CS1231 Discrete Structures **Name:** ____________________
AY2017/2018 Semester 1
Mock Test
27/9/2017
Time Limit: 120 Minutes
Total score: 60 points

1 Multiple Choice Questions

Recall that $\mathbb{N}$ is the set of natural numbers, $\mathbb{Z}$ is the set of integers, $\mathbb{Q}$ is the set of rational numbers, and $\mathbb{R}$ is the set of real numbers.

1. (2 points) Which of the following statements is logically equivalent to $\sim p \vee (q \wedge r)$?
   A. $(p \rightarrow q) \wedge (p \rightarrow r)$.
   B. $\sim(p \wedge \sim q) \wedge (r \rightarrow p)$.
   C. $(\sim p \wedge q) \vee (p \wedge \sim r)$.
   D. All of the above.
   E. None of the above.

2. (2 points) Which of the following are rows of truth table of $p \rightarrow (q \rightarrow (r \rightarrow q))$? (The columns of the table are in the order p, q, r and $p \rightarrow (q \rightarrow (r \rightarrow q))$.)
   A. $true, false, true, false$.
   B. $true, true, false, true$.
   C. $false, true, false, false$.
   D. All of the above.
   E. None of the above.

3. (2 points) Which of the following statements translates into "All integers are multiples of 1"? Note that the notation $a \in \mathbb{Z}$ means that a is an integer.
   A. $\forall n \ (n \in \mathbb{Z} \wedge (\exists m \ (m \in \mathbb{Z} \rightarrow n = 1 \times m)))$.
   B. $\forall n \ (n \in \mathbb{Z} \rightarrow (\exists m \ (m \in \mathbb{Z} \wedge n = 1 \times m)))$.
   C. $\forall n \ (n \in \mathbb{Z} \rightarrow (\exists m \ (m \in \mathbb{Z} \rightarrow n = 1 \times m)))$.
   D. All of the above.
   E. None of the above.

4. (2 points) Which of the following statements is logically equivalent to the formula

$$\forall X\ (p(X) \lor q(X))?$$

   A. $(\forall X\ p(X)) \land (\forall Y\ q(Y))$
   B. $(\forall X\ p(X)) \lor (\forall Y\ q(Y))$.
   C. $(\exists X\ p(X)) \land (\exists Y q(Y))$.
   D. $(\exists X\ p(X)) \lor (\exists Y q(Y))$.
   E. None of the above.

5. (2 points) Given the following three statements, which of the following options are true?

   Statement 1: All smart people are tall.
   Statement 2: There is a person who is smart but not tall.
   Statement 3: All tall people are not smart.
   Statement 4: All smart people are not tall.

   A. Statement 4 is the negation of statement 1.
   B. Statement 3 is the contrapositive of statement 1.
   C. Statement 2 is the converse of statement 1.
   D. All of the above.
   E. None of the above.

6. (2 points) Let $n \in \mathbb{N}^+$, $m \in \mathbb{N}^+$. Suppose $5 \times n^2 = m$. Which of the following statement is true about the prime factorization of m?

   A. It may be empty.
   B. It may contain an even number of factors.
   C. It may contain an odd number of factors.
   D. All of the above.
   E. None of the above.

7. (2 points) Which of the following statements is true?

   A. 57 is a prime.
   B. $2^a = 5^b$ has no integer solution for a and b because all natural numbers have a unique prime factorization.
   C. If $p_1, p_2, \cdots, p_n$ are prime numbers, then $p_1 p_2 \cdots p_n + 1$ is also a prime number.
   D. All of the above.
   E. None of the above.

8. (2 points) Which of the following statement is true?
   - A. For $x, y \in \mathbb{Z}$, we have $\gcd(x, y) = \gcd(x + y, x - y)$
   - B. For $x, y \in \mathbb{Z}$, if $\gcd(x, y) = d$, then $\gcd(\frac{x}{d}, y) = 1$.
   - C. $\gcd(17040, 2136) = 24$.
   - D. All of the above.
   - E. None of the above.

9. (2 points) Which of the following statement is true?
   - A. $\text{lcm}(48, 27) = 1296$.
   - B. For $x, y \in \mathbb{Z}$, we have $\text{lcm}(x, y) = \text{lcm}(y, x\%y)$.
   - C. For all $x, y \in \mathbb{Z}$, if $x \mid z$ and $y \mid z$, then $\text{lcm}(x, y) \mid z$.
   - D. All of the above.
   - E. None of the above.

10. (2 points) What is $(1010101101)_2$ in base 10?
    - A. 685.
    - B. 687.
    - C. 1371.
    - D. 1375.
    - E. None of the above.

2 Structured Questions

Please provide full working in the answer script for the questions below. Omission of important working will result in loss of marks.

11. Translate the following sentences into predicate logic. Assume that the domain is the set of all human beings, that each human being can only be a male or a female. You may only use the following predicates:

    $parent(p, q)$: p is the parent of q.
    $female(p)$: p is a female.
    $p = q$: p and q are the same person.

    (a) (2 points) Joan has a daughter. (possibly more than one, and possibly sons as well)
    (b) (2 points) Kevin has no son.
    (c) (2 points) Joan has at least one child with Kevin, and no children with anyone else.

12. Study the following arguments and identify which of the following arguments are valid. For valid arguments, state the rules of inference(s) used to arrive at the conclusion. For invalid arguments, state whether the arguments exhibit the converse or inverse error.

    (a) (2 points) If Tom is not on Team A, then Hua is on team B.
    Tom is not on Team A.
    $\therefore$ Hua is on team B.

    (b) (2 points) All cheaters sit in the back row.
    Monty sits in the back row.
    $\therefore$ Monty is a cheater.

    (c) (2 points) If an infinite series converges, then its terms go to 0.
    The terms of the infinite series $\displaystyle\sum_{i=1}^{\infty} \frac{n}{n+1}$ do not go to 0.
    $\therefore$ The infinite series $\displaystyle\sum_{n=1}^{\infty} \frac{n}{n+1}$ does not converge.

13. (a) (3 points) Compute $273^{-1} \mod 997$.

    (b) (3 points) Given $a, b, n \in \mathbb{Z}^+$, suppose both a and b have multiplicative inverse modulo n. Prove that ab also has multiplicative inverse modulo n.

    (c) (2 points) Given $a, b, n \in \mathbb{Z}^+$, suppose both a and b have multiplicative inverse modulo n. Is it true that $a + b$ has multiplicative inverse modulo n?

    (d) (4 points) Given a prime p and $n \in \mathbb{Z}^+$, prove that if $n|(p-1)$ and $p|(n^2-1)$ then $p = n + 1$.

14. (a) (3 points) Suppose $a, b \in \mathbb{Z}^+$. Suppose there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Show that $\gcd(a, b) = 1$.

    (b) (3 points) Using part(a) or otherwise, show that for any $n \in \mathbb{Z}^+$, one has

$$\gcd(\ 8^n, 4^n + 2^n + 1\ ) = 1$$

15. Prove the following statements using mathematical induction.

    (a) (4 points) Prove that for all integers greater than or equal to 2, it can be expressed as a product of prime factors raised to exponents.

    (b) (6 points) A group of $n \geq 2$ badminton players play a round-robin tournament (i.e. everyone plays against everyone else once). Each game ends in either a win or a loss. Show that it is possible to label the players $P_1, P_2, \cdots, P_n$ in such as way that P_1 defeated P_2, P_2 defeated P_3, $\cdots$, and P_{n-1} defeated P_n.

3 Solutions

1. A. Construct truth table to verify the answer.

2. B.

3. B. A is wrong as the statement will become false when n is not an integer. C is wrong as $\exists m\ (m \in \mathbb{Z} \to n = 1 \times m$ holds true if $m \notin \mathbb{Z}$ regardless of whether $n = 1 \times m$.

4. E.

5. E. Negation of statement 1 is "exist a smart person who is not tall". Contrapostitive of statement 1 is "all people who are not tall are not smart". Converse of statement 1 is "all tall people are smart".

6. C. Since n^2 is non-zero, it must contain an even number of prime factors. Hence m must contain an odd number of prime factors.

7. E. $57 = 3 \times 19$ (google Grothendieck prime for an interesting backstory). $a = b = 0$ is a solution to $2^a = 5^b$. $p_1 = 3$ and $p_2 = 5$ is a counterexample to option C.

8. C. A is false by setting $x = y$. B is false by setting $x = 4, y = 2$.

9. C. A is false as $\text{lcm}(27, 48) = 432$. B is false by picking $x = y$.

10. A.

11. (a) $\exists x(female(x) \land parent(Joan, x))$

    (b) $\forall x(\neg female(x) \Rightarrow \neg parent(Kevin, x))$

    Marker's comments: I also accept $\neg\exists x(parent(Kevin, x) \land \neg female(x))$ or $\forall x(parent(Kevin, x) \Rightarrow female(x))$.

    (c) $\exists x(parent(Joan, x) \land parent(Kevin, x)) \land \forall x(parent(Joan, x) \Rightarrow parent(Kevin, x))$

12. (a) Valid: Modus ponens.

    (b) Invalid: Converse error.

    (c) Valid: Universal modus tollens.

13. (a) By Euclidean algorithm,

$$
\begin{aligned}
997 &= 3 \times 273 + 178 \\
273 &= 1 \times 178 + 95 \\
178 &= 1 \times 95 + 83 \\
95 &= 1 \times 83 + 12 \\
83 &= 6 \times 12 + 11 \\
12 &= 1 \times 11 + 1
\end{aligned}
$$

Hence $\gcd(273, 997) = 1$ and 273^{-1} exists. On the other hand,

$$\begin{aligned}
1 &= 12 - 1 \times 11 \\
&= 12 - 1 \times (83 - 6 \times 12) \\
&= -83 + 7 \times 12 \\
&= -83 + 7 \times (95 - 1 \times 83) \\
&= 7 \times 95 - 8 \times 83 \\
&= 7 \times 95 - 8 \times (178 - 1 \times 95) \\
&= -8 \times 178 + 15 \times 95 \\
&= -8 \times 178 + 15 \times (273 - 1 \times 178) \\
&= 15 \times 273 - 23 \times (178) \\
&= 15 \times 273 - 23 \times (997 - 3 \times 273) \\
&= -23 \times 997 + 84 \times 273
\end{aligned}$$

Hence the inverse of 273 modulo 997 is 84.

(b) (Proof by construction) Let a^{-1} and b^{-1} denote the inverse of a and b modulo n respectively. We claim that $b^{-1}a^{-1}$ is the inverse of ab. Indeed, we have

$$(ab)(b^{-1}a^{-1}) \equiv a(bb^{-1})a^{-1} \equiv aa^{-1} \equiv 1 \pmod n$$

(c) It is not true. Suppose we have $p = 7$, $a = 3$, $b = 4$. Both a and b have inverse modulo n because they are relatively prime to n, but $3 + 4 = 7$ does not have an inverse modulo n.

14. First we know that since $n|(p-1)$ that $p = nk + 1$, for some $k \in \mathbb{Z}^+$. We note that if $k \geq 1, nk + 1 \geq n + 1$, hence $p \geq (n+1)$. Now for the other statement, since $p|(n^2 - 1)$ it implies $p|(n+1)$ or $p|(n-1)$. We know the second one is not true since $nk+1 \geq n+1 > n-1$ for all positive integers n. Hence, it must be the case that $p|(n+1)$. This implies $p \leq n+1$. Then combining both inequalities together, we get that $p = n + 1$.

15. (a) Denote $d = \gcd(a, b)$. By definition of gcd, we note that $d \mid a$ and $d \mid b$. By theorem 4.1.1, $d \mid ax + by = 1$. Hence $d \leq 1$. Since $d = \gcd(a, b) \in \mathbb{Z}^+$, we must have $d = 1$.

(b) Note that for all $n \in \mathbb{Z}^+$, $2^n - 1 \in \mathbb{Z}$. Given any n, we have

$$8^n - (2^n - 1)(4^n + 2^n + 1) = 1.$$

Hence $\gcd(8^n, 4^n + 2^n + 1) = 1$ by part (a).

16. (a) Sketch: Prove the base case for 2, then use strong induction to show that since any integer between 2 and k can be expressed using prime factors. Then consider the $k + 1$ case. If $k + 1$ is prime, then we are done. If not, then we can find two factors a, b such that $1 < a, b < k + 1$. Both can be expressed in prime factorization form. Hence it still holds via Strong Induction.
Note : This is not the proof of the Fundamental Theorem of Arithmetic as we have not proved uniqueness!

1 mark for base case, 2 marks for induction step.

(b) Sketch: First, state the base case for $n = 1$, which is trivially true. Then, for $n + 1$ players, choose any n players and use the induction hypothesis to generate an ordering $P_1, P_2, \cdots, P_n$. Let's call the additional player P. If P lost to everyone, then place P after P_n. Otherwise by well-ordering principle, there must be a smallest integer i such P won P_i. Prove that if $i \neq 1$ then P must have lost to P_{i-1}. Hence we can simply place P in front of P_i in the new ordering.

1 mark for base case, 1 mark for using induction hypothesis, 4 marks for justifying where to place the last player.