密码学作业001 学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_姓名\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

（以Word文档提交,提交文档时在文件名和文档内部都写上学号和姓名,此后的各次作业按照此法处理）：

1. 用伪码表示非递归版本的欧几里得算法。
2. 用伪码表示递归版本的欧几里得算法。
3. 用伪码表示非递归版本的扩展欧几里得算法。
4. 用伪码表示递归版本的扩展欧几里得算法。
5. 扩展欧几里得算法有何用途？
6. 欧几里得算法的时间复杂度是对数量级还是线性量级？
7. 直接的幂算法或模幂算法的时间复杂度是什么量级？
8. 设a与b都为正整数，集合 {xa+yb|x,y都是整数}中的最小正整数记为d，证明：gcd(a,b)=d
9. 若a,b,q,r皆为整数， a=bq+r, 证明gcd(a,b)= gcd(b,r)