question	1	2	3	4	5	Total
score						

MATH213 First Midterm Solution
Fall 2023

NAME: ______________________

Instructor: M. Zhang

Please answer all first *four* questions (question 5 is optional).

- You are allowed one double-sided cheat sheet.
- Show all work for full credit.
- No calculators are permitted.

Good luck!

1. (20 points) Given the following predicates,

$T(x)$: x is a tail.
$H(x)$: x is a horse.
$W(x)$: x is white.
$S(x, y)$: y is on x.
$E(x)$: x is an eye.
$F(x)$: x is a left eye.
$L(x, y)$: x is on the left side of y.

Translate the following natural language sentences to predicate logic expressions.

Example: There is a horse with two tails.
$\Longrightarrow$ $\exists h\,(H(h) \wedge \exists t_1 \exists t_2 (T(t_1) \wedge S(h, t_1) \wedge T(t_2) \wedge S(h, t_2)))$

(a) All white horses with tails have white tails.

(b) Every eye that has another eye on the left side of it is not a left eye.

(a)

$$\forall h\,[H(h) \wedge W(h) \wedge \exists t_1 (T(t_1) \wedge S(h, t_1)) \to \exists t_2 (T(t_2) \wedge S(h, t_2) \wedge W(t_2))]$$

Here's a tail issue here. There might exists a white horse with a black tail and a white tail, i.e. horses might have more than one tails, so we need t_1 and t_2 here. Also, we can't say all tails of one white horse are white.

(b)

$$\forall e_1 [E(e_1) \wedge \exists e_2 (E(e_2) \wedge L(e_2, e_1) \to \neg F(e_1)]$$

Easy one.

2. (30 points) Concepts of functions, countable and uncountable sets.

   (a) Consider the sets $A = \{a, b, c\}$ and $B = \{b, c, d, e\}$.

   - Find the Cartesian product $A \times B$.
   - Find the power set of A.

   Solution

   - $A \times B = \{(a, b), (a, c), (a, d), (a, e), (b, b), (b, c), (b, d), (b, e), (c, b), (c, c), (c, d), (c, e), (d, b), (d, c), (d,$
   - $\mathbb{P}(A) = \{, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\},.$

   Solution

   - **Cartesian Product $A \times B$:** The Cartesian product of two sets A and B, denoted as $A \times B$, is defined as the set of all ordered pairs where the first element is from A and the second element is from B. Thus, the Cartesian product $A \times B$ is given by:

     $$A \times B = \{(a, b), (a, c), (a, d), (a, e), (b, b), (b, c), (b, d), (b, e), (c, b), (c, c), (c, d), (c, e)\}.$$

     Note: The pairings such as (d, b), (d, c), (d, d), and (d, e) are not included since d is not an element of set A.
   - **Power Set of A (denoted as $\mathbb{P}(A)$):** The power set of a set A is the set of all possible subsets of A, including the empty set and A itself. For set $A = \{a, b, c\}$, the power set $\mathbb{P}(A)$ is:

     $$\mathbb{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

   (b) Just circle **True** or **False**. (4 points each)

   - (**True** / **False**) The set of all prime numbers is uncountable.
   - (**True** / **False**) The set of all rational numbers is countable.
   - (**True** / **False**) The power set of the empty set is itself.
   - (**True** / **False**) Two sets A and B have the same cardinality if there exists a one-to-one function from A to B.

3. (20 points)

   (a) Prove or disprove that $\log(n)$ is $\mathcal{O}(\sqrt{n})$.

   (b) Prove or disprove that $n2^n$ is $\mathcal{O}(2^n)$.

Solution

(a) To prove that $\log(n)$ is $\mathcal{O}(\sqrt{n})$, consider the limit:

$$\lim_{n\to\infty} \frac{\log n}{\sqrt{n}}.$$

Applying L'Hôpital's rule:

$$\lim_{n\to\infty} \frac{\log n}{\sqrt{n}} = \lim_{n\to\infty} \frac{1/n}{(1/2)n^{-1/2}} = \lim_{n\to\infty} \frac{2}{\sqrt{n}} = 0.$$

Since the limit of the ratio of $\log n$ to $\sqrt{n}$ as n approaches infinity is 0, it follows that $\log(n)$ grows asymptotically slower than $\sqrt{n}$. Therefore, $\log(n)$ is indeed $\mathcal{O}(\sqrt{n})$.

(b) Proof by Contraction

Assume for contradiction that there exists a constant $c > 0$ and $n_0 \in \mathbb{N}$ such that for all $n > n_0$:

$$n \cdot 2^n \leq c \cdot 2^n.$$

Dividing both sides by 2^n, we get:

$$n \leq c.$$

This is clearly not possible since n can be arbitrarily large, and c is a constant. Therefore, by contradiction, we conclude that $n \cdot 2^n$ is not $\mathcal{O}(2^n)$.

4. (30 points)

   (a) Use the Euclidean Algorithm to compute:

   $$\gcd(245, 63)$$

   (b) Find the solution x to the following system of congruences:

   $$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

Solution

(a) The Euclidean Algorithm is used to find the greatest common divisor (gcd) of two numbers by applying a series of divisions. We start with the two numbers, 245 and 63, and repeatedly divide the larger number by the smaller one, replacing the larger number with the remainder, until we reach a remainder of 0. The last non-zero remainder is the gcd.

$$\begin{aligned} \text{Step 1:} \quad 245 &= 63 \times 3 + 56 && \text{(Divide 245 by 63)} \\ \text{Step 2:} \quad 63 &= 56 \times 1 + 7 && \text{(Divide 63 by the remainder 56)} \\ \text{Step 3:} \quad 56 &= 7 \times 8 + 0 && \text{(Divide 56 by the remainder 7)} \end{aligned}$$

Since the remainder is now 0, we stop. The last non-zero remainder was 7.
Therefore, $\gcd(245, 63) = 7$.

(b) Given the system of congruences:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{4}$$
$$x \equiv 1 \pmod{5}$$

To solve this, we apply the Chinese Remainder Theorem. The moduli are coprime and their product is $M = 3 \times 4 \times 5 = 60$. We calculate $M_i = M/m_i$ for each modulus m_i:

$$M_1 = 60/3 = 20,$$
$$M_2 = 60/4 = 15,$$
$$M_3 = 60/5 = 12.$$

Next, we find the multiplicative inverses y_i of each M_i modulo m_i:

$$20y \equiv 1 \pmod{3}, \quad \text{so } y_1 = 2,$$
$$15y \equiv 1 \pmod{4}, \quad \text{so } y_2 = 3,$$
$$12y \equiv 1 \pmod{5}, \quad \text{so } y_3 = 3.$$

Then we compute x using the formula $x = \sum(a_i M_i y_i) \pmod{M}$:

$$x = (2 \cdot 20 \cdot 2) + (3 \cdot 15 \cdot 3) + (1 \cdot 12 \cdot 3)$$
$$x = 80 + 135 + 36$$
$$x = 251$$

Reducing x modulo M gives:

$$x \equiv 251 \pmod{60}$$
$$x \equiv 11 \pmod{60}$$

Thus, the smallest non-negative solution is $x = 11$.

Note: In applying the CRT, we first compute the product of the moduli M, then determine the multiplicative inverses of M_i modulo m_i. The final step is summing the products of the given residues, M_i, and the inverses, and then reducing the sum modulo M to find the smallest non-negative solution.

5. (Bonus 25 points) Prove that if p is a prime number, then $p^2 + 26$ is composite.

Solution

Due to the complexity of proving question, we prepared several sample answer from students. There would be a more detailed version of answer later.

Consecutive Divisible Proof

$$\begin{aligned} p^2 + 26 &= p^2 - 1 + 27 \\ &= (p-1)(p+1) + 27. \end{aligned}$$

Notice that **the product of any three consecutive integers is divisible by 3.** $(*)$ As a result, $(p-1)p(p+1)$ is divisible by 3, i.e., $3 \mid [(p-1)p(p+1)]$. Since p is a prime number, $(p-1)(p+1)$ is divisible by 3, i.e., $3 \mid [(p-1)(p+1)]$. Therefore, $3 \mid [(p-1)(p+1)+27]$, leading to the conclusion that $p^2 + 26$ has a factor of 3, and thus $p^2 + 26$ is composite.

This proof is good, but you need to prove this first to gain full mark, because the statement that the product of any three consecutive integers is divisible by 3 is indeed a mathematical fact, but it's typically not referred to as a formal theorem. It's more of a mathematical observation or property that arises from the nature of integer sequences and divisibility rules.

Proof for $(*)$: Consider any three consecutive integers, represented as n, $n+1$, and $n+2$, where n is any integer.

We examine the three cases regarding divisibility by 3:

(a) If n is divisible by 3: In this case, n is a multiple of 3, so the product $n \times (n+1) \times (n+2)$ will also be divisible by 3, as it contains n, which is a multiple of 3.

(b) If n is not divisible by 3, but $n+1$ is: Here, $n+1$ is a multiple of 3. Thus, the product $n \times (n+1) \times (n+2)$ will be divisible by 3, as it contains $n+1$, a multiple of 3.

(c) If neither n nor $n+1$ is divisible by 3, then $n+2$ must be: After two consecutive integers that are not divisible by 3, the next integer must be divisible by 3. Hence, in this case, $n+2$ is a multiple of 3, making the product $n \times (n+1) \times (n+2)$ divisible by 3.

In each case, at least one of the integers n, $n+1$, or $n+2$ is divisible by 3, ensuring the product of these three consecutive integers is always divisible by 3.

Proof by Cases

Base Cases:

1. If $p = 2$, then $p^2 + 26 = 30$ which is composite.
2. If $p = 3$, then $p^2 + 26 = 35$ which is composite.

General Case for $p > 3$:

Consider p as a prime greater than 3. We analyze the cases based on the congruence of p modulo 3. Since p is prime and greater than 3, $p \neq 3k$ (where $k \geq 1$) as that would make p composite. Therefore, p must be of the form $3k + 1$ or $3k + 2$.

Case 1: $p = 3k + 1$

$$\begin{aligned} p^2 + 26 &= (3k + 1)^2 + 26 \\ &= 9k^2 + 6k + 1 + 26 \\ &= 9k^2 + 6k + 27 \\ &= 3(3k^2 + 2k + 9), \end{aligned}$$

which is divisible by 3 and thus composite.

Case 2: $p = 3k + 2$

$$\begin{aligned} p^2 + 26 &= (3k + 2)^2 + 26 \\ &= 9k^2 + 12k + 4 + 26 \\ &= 9k^2 + 12k + 30 \\ &= 3(3k^2 + 4k + 10), \end{aligned}$$

which is also divisible by 3 and therefore composite.

Conclusion:

For any prime p greater than 3, $p^2 + 26$ is always divisible by 3, hence composite. Combining this with the base cases, we conclude that for any prime number p, $p^2 + 26$ is always composite.

Thus, the statement is proven.

Proof by Contradiction

Assume for the sake of contradiction that p is a prime number and $p^2 + 26$ is also prime.

We know that for any prime $p > 3$, p^2 is congruent to 1 modulo 3. This is because all primes greater than 3 can be written in the form $6k \pm 1$, and squaring these gives $36k^2 \pm 12k + 1$, which leaves a remainder of 1 when divided by 3.

Therefore, $p^2 + 26$ will be congruent to $1 + 26$ modulo 3, which simplifies to 27 modulo 3, and hence is 0 modulo 3. This means $p^2 + 26$ is divisible by 3 for any prime $p > 3$, and thus cannot be prime itself.

This leads to a contradiction since we have assumed $p^2 + 26$ is prime, but have shown that it must be composite as it is divisible by 3 for any prime $p > 3$.

Hence, the assumption must be incorrect, and then we prove: if p is a prime number, then $p^2 + 26$ is composite.

Other correct solution

(a) Fermat's Little Theorem can also prove, but you need to prove it first.

(b) Counting last digit and prove by case can also works. And you must discuss each last digit case clearly, each one deserves for 5 pts.