《信息安全数学基础》

陈大江 副教授
信息与软件工程学院
电子科技大学
djchen@uestc.edu.cn

目　　录

第一章 整数

- 1.1 整数概念和基本性质
- 1.2 欧几里得算法及其扩展算法
- 1.3 素数与算术基本定理

第二章 同余

- 2.1 同余的概念和基本性质
- 2.2 同余类与剩余系
- 2.3 模m的算法
- 2.4 RSA公钥加密算法

第三章 同余方程

- 3.1 同余类与剩余系
- 知道什么是二次剩余

第四章　群

- 4.1　二元运算
- 4.2 群的定义和简单性质
- 4.3 子群、陪集
- 4.4 正规子群、商群和同态
- 4.5 循环群
- 知道ElGamal公钥加密算法

第五章 环与域

- 5.1 环的定义
- 5.2 整环、除环和域
- 5.3 子环、理想和商环

第六章 多项式

- 6.1 多项式相关概念
- 6.2 因式
- 6.3 多项式同余

多项式环中的扩展欧几里得算法；

如何域上的多项式环得到一个扩域。

第七章 有限域

- 7.2 有限域的结构

  有限域只能是F_{p^n}；F^*为乘法群；子域的结构

- 7.4 有限域上元素的表示

  怎么从F_p得到 F_{p^n}

- 7.5 有限域中的算法

第八章 椭圆曲线

- 8.2 椭圆曲线（循环群）的运算；
- 8.4 椭圆曲线的离散对数(小步-大步算法可了解)
- 8.5 基于椭圆曲线的ElGamal公钥加密算法

Any

Question?