若出现学生考试违规与作弊，抄袭他人论文或其他伪造成果的行为，按四川理工学院相应政策处理。

课程资源

1、教材与参考书

本课程教材为：闵嗣鹤, 严士健著，高等教育出版社出版的《初等数论》（第三版）（2013 年 9 月第 22 次印刷）

本课程参考书目可选：

[1] 潘承桐, 潘承彪. 简明数论. 北京：北京大学出版社，2000.

[2] 柯召, 孙琦. 数论讲义. 北京：高等教育出版社, 2003.

[3] 布恩（英）著, 于秀源译. 数论入门. 哈尔滨: 哈尔滨工业大学出版社, 2011.

[4] 华罗庚. 华罗庚文集：数论卷. 北京：科学出版社，2010.

2、专业学术著作

《初等数论》是数学与应用数学专业的一门重要的专业必修课，相对其他数学课程的抽象性，《初等数论》更容易理解和掌握。与《初等数论》有关的学术著作和科研论文比较多，除上述参考书目外，还有如下著作等（不能完全列出）。

[1] 罗森 (KennethH. Rosen). 初等数论及其应用 (英文版). 北京：机械工业出版社, 2010.

[2] 维诺格拉多夫（俄罗斯）著, 裘光明译. 数论基础. 哈尔滨: 哈尔滨工业大学出版社, 2011.

[3] ZHANG Weidong, Lü Xixiang, LI Hui. Efficient Broadcast Encryption

Scheme Based on Number Theory Research Unit. Wuhan University Journal of Natural Sciences , 2010, 15(3): 247-250.

[4] 蒋亦华. “初等数论”教学中的创造性思维训练与能力建构. 大学数学, 2006, 22(3): 32-34.

3、专业刊物

Acta Mathematica Sinica (English Series) 、 Chinese Science Bulletin、 Northeastern Mathematical Journal、Science China (Mathematics)、《数学进展》,《应用数学学报》、《数学年刊》、《数学的实践与认识》、等刊物，以及一些高校学报均可刊登初等数论方面的文章。

4、网络课程资源

爱课程：http://www.icourses.cn

中国大学 MOOC：http://www.icourse163.org/

网易公开课：http://open.163.com/

初等数论，北师大视频教程

http://video.1kejian.com/university/ligong/26520/

5、课外阅读资源

[1] JosephH. Silverman. 数论概论，北京：机械工业出版社, 2008.

[2] 王元，严士健，石钟慈，谈德颜编译. 数学百科全书（5 卷本）. 北京：科学出版社，1994－2000.

[3] 张奠宙. 20 世纪数学经纬. 上海：华东师范大学出版社，2002.

教学合约

本人已阅读《初等数论》课程实施大纲，理解了其中内容。本人同意遵守课程实施大纲中阐述的标准和期望，并将本课程的重点、难点、课程要求、课堂纪律，课堂礼仪、考核形式及要求传达给学生。