目　录

绪论

第一部分　初等数论基础

第1章整除
1.1　整除
1.2　最大公因子与最小公倍数
1.3　欧几里德算法
1.4　求解一次不定方程--Euclid 算法应用之一
1.5　整数的素分解

第 2 章　同余
2.1　同余
2.2　剩余类与剩余系
2.3　Euler　定理
2.4　Wilson 定理

第 3 章　同余方程
3.1　一元高次同余方程的概念
3.2　一次同余方程
3.3　一次同余方程组　孙子定理
3.4　一般同余方程组
3.5　二次剩余
3.6　Legendre 符号与 Jacobi 符号

第 4 章　指数与原根
4.1　指数及其性质
4.2　原根及其性质
4.3　指标、既约剩余系的构造
4.4　n 次剩余

第 5 章　素数分布的初等结果
5.1　素数的基本性质与分布的主要结果介绍
5.2　Euler 恒等式的证明
5.3　素数定理的初等证明
5.4　素数定理的等价命题

第二部分　近世代数基础

第 6 章　基本概念

6.1 映射
6.2 代数运算
6.3 带有运算集合之间的同态映射与同构映射
6.4 等价关系与分类

第 7 章 群
7.1 群的定义
7.2 循环群
7.3 变换群、置换群
7.4 子群 子群的陪集
7.5 同态基本定理
7.6 有限群及实例

第 8 章 环与域
8.1 环的定义
8.2 整环、域、除环
8.3 子环、理想、环的同态
8.4 商域

第 9 章 唯一分解整环
9.1 分解的基本概念
9.2 唯一分解整环
9.3 主理想整环
9.4 唯一分解整环上的多项式环

第 10 章 扩域
10.1 域的特征
10.2 扩域
10.3 有限域
10.4 编码（有限域的一个应用）

第 11 章 公钥密码学中的数学问题
11.1 时间估计与算法复杂性
11.2 分解因子问题
11.3 素检测
11.4 RSA 问题与强 RSA 问题
11.5 二次剩余
11.6 离散对数问题