CS201: Discrete Math for Computer Science
2022 Spring Semester

Total number of questions: $10 + 1$ (optional)
Total points: $100 + 10$ (bonus)

Q. 1. (10 points) Determine whether the following statements are correct or incorrect. Explain your answer. Assume that p, q and r are logical propositions, x and y are real numbers, and m and n are integers.

(1) $(\neg p \wedge (p \to q)) \to \neg q$ is a tautology.

(2) $(p \vee q) \to r$ and $(p \to r) \wedge (q \to r)$ are equivalent.

(3) Under the domain of all real numbers, the truth value of $\exists x \forall y (y \neq 0 \to xy = 1)$ is T.

(4) Under the domain of all integers, the truth value of $\exists n \exists m (n^2 + m^2 = 5)$ is T.

Q. 2. (8 points) For each of the following argument, determine whether it is valid or invalid. Explain using the validity of its argument form.

(1) Premise 1: If you did not finish your homework, then you cannot answer this question.

Premise 2: You finished your homework.

Conclusion: You can answer this question.

(2) Premise 1: If all students in this class has submitted their homework, then all students can get 100 in the final exam.

Premise 2: There is a student who did not submit his or her homework.

Conclusion: It is not the case that all student can get 100 in the final exam.

Q. 3. (8 points) Suppose that p, q, r, s are all logical propositions. You are given the following statement

$$(\neg r \vee (p \wedge \neg q)) \to (r \wedge p \wedge \neg q)$$

Prove that this implies $r \vee s$ using logical equivalences and rules of inference.

Q. 4. (16 points) Consider sets A and B. Prove or disprove the following.

(1) $\mathcal{P}(A \times B) = \mathcal{P}(B \times A)$.

(2) $(A \oplus B) \oplus B = A$, where $A \oplus B$ denotes the set containing those elements in either A or B, but not both.

(3) For any function $f : A \to B$, $f(S \cap T) = f(S) \cap f(T)$, for any two sets $S, T \subseteq A$.

(4) For function $f : A \to B$, suppose its inverse function f^{-1} exists. $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$, for any $S, T \subseteq B$.

Q. 5. (10 points) Prove or disprove that there exists an infinite set A such that $|A| < |\mathbf{Z}^+|$.

Q. 6. (10 points) Order the following functions by asymptotic growth rates, that is, list them as $f_1(n), f_2(n), \ldots, f_6(n)$, such that $f_i(n) = O(f_{i+1}(n))$ for all i. Then, explain your answer related to the first pair, i.e., $f_1(n)$ and $O(f_2(n))$. (Note: providing the explanation of the first pair is sufficient. There is no need to explain all pairs.)

$$2^n, n^{20}, n^2(\log n)^{20}, (n!)^5, (\log n)^{\log \log n}, \log(n^n),$$

where the base of the logarithm is 2.

Q. 7. (12 points) There are a group of people. If we count them by 2's, we have 1 left over; by 3's, we have nothing left; by 4, we have 1 left over; by 5, we have 4 left over; by 6, we have 3 left over; by 7, we have nothing left; by 8, we have 1 left over; by 9, nothing is left. How many people are there? Give the details of your calculation.

Q. 8. (12 points) Compute the following without calculator and explain your answer.

(1) $(33^{15} \mod 32)^3 \mod 15$

(2) $\gcd(210, 1638)$

(3) $34x \equiv 77 \pmod{89}$

(4) The last decimal digit of 3^{1000} (Hint: Fermat's little theorem)

Q. 9. (8 points) Prove that if $2^m + 1$ is an odd prime, then m does not has any odd factor that is greater than one. (Note: $x^m + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + ... - x^k + 1)$, where $m = kt$ and t is odd.)

Q. 10. (6 points) Recall the RSA public key cryptosystem. Consider prime numbers $p = 89$ and $q = 61$. Answer whether the following pairs of public key (n, e) and private key d are valid (whether the pair satisfies the required properties) or not, and explain your answer.

(1) $n = 5429$, $e = 61$; $d = 4501$

(2) $n = 5429$, $e = 89$; $d = 2829$

(3) $n = 5429$, $e = 30$; $d = 1568$

Q. 11. (Optional, bonus 10 points) The following ciphertext is encrypted with one of the encryption methods we taught in lecture. Try to recover the plaintext and describe the method (and parameters) used for encryption. Please explain the process how you get the answer. For example, if you write a program, please provide the code (uploading the source file as well). If you make a guess and use number theory, please provide the details.

"Qy qaq iloiyu uiwx lwhc oiu lwgc i nat ah srasalizcu. Yae vcjcp gvao oriz yae'pc mavvi mcz."