

考试复习备忘录（自我检查列表）

1. 是否熟悉欧几里得除法？
 2. 是否能够根据辗转相除法计算最大公因子？
 3. 能否利用贝祖等式求逆？
 4. 能否利用标准分解式证明相关等式？
 5. 能否用反证法证明某种素数有无穷多个？
 6. 能否判断某个一次同余式是否有解并正确求出其解？
 7. 能否利用中国剩余定理化简高次同余式？
 8. 能否利用费马小定理化简高次同余式？注意关系成立时对模的要求。
 9. 是否对某个高次同余式做过一次完整求解？参考书上例题和作业自我测试一次，了解对模值的要求和相应的处理方法。
 10. 是否熟悉勒让德符号计算以及二次互反律计算方法？雅可比符号，二次互反律计算方法？掌握它们在二次剩余德判断中有何不同？
 11. 原根与指标、指数的关系？如何判断某个模值是否存在原根？
 12. 对几种基于概率的拟素数的判断方法是否熟悉？了解它们之间的差异，能够证明是否满足相关条件。
 13. 对群及子群的判断条件？注意有限集合与无穷集合的差别。
 14. 置换群及其计算，参考书上相应例子，给定两种置换变换，至少能够计算其复合变换的结果，以及某个置换的逆变换。
 15. 对几种特殊环（包括域）、理想及其相关性质的证明要熟悉，参看书上相关例子；对环同态及其性质也要熟悉。
- 如果确保上述 15 点你都能够顺利解决，完全理解了相关内容，那么恭喜你，你已经做好了这次考试的充分准备。祝各位取得好成绩！