考试要求

本学期课时只有24， 所以讲过的知识点基本上都可能要考到。没讲过的肯定不考。

虽然只有24学时，但出于让大家扩大知识面，多接触些内容的目的， 讲得比较多、比较快，没有讲那么细。考试时主要注重基础。

题目类型以及大概的分数分布

- **填空6×3** 分
- **解答题，**每小题5到8分。 共52分
- 其中解答包括了一些计算，判断说明理由之类的内容

- **证明2×10 分**（组合分析法证明、数论及应用的证明）
- 综合10分（建模及求解）
- **内容分布比例：**
- 组合计数：65分左右
- 数论及应用 35 分左右

组合计数问题

- 无重复排列组合；可重复的排列与组合；尤其是可重复的组合计数
- 鸽洞原理及其应用
- 二项式系数的组合理解、组合分析法证明等式
- 多重集合的r-组合数、r-排列。

- 递推方程建模
- 常系数线性齐次递推方程求解；
- 常系数线性非齐次递推方程的解与相伴齐次递推方程的解的关系；非齐次的尾部函数F(n)为1次或2次多项式情形的特解的求法；

(尤其是2阶的递推关系、分特征方程有重根和无重根两种情况，都需要搞清楚)

组合计数问题

- 利用生成函数求解物体配置的计数问题；
- 利用生成函数求解带限制条件的不定方程；先把问题用不定方程的模型表示出来，然后再利用生成函数求解不定方程；
- 钱币组合计数问题；
- 生成函数求解多重集的元素组合选取问题。
- (生成函数求解递推方程不考)
- 容斥原理及其简单应用；容斥原理中有关$N(p_1p_2...p_k)$的求解；
- 分治部分（不考）
- 整数拆分部分（不考）

数论

- 素数性质、整除方面的问题
- 最大公约数的计算和性质
- 余数运算性质及其证明，熟悉模余计算；
- 模指数运算
- 求模逆；求解单个同余方程
- 求解同余方程组部分不考；大整数计算应用不考；
- 欧拉函数，欧拉定理与菲尔马小定理在模余计算中的应用
- RSA中加密函数与解密函数之间的关系，RSA加解密计算；RSA解密钥匙的获取；
- 数字签名（不考）；
- Diff-Helmen key交换协议部分不考；
- 模余应用（生产伪随机数、校验位产生等)不考；

建议

- 建议大家不要去买复印店里那些所谓的考题。
- 好好看看、想想、更多关注平时讲过的例题和做过的习题的类型；