

## 离散数学(二)复习重点

1. 二进制模幂算法。参考上课 PPT: 001 数论和密码学 第 16 页—20 页
2. 欧几里得算法。参考上课 PPT: 001 数论和密码学 第 48 页—49 页
3. 扩展欧几里得算法求贝祖系数。参考上课 PPT: 001 数论和密码学 第 52 页—56 页
4. 求解逆元。参考上课 PPT: 001 数论和密码学 第 62 页—64 页
5. 用逆元求解一次同余方程。参考上课 PPT: 001 数论和密码学 第 65 页
6. 用中国剩余定理求解同余方程组。参考上课 PPT: 001 数论和密码学 第 67、68、70 页
7. 校验位 ISBNs。参考上课 PPT: 001 数论和密码学 第 88 页
8. 密码系统—RSA。参考上课 PPT: 001 数论和密码学 第 103 页—107 页。注意 RSA 会用到欧拉函数  $\phi(n)$  计算, 参考上课 PPT: 001 数论和密码学 第 73 页。
9. 加密协议—数字签名。参考上课 PPT: 001 数论和密码学 第 110 页—112 页。
10. 母函数。参考上课 PPT: 002 计数 第 68—75 页。
11. 002-计数重点看例题。
12. 用生成函数求解递推方程。参考上课 PPT: 003 高级计数 第 16—18 页。
13. 求解常系数线性非齐次递推关系。参考上课 PPT: 003 高级计数 第 36—37 页。
14. 求给定公式的真值表。参考上课 PPT: 004 命题逻辑 第 40—42 页
15. 证明公式之间的等价关系 (利用等价公式或证明等号两端的式子永真或永假)。参考上课 PPT: 004 命题逻辑 第 61、63 页
16. 奇怪岛上的逻辑问题。参考上课 PPT: 004 命题逻辑 第 70—80 页
17. 求主析取范式极小项、主合取范式极大项。参考上课 PPT: 004 命题逻辑 第 90—96 页
18. 求主析取范式和主合取范式的方法 (公式转换法、真值表技术)。参考上课 PPT: 004 命题逻辑 第 102—112 页。第 53—55 页基本等价公式需要重点记忆
19. 判断公式永真、永假或可满足。参考上课 PPT: 004 命题逻辑 第 44、119—124 页
20. 谓词逻辑推理的应用。参考上课 PPT: 006 推理与证明技术 第 66—82 页