《初等数论》教学大纲

课程编码：110823

课程名称：初等数论

学时/学分：54/3

先修课程：《数学分析》、《高等代数》

适用专业：信息与计算科学

开设教研室：代数与几何教研室

一、课程性质与任务

1．课程性质：初等数论是信息与计算科学专业的一门专业必修课程。该课程是研究整数性质和方程（组）整数解的一门学科，也是一个古老的数学分支。初等数论是现代密码学的一门基础课程，也是高等学校信息安全专业的一门重要的基础课。初等数论在计算技术、通信技术等技术学科中也得到了广泛的应用。

2．课程任务：初等数论是信息与计算科学专业的一门重要的专业必修课，开设的目的在于使学生熟悉和掌握数论的基础知识，基本理论和基本的解题技能技巧，培养学生的逻辑思维能力，更深入地理解初等数论与其它邻近学科的关系，为进一步学习信息安全领域的其它学科打下坚实的基础。

二、课程教学基本要求

初等数论是研究整数性质的一门学科，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，容易引起人的兴趣，但是解决它们却非常困难。本课程的目的是简单介绍在初等数论研究中经常用到的若干基础知识、基本概念、方法和技巧。

通过本课程的学习，使学生加深对整数的性质的了解，更深入地理解初等数论与其它邻近学科的关系。

1. 有关定义、定理、性质等概念的内容按“知道、了解和理解”三个层次要求；有关计算、解法、公式和法则等方法的内容按“会、掌握、熟练掌握”三个层次要求。

2. 本课程开设在第 5 学期，总学时 54，其中课堂讲授 54 学时，课堂实践 0 学时。教学环节以课堂讲授为主，研制电子教案和多媒体幻灯片以及 CAI 课件，在教学方法和手段上采用现代教育技术。

3. 成绩考核形式：期终成绩（闭卷考试）（70%）＋平时成绩（平时测验、作业、课堂提问、课堂讨论等）（30％）。成绩评定采用百分制，60 分为及格。

三、课程教学内容

第一章　整数的可除性

1. 教学基本要求

以带余除法为先导，以辗转相除法、最大公因数、最小公倍数和算术基本定理为主干、讲授整除理论中最基本的性质。

2. 要求学生掌握的基本概念、理论、原理

通过本章学习，使学生能准理解整数整除、公因数、公倍数的概念及相关性质，理解剩余定理，熟练掌握用剩余定理求最大公因数、最小公倍数的方法。理解素数与合数的概念、素数的性质，理解整数的素数分解定理，会用筛法求素数。了解函数[x]与{x}的概念、性质，n!的素数分解、组合数为整数的性质。

3. 教学重点和难点

教学重点是最大公因数，互素的概念及性质，算数基本定理的应用；$n(\geq 2)$ 个整数的最大公因数及将最大公因数表为原 n 个整数的倍数和的求法。教学难点是最大公因数的性质及应用，算术基本定理的证明及应用。

4. 教学内容

第一节　整除的概念、带余数除法

1. 整除的概念及性质
2. 奇、偶数的运算性质
3. 带余数除法定理

第二节　最大公因数与辗转相除法

1. 最大公因数的概念与性质
2. 求最大公因数的辗转相除法

第三节　整除的进一步性质及最小公倍数

1. 最大公因数 (a,b) 为 a,b 的倍数和
2. 互素的性质
3. 最小公倍数与最大公因数的关系

第四节　质数、算术基本定理

1. 质数的概念及性质
2. 算术基本定理及应用
3. 质数的分布

第五节　高斯函数[x]，{x}及其在数论中的一个应用

1. 高斯函数[x]，{x}的定义及性质
2. 求 n!的标准分解式

第二章　不定方程

1. 教学基本要求

讨论二元一次不定方程有解的条件及其解法，进而研究多元一次不定方程有解的条件及其解法。介绍一些特殊的二元二次不定方程（商高不定方程）的解法。

2. 要求学生掌握的基本概念、理论、原理

通过本章学习，使学生能准确理解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，熟练掌握利用剩余定理（辗转相除法）求二元一次不定方程的方法。知道多元一次不定方程有解的条件，会求解简单的多元一次不定方程。知道勾股方程的整数解的形式，会求其在特定条件下的整数解。

3. 教学重点和难点

教学重点是二元一次不定方程、商高方程的理论及应用。教学难点是二元一次不定方程有解的条件及其解法，二元二次不定方程（商高不定方程）的解法。

4. 教学内容

第一节　二元一次不定方程

1. 二元一次不定方程有整数解的判别法则
2. 二元一次不定方程的通解及求通解的步骤

第二节　多元一次不定方程

1. 多元一次不定方程有整数解的判别法则
2. 多元一次不定方程的解法（引入辅助未知量法、逐步降低系数法、矩阵列变换法）
3. 多元一次不定方程组的一般解法原则

第三节　勾股数

1. 求商高方程的整数解
2. 勾股数的性质

第三章　同余

1. 教学基本要求

同余是数论中的一个基本概念，是整除概念的推广。本章首先介绍同余的概念及基本性质，引入完全剩余系与简化剩余系的概念，建立 Euler 定理和 Fermat 定理。

2. 要求学生掌握的基本概念、理论、原理

通过本章学习，使学生能准确理解并掌握整数同余的概念、同余的基本性质，整数具有素因子的条件，会利用同余简单验证整数乘积运算的结果。理解剩余系、完全剩余系的概念，掌握判断剩余系的方法，欧拉函数的定义及性质。了解欧拉定理、Fermat 小定理，循环小数的判定条件。

3. 教学重点和难点

教学重点是同余的概念及基本性质、简化剩余系的判定与应用。教学难点是简化剩余系及欧拉函数、欧拉定理及其应用。

4. 教学内容

第一节　同余的概念及其基本性质

1. 同余概念与整除概念的联系
2. 同余的性质及应用

第二节　剩余类及完全剩余系

1. 模 m 的剩余类及完全剩余系的概念
2. 模 m 的最小非负完全剩余系
3. 完全剩余系的性质

第三节　简化剩余系与欧拉函数

1. 简化剩余系的概念及性质
2. 欧拉函数的概念、计算公式及简单性质

第四节　欧拉定理、费尔马定理

1. 欧拉定理、费尔马定理
2. 欧拉定理、费尔马定理的应用

第四章　同余式

1. 教学基本要求

介绍同余式的解法，主要研究一次同余式（组）、素数模的高次同余式及合数模的高次同余式。

2. 要求学生掌握的基本概念、理论、原理

通过本章学习，使学生能准确理解同余式的定义，掌握一次同余式有解的条件，熟练掌握求解一次同余式。理解中国剩余定理，掌握中国剩余定理的应用，会求解同余式方程组。了解判断高次同余式的解个数，知道解高次同余式的方法，了解模整数同余式与模素数同余式的关系，掌握求解简单的（3、4 次）同余式。了解素数模同余式的次数化简，Wilson 定理，同余式的次数与解数的关系，知道 n 次同余式有 n 个解的条件。

3. 教学重点和难点

教学重点是一次同余式的解法、孙子定理。教学难点是高次同余式、质数模的同余式的求解。

4. 教学内容

第一节　基本概念及一次同余式

1. 同余式的一般概念

2. 一次同余式的判别定理（解的存在性及解的个数）

3. 一次同余式的解法（一次简约同余式的解法：穷举法、辗转相除法、分数法(用同余的性质求解)、公式法）

第二节　孙子定理

1. 一次同余式组的概念

2. 一次同余式组的解法（孙子定理）

第三节　高次同余式的解数及解法

1. 通过模的分解化简同余式

2. 以质数幂 P^{α} 为模的高次同余式

第四节　质数模的同余式

1. 同余式次数的降低

2. 高次同余式解的性质

3. 威尔逊定理

4. 高次同余式的解数与次数的关系

第五章　二次同余式与平方剩余

1. 教学基本要求

引入平方剩余与平方非剩余的概念,介绍平方剩余与平方非剩余的判别条件。引入 Lerandre 符号、Jacobi 符号，并用它研究素数模的二次同余式及合数模的二次同余式。

2. 要求学生掌握的基本概念、理论、原理

通过本章学习，使学生能准确理解二次同余式的一般形式、模整数同余与模素数幂同余的关系、平方剩余与平方非剩余的概念。理解单素数的平方剩余与平方非剩余的欧拉判定法，了解单素数的平方剩余与平方非剩余的个数。了解 Legendre 符号的定义、性质及 Jacobi 符号的定义、性质，熟练掌握利用 Legendre 和 Jacobi 符号判断同余式的解的存在性。掌握非素数模的二次同余式有解的条件及解的个数的有关结论。

3. 教学重点和难点

教学重点是单质数模的平方剩余与平方非剩余的概念及判定、互倒定律、单质数模 P 的二次同余式 $x^2 \equiv a(\mathrm{mod}\, p)$ 的解法。教学难点是平方剩余与平方非剩余的概念，Lerandre 符号。

4. 教学内容

第一节　一般二次同余式

1. 一般二次同余式的转化

2. 模 m 的平方剩余与平方非剩余的概念

第二节　单质数的平方剩余与平方非剩余

1. 欧拉判别条件

2. 平方剩余与平方非剩余的基本性质

第三节　勒让得符号

勒让得符号的定义及性质

第四节　前节定理的证明

前节定理 3 的证明

第五节　雅可比符号

1. 雅可比符号的定义

2. 雅可比符号与勒让得符号在概念上的区别

3. 雅可比符号的性质

第六节　合数模的情形

1. 以奇质数的方幂为模的二次同余式

2. 模2^{α}的二次同余式

3. 一般合数模的二次同余式

四、学时分配表

章序	内容	课时	备注
一	整数的可除性	14	
二	不定方程	9	
三	同余	12	
四	同余式	9	
五	二次同余式与平方剩余	10	
合计		54	

五、主用教材及参考书

（一）主用教材：

《初等数论》（第三版） 主编：闵嗣鹤　出版社：高等教育出版社　出版时间：2003 年。

（二）参考书：

1. 《初等数论》　主编：于秀源　出版社：山东教育出版社　出版时间：2004 年。

2. 《简明数论》　主编：潘承洞　出版社：北京大学出版社　出版时间：1998 年。

3. 《初等数论及其在密码学中的应用与 Maple 实现》　主编：游林　出版社：科学出版社　出版时间：2009 年。

4. 《初等数论及其在信息科学中的应用》　主编：朱萍　出版社：清华大学出版社　出

版时间：2010 年。

执笔：皮　磊
审定：郭宏旻　梁桂珍