离散数学 (CS201) 2024春期中考试

共 11 道大题，总分 110 分（10分 bonus），时间 120 分钟

Q1. (12分) S 是一个联结词的集合，如果任何一个真值函数都可以用仅含 S 中的联结词的命题公式表示，那么称 S 是全功能集。在本题中，所有命题的域都相同。

a) 已知 $\neg$，$\vee$，$\wedge$ 能够组成一个全功能集，证明 $\neg$，$\vee$ 能够组成一个全功能集

b) 证明 $((\neg p \vee q) \wedge (p \vee r)) \rightarrow (q \vee r)$ 是 tautology

c) 已知 $\forall x(P(x) \rightarrow (Q(x) \wedge R(x)))$，$\forall x(P(x) \wedge S(x))$，使用 rules of inference 证明 $\forall x(R(x) \wedge S(x))$，不要使用逻辑恒等式

Q2. (10分)

a) 证明或反证对于正整数 x, y，$x^4 + y^4 = 625$ 有解

b) 证明或反证 $n^2 - 79n + 1601$ 对于任意正整数 n 均为质数

Q3. (10分) 证明或反证存在有理数 x 和无理数 y 使得 x^y 是无理数，在本题中，$\sqrt{2}$ 是无理数的结论可以直接使用

Q4. (10分) 函数 $f : A \rightarrow B$，S 是 B 的一个子集，那么 $f^{-1}(S)$ 定义为 $f^{-1}(S) = \{a \in A | f(a) \in S\}$. 证明或反证对于任意 S，$f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$

Q5. (8分) 函数 $f(x) = \frac{x^2+1}{x^2+2}$，定义域和值域都是 $\mathbb{R}$

a) 证明或反证 $f(x)$ 是单射

b) 证明或反证 $f(x)$ 是满射

Q6. (10分) 证明若 n 是奇数，那么 $n^2 \equiv 1 \, (mod \ 8)$

Q7. (10分) 证明不存在从 $\mathbb{Z}^+$ 到 $\mathcal{P}(\mathbb{Z}^+)$ 的一一映射，在本题中，$\mathcal{P}(\mathbb{Z}^+)$ 可数与否并不已知，除非经过证明

Q8. (8分) 本题不需要写过程，只需要写答案

a) 写出以下 3 个多项式的最简大 O 函数（最简指形式中没有和），例如 $5n! + 10n^3$ 的最简大 O 函数为 $n!$

$$\text{i)} \ n\log(n^2+1) + (n^2+n)\log n \qquad \text{ii)} \ n^{2^n} + n^{n^2} \qquad \text{iii)} \ 10(n!)^3 + 2^n$$

b) 将上面 $\mathrm{i})$ 和 $\mathrm{ii})$ 得到的大 O 函数在 n 很大时进行大小比较

Q9. (10分) 使用中国剩余定理解线性同余方程：$x \equiv 1\,(mod\ 2)$，$x \equiv 2\,(mod\ 3)$，$x \equiv 3\,(mod\ 5)$，$x \equiv 4\,(mod\ 11)$

Q10. (12分) 在某个 RSA 加密中，$p = 53$，$q = 61$，$e = 17$，且字母 A 到 Z 的编码分别为 00, 01, ... , 25

a) 求 RSA 加密的解密密钥 d

b) 该 RSA 加密算法最多能够加密多长的信息，简单阐述理由

c) 计算信息 "AB" 经过加密密钥加密后的密文是什么

Q11. (bonus 10分) 希尔伯特酒店

a) 如果在希尔伯特酒店旁边，又建造了一座新的希尔伯特酒店，证明，原希尔伯特酒店里的旅客也可以填满这两座（原来的和新的）希尔伯特酒店

b) 希尔伯特酒店旁来了无穷但可数辆大巴，每辆大巴里面有无穷但可数个旅客，证明，新来的旅客还是能够成功入住希尔伯特酒店