**25.7.4信息安全数学基础**

一简答8\*5=40分

1.辗转相除法求gcd（a，b） （数据忘了）

2.求s，t。as+bt＝gcd（a，b）

3.求243^402（mod 1000）

4.弃9法检验

5. 忘了，反正很简单

6.求某个数全部的原根

7.已知5为17的原根，求5^2模17的？（忘记是什么了）

8.已知35为2模71的指数，求模71的一个原根

二、4\*5=20分

1.2^a -1 除去2^b -1的最小正余数为2^r -1， a除去b的最小正余数为r，求证其最大公因数为2^（a，b） -1

2.简单证明题，忘记题干了，是要求证x|（a，b）。然后题干能简单推出x|a，x|b。

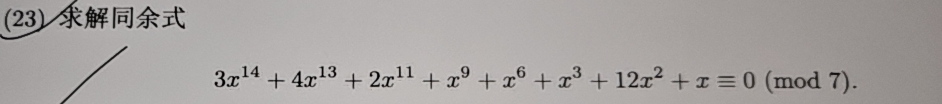
3. 简单证明题，也忘了

4.大概长这样，



三2\*10=20分

1.同类题，就左侧方程的未知数系数不一样



2.求2^1000000（mod1309），它还非常贴心的给了1309＝7\*11\*17

四综合2\*10=20分

1.已知p为素数，求证p-3为p的平方剩余

2.给了指标表，求什么东西（我不会做就没看题）

请谅解，编者因为熬夜贯彻速通精神，导致记忆力衰退忘记了不少题目