华中科技大学计算机与科学技术学院

“ 离散数学（二）”考试试卷 (A 卷)

考试方式 闭卷 考试日期 _____ 考试时长 **150** 分钟

专业班级 _____ 学　　号 _____ 姓　　名 _____

题号	一	二	三	四	五	六	总分	核对人
分值	24	46	10	20			100	
得分								

分　数	
评卷人	

一. 填空题(每小题 4 分，共 24 分)

(1) 1---20 中至少要取_____个数才能保证取到的数中一定有一个是另一个的因数。

(2) 9 个人平均分成 3 部分有_____种分法。

(3) 三元四次多项式最多有_____项。

(4) 10 个人举行一次舞会，其中 3 个女生，7 个男生，规定女生不可能跟女生跳舞，每个人都必须找一个舞伴跳舞，共有_____种舞伴的搭配方案。

(5) 1200 和 1800 有_____个公共的正因数。

(6) 7 模 10 的逆是_____.

分　数	
评卷人	

二． 解答题 （共　分）

(7) 不含有两个连续 1 的 n 位的二进制串有多少个？要求写出一个递推关系，以及递推关系的初始条件。(6 分)

(8) 解递推式：$a_n = 5a_{n-1} - 4a_{n-2} + n^2$, $n \geq 2$. 已知 $a_0 = 0$, $a_1 = 1$. (10 分)

(9) 请用生成函数法，求方程 $x + y + z = 15$ 满足 $1 \leq x \leq 4$, $2 \leq y \leq 5$, $3 \leq z \leq 6$ 的整数解的个数。(8 分)

(10) A,B,C,D,E,F,G,H 等 8 人参加体能考核，考核出了 3 种结果（优，及格，不及格）。已经知道 B 的考核结果是优。 问有多少种可能的结果搭配组合? (10 分)

(11) 求 $((P^{17}-P+1)^{20} \bmod 12$, 其中 P 是大于 3 的素数。(6 分)

(12) 求解同余式：$65x \equiv 25 \pmod{111}$. (6 分)

分　数	
评卷人	

三． 数论在密码学的应用（共 10 分）

(13) 令 N=55, k=37, t=54. (10 分)

(a) 求出以 k 作为公钥，密文 t 对应的明文;

(b) 求出以 k 作为私钥，明文 t 对应的密文。

(c) 对于任意的两个不同的素数的乘积 n，假设不知道 RSA 算法使用的私钥。如果知道明文 M 以及相对应的密文 C，如何求出密钥，给出求密钥的方程式。 并且分析求解该方程的可行性以及可能存在的问题。

分　数	
评卷人	

四. 证明 (每题 10 分，共 20 分)

(14) 已知整数 n 与 6 互素，求证：18 | (n^7 − n). (10 分)

(15) 用组合分析法证明:

$$\sum_{k=0}^{m} \binom{n-k}{n-m}\binom{n}{k} = 2^m \binom{n}{m}$$

解答内容不得超过装订线