第一章 初等数论

1.1 整除基本性质。

1.2 二元一次不定方程。

1.3 Euler 函数的计算、Euler 定理的应用、缩系的概念。

1.4 求解一次同余式。

1.5 模为合数的同余式的解法。

1.6 Legendre 符号的应用。

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。

2.2 子群，子群的判定，正规子群。

2.3 群同态，同态映射的性质，群同构，同态核，同态核和同态像的性质。

2.4 环的概念和环上元素的性质、多项式环的概念和次数。

2.5 域的概念，有限域上多项式的加法、乘法、求逆运算，有限域的构造（给定不可约多项式，要求会构造有限域）。

第三章 组合数学

3.1 允许重复的排列与组合问题。

3.2 把物体放入盒子问题。

3.3 容斥原理与鸽笼原理。

3.4 母函数与指数母函数。

第四章 信息论基础

4.1 事件的自信息的定义与性质，随机变量的平均自信息（熵）的定义与性质，Jensen 不等式及其推论（不要求会证，会应用）。

4.2 事件的联合自信息的定义与性质，事件的条件自信息的定义与性质，联合熵和条件熵定的义与性质，熵、联合熵与条件熵的关系。

4.3 事件的互信息，随机变量的平均互信息的定义与性质。

第五章 计算复杂性理论

5.1 Θ 记号、O 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 函数的多项式相关。

5.4 可忽略的函数。

5.5 计算复杂理论证明加密方案的框架。