MAT102F - Intro. to Mathematical Proofs - Fall 2019 - UTM

Exam Jam! - Solutions

MCQ

1. Suppose $f : A \to B$ and $g : B \to C$ are functions and $g \circ f$ is injective. Which of the following statement is always true?

   (a) f is injective. (b) g is injective. (c) $A = C$

   Solution. a. Proof is by contrapositive. Suppose f is not injective. So there are $a, b \in A$ with $a \neq b$ and $f(a) = f(b)$. Therefore $g \circ f(a) = g \circ f(b)$. So $g \circ f$ is not injective.
   b. is not correct as the witness to non-injectivity of g could happen on $B \setminus \operatorname{ran}(f)$. c. is not correct as the codomain of g could be very large.

2. Suppose S is a statement form with n variables $P_1, P_2, \ldots, P_n$, where $n \geq 3$. In exactly how many rows of the truth table for S is P_1 false?

   (a) 1. (b) 2. (c) 2^{n-1}. (d) 2^n.

   Solution. c. There are n columns, one for each variable, and there are 2^n total possible assignments of True/False to the variables. This gives 2^n rows. In exactly half of them, P_1 is false. Half of 2^n is 2^{n-1}.

3. Suppose S is a statement form with n variables $P_1, P_2, \ldots, P_n$, where $n \geq 4$. In exactly how many rows of the truth table for S is P_1 false while P_2 is true?

   (a) 1. (b) 2. (c) 2^{n-1}. (d) 2^{n-2}.

   Solution. d. Similar to the previous question, the condition on P_1 halves the number of possibilities, and the condition on P_2 halves it again. So the answer is $\frac{2^n}{4} = 2^{n-2}$.

4. Which statement is a tautology?

   (a) $P \implies (P \implies Q)$

   (b) $(P \wedge Q) \implies (P \vee R)$

   (c) $(P \implies Q) \iff Q$

   (d) $(P \implies Q) \implies Q$

   Solution. b. This can be solved by truth table, or notice that the implication is vacuously true unless $P \wedge Q$ is true. That only happens when P is true. So $P \vee R$ will be true, and the implication will be true.

5. Which of the following statement is always true?

(a) $\{1, 2, 3\} = \{2, 1, 3, 3, 2\}$

(b) $\{5, \emptyset\} = \{5\}$

(c) $\{5\} \in \{2, 5\}$

(d) $\{1, 2\} \subseteq \{3, \{1, 2\}\}$

Solution. a. Sets do not care about repeated elements.

6. Given two sets A and B, which of the following 2 statements are always true?

(a) $P(A \cup B) = P(A) \cup P(B)$.

(b) $\emptyset \notin P(A) \setminus P(B)$.

(c) $P(A \cap B) \subseteq P(A) \cap P(B)$.

(d) $P(A \setminus B) \neq P(A)$.

Solution. b. Fact: $\forall X, \emptyset \subseteq X$, so $\emptyset \in P(X)$.
c. If $X \in P(A \cap B)$, then $X \subseteq A \cap B$, so $X \subseteq A$ and $X \subseteq B$. So $X \in P(A)$ and $X \in P(B)$. So $X \in P(A) \cap P(B)$.
a. is false if $A \neq B$. d. is false if $A \cap B = \emptyset$.

7. How many zeroes would appear on the right side of the number $N = 100!$?

(a) 24 (b) 25 (c) 26 (d) 20

Solution. a. This question is equivalent to "how many factors of 10 does N have?", and in fact is equivalent to "how many factors of 5 does it have?".
It has 1 for each multiple of 5 (20 total), and 1 additional factor for each multiple of 25 (4 total). That makes 24 total.

8. Given $|S| = m$ and $|T| = n$ where S and T are two sets, how many functions are there with domain S and codomain T?

(a) n^m (b) m^n (c) mn (d) $m + n$

Solution. a. This is a generaliztion of a PS5 question. It might be easier to think of these functions as strings, or License plates.
Each element of S has n choices. This is repeated m times, independently. So n^m total functions.

Long Answers

1. Prove that every integer n satisfies the congruence $n^3 \equiv n \pmod 6$.

Solution. Run through the possibilities $n = 0, 1, 2, 3, 4, 5$. Which gives n^3 is: $0, 1, 8 = 6 + 2 \equiv 2, 27 = 24 + 3 \equiv 3, 64 = 60 + 4 \equiv 4, 125 = 120 + 5 \equiv 5$.

2. Given $(k, m) = 1$, show that the following cancellation law holds:

$$ka \equiv kb \pmod m \implies a \equiv b \pmod m$$

Use this result, prove every integer is congruent modulo m to exactly one of the integers

$$0, k, 2k, \ldots, (m-1)k.$$

Solution. Suppose that $(k, m) = 1$ and $ka \equiv kb \pmod m$. By definition, $m|ka - kb$. So $m|k(a - b)$. Since $(k, m) = 1$, we must have $m|(a - b)$. So $a \equiv b \pmod m$.
[Existence] ???
[Uniqueness] Suppose that $ak \equiv bk \pmod m$ with $0 \leq a, b < m$. Then by the above result $a \equiv b \pmod m$, so by the restriction $0 \leq a, b < m$ we must have $a = b$. So $ak = bk$.

3. Suppose that $f : \{1, 2, \ldots, 2019\} \to \{0, 1\}$ is a function such that $f(1) = 0$ and $f(2019) = 1$. Prove that there is an $k \in \{1, 2, \ldots, 2019\}$ such that $f(k) = 0$ and $f(k + 1) = 1$.

Solution. Suppose for the sake of contradiction that this is not true. So then $f(k) = 0 \implies f(k+1) = 0$ for all $k \in \{1, 2, \ldots, 2018\}$. Since $f(1) = 0$, by induction we must have $f(2019) = 0$, a contradiction.

4. Let A be a set.
   (a) Prove that $R = A \times A$ is an equivalence relation on A.
   (b) Prove that $S = \{(a, a) : a \in A\}$ is an equivalence relation on A.
   (c) For the above relations, is $R \subseteq S$, $S \subseteq R$ or neither?

Solution. a. Reflexive: Suppose $a \in A$, so $(a, a) \in A \times A = R$.
Symmetric: If $(x, y) \in R = A \times A$, then $x \in A$ and $y \in A$, so $(y, x) \in A \times A = R$.
Transitive: Suppose $(x, y) \in R$ and $(y, z) \in R$. So $x, y, z \in A$. So $(x, z) \in A \times A = R$.

Solution. b. Reflexive and symmetric are obvious, by definition. If $(x, y), (y, z) \in S$, then $x = y$ and $y = z$. So $(x, z) = (x, y) \in S$.

Solution. c. $S \subseteq R$. Let $x \in S$. Then $x = (a, a)$ for some $a \in A$. Since R is an equivalence relation, it is reflexive. So $x = (a, a) \in R$.

5. Show that the set $\mathbb{N} \times \mathbb{N}$ can be expressed as the union of a countably infinite family of countably infinite sets.

Solution. For $n \in \mathbb{N}$, let $A_n = \{n\} \times \mathbb{N}$. the set of all pairs with n as its first coordinate. Clearly $A_1 \cup A_2 \cup \ldots = \mathbb{N} \times \mathbb{N}$. Also, for each n, there is an obvious bijection $f_n : \mathbb{N} \to A_n$, namely $f_n(x) = (n, x)$.

6. Define $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$:

$$g(m, n) = 2^{m-1}(2n - 1)$$

Show that g is a bijection. What does it say about the cardinality of $\mathbb{N} \times \mathbb{N}$?

Solution. I'm not going to write the whole proof here. Notice that on PS4 they proved that every number can be written in the form 2^{m-1}(odd), so that gives them the surjectivity part of this argument. Injectivity is by the Fundamental theorem of arithmetic. This proves that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, i.e. $\mathbb{N} \times \mathbb{N}$ is countable.

7. A set A is <u>defined</u> to be "Dedekind infinite" if there exists an injection $f : A \to A$ that is not a surjection.

   (a) Prove that $\mathbb{N}$ and $\mathbb{R}$ are Dedekind infinite.

   (b) Prove that $\{1\}$ is not Dedekind infinite.

   (c) (**Challenge!**) Prove by induction that for all $n \in \mathbb{N}$ that $\{1, \ldots, n\}$ is not Dedekind infinite.

Solution. a. The function $f : \mathbb{N} \to \mathbb{N}$ given by $f(n) = n+1$ is clearly an injection that is not a surjection. For $\mathbb{R}$ we can use e^x or $\arctan(x)$, or some CSB argument that gives us a bijection $\mathbb{R}$ to an interval.

Solution. b. Suppose that $f : \{1\} \to \{1\}$ is a function. Then $f(1)$ is defined, and must be $\{1\}$. So f is a bijection.

Solution. c. The previous question is the base case. Suppose for the sake of contradiction that $P(n)$ is true, but $P(n + 1)$ is false. Let $f : \{1, \ldots, n + 1\} \to \{1, \ldots, n + 1\}$ be an injection that is not a surjection.
Case 1. Suppose $f(n + 1) = n + 1$. Note $\exists N \leq n$ with $f(x) \neq N$ for all $x \in \{1, \ldots, n\}$. Then f restricted to $\{1, \ldots, n\}$ is still an injection, and still is not a surjection since it still misses N.
Case 2. Suppose $f(n + 1) = N < n + 1$.
Case 2.1 If there is no x with $f(x) = n + 1$, then define the function $g : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $g(k) = f(k)$ is still an injection, and it is a surjection because the only $f(k) = N$ is $f(n + 1)$. So there is no $g(k) = N$.
Case 2.2. If there is an $x \leq n$ with $f(x) = n + 1$, then define the function $g : \{1, \ldots, n\} \to \{1, \ldots, n\}$ by $g(k) = f(k)$, unless $k = x$, in which case $g(x) = N$. This is still an injection, and it is not a surjection because it misses the same points in $\{1, \ldots, n\}$ that f missed.