第一章 初等数论

1.1 整除基本性质的应用。

1.2 最大公约数的计算。

1.3 求解二元一次不定方程。

1.4 同余基本概念的应用。

1.5 Euler 函数的计算、Euler 定理和 Fermat 小定理的应用、缩系的概念。

1.6 求解一次同余式。

1.7 中国剩余定理及其应用。

1.8 Legendre 符号计算。

1.9 求解模为合数的二次同余式。

1.10 模为素数的次数的性质、原根的判定方法。

第二章 代数基础

2.1 代数运算，群，交换群，剩余类加群，剩余类乘法群，群的阶，群元素的阶，定理 2.1，循环群。

2.2 子群，子群的判定，陪集，陪集的性质，定理 2.5（Lagrange 定理），子群在群中的指数，正规子群，商群。

2.3 群同态，同态映射的性质，群同构，同态核，定理 2.7（同态基本定理）。

2.4 环的概念和环上元素的性质。

2.5 子环和理想的概念。

2.6 环同态的定义。

2.7 域的概念，有限域上多项式的加法和乘法运算，有限域的本原元，有限域的构造（给定不可约多项式，要求会构造有限域）。

第四章 信息论基础

4.2 事件的自信息，随机变量的平均自信息（熵），Jensen 不等式及其推论（不要求会证，会应用），熵的性质 1-7。

4.3 事件的联合自信息，事件的条件自信息，联合熵，条件熵，熵、联合熵与条

件熵的关系。

4.4 事件的互信息，随机变量的平均互信息，平均互信息的基本性质（定理 4.5）。

4.5 离散信源的概念，离散无记忆信源的概念，定理 4.6。

4.6 密码系统模型，完全保密密码系统的概念，定理 4.9，密码系统明文熵，密码系统密钥熵，唯一解距离。

第五章 计算复杂性理论

5.1 Θ 记号、o 记号、w 记号的使用。

5.2 设计多带确定性图灵机解决简单算术问题，例如，计算两个二进制整数相乘。

5.3 计算复杂理论证明加密方案的框架。