CSE 20, Fall 2020 - Midterm 2 Review Solutions

Question 1

Prove that for any real number $x > -1$, and any positive integer n, $(1+x)^n \geq 1+nx$.

Solution:

Towards a proof by mathematical induction for n:

Base Case: For $n = 1$, $LHS = (1+x)^n = (1+x)^1 = 1+x$

$RHS = (1+nx) = 1+1.x = 1+x$

Therefore, $LHS = RHS$

Inductive Hypothesis: For a positive integer k, we assume that $(1+x)^k \geq 1+kx$.

We need to show that $(1+x)^{k+1} \geq 1+(k+1)x$

$LHS = (1+x)^{k+1} = (1+x)^k(1+x)$

From the IH, we know that: $(1+x)^k \geq 1+kx$

Therefore:

$(1+x)^k(1+x) \geq (1+kx)(1+x)$

$\Rightarrow (1+x)^k(1+x) \geq 1+(k+1)x+kx^2$

Since $x^2 > 0$, and $k > 0$, $kx^2 > 0$

Therefore, $(1+x)^{k+1} \geq 1+(k+1)x$

Hence Proved.

Question 2

Let U be the universal set, and let $A, B \text{ and } C$ be sets. Use the definition of set equality to prove: $A-(B \cup C) = (A-B)-C$

Solution:

Recall that for two sets to be equal

$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$

Therefore, $A-(B \cup C) = (A-B)-C$ if and only if $A-(B \cup C) \subseteq (A-B)-C$ and $(A-B)-C \subseteq A-(B \cup C)$

To prove that $A-(B \cup C) \subseteq (A-B)-C$

Assume that $x \in A - (B \cup C)$. We need to show that $x \in (A - B) - C$

$x \in A - (B \cup C) \Rightarrow x \in A \wedge \neg(x \in (B \cup C))$ (from the definition of set difference)

$\Rightarrow x \in A \wedge \neg(x \in B \vee x \in C)$

$\Rightarrow x \in A \wedge (\neg(x \in B) \wedge \neg(x \in C))$ (De-Morgan's law)

$\Rightarrow x \in A \wedge (x \notin B) \wedge (x \notin C)$

$\Rightarrow (x \in A \wedge (x \notin B)) \wedge (x \notin C)$

$\Rightarrow x \in (A - B) \wedge x \notin C$

$\Rightarrow x \in (A - B) - C$

Therefore, $x \in A - (B \cup C) \Rightarrow x \in (A - B) - C$

$A - (B \cup C) \subseteq (A - B) - C$

To prove that $(A - B) - C \subseteq A - (B \cup C)$

Assume that $x \in (A - B) - C$. We need to show that $x \in A - (B \cup C)$

$x \in (A - B) - C \Rightarrow (x \in (A - B)) \wedge (x \notin C)$

$\Rightarrow (x \in A \wedge x \notin B) \wedge (x \notin C)$

$\Rightarrow x \in A \wedge x \notin B \wedge x \notin C$

$\Rightarrow x \in A \wedge (x \notin B \wedge x \notin C)$

$\Rightarrow x \in A \wedge (\neg(x \in B) \wedge \neg(x \in C))$

$\Rightarrow x \in A \wedge \neg((x \in B) \vee (x \in C))$

$\Rightarrow x \in A \wedge \neg(x \in (B \cup C)$

$\Rightarrow x \in A \wedge x \notin (B \cup C)$

$\Rightarrow x \in (A - (B \cup C))$

Therefore, $x \in (A - B) - C \Rightarrow x \in A - (B \cup C)$

$(A - B) - C \subseteq A - (B \cup C)$

Since, $A - (B \cup C) \subseteq (A - B) - C$ and $(A - B) - C \subseteq A - (B \cup C)$

Therefore, $A - (B \cup C) = (A - B) - C$

Hence proved.

Question 3

If $n \bmod 3 = 2$, then show that $n^2 + 2n$ is not divisible by 3.

Solution:

Towards a direct proof:

$n \bmod 3 = 2$. Therefore, we can write $n = 3k + 2$, where $k \in Z^+$

Therefore,

$$
\begin{aligned}
n^2 + 2n &= (3k+2)^2 + 2(3k+2) \\
&= 9k^2 + 12k + 4 + 6k + 4 \\
&= 9k^2 + 18k + 8 \\
&= (9k^2 + 18k + 6) + 2 \\
&= 3(3k^2 + 6k + 2) + 2 \\
&= 3l + 2
\end{aligned}
$$

Where, $l = 3k^2 + 6k + 2$ is an integer

Therefore, $n^2 + 2n = 3l + 2$, which is not divisible by 3.
Hence proved!

Question 4

For each of the following relations R on the given domain A, categorize them as one of the following:

- Not an equivalence relation
- An equivalence relation with finitely many distinct equivalence classes
- An equivalence relation with infinitely many distinct equivalence classes

a) $A = \{1, 2, 3\},\ R = \{(1,1), (2,2), (3,3)\}$
b) $A = \Re,\ R = \{(x,y) | x^2 = y^2\}$
c) $A = Z \times Z^*,\ R = \{((a,b),(c,d)) \mid ad = bc\}$, where Z^* are the set of non-zero integers

Solution:

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

Equivalence Relation with finitely many equivalence classes.

- Reflexive: This is trivially true since the relation contains all tuples of the form $(n,n),\ where\ n \in A$
- Symmetric: Again, this is also trivially true for each of the tuples $\{(1,1), (2,2), (3,3)\}$
- Transitive: Since there are no tuples of the form (a,b), the transitivity property is also trivially satisfied.

The three equivalence classes are $\{1\}, \{2\}, \{3\}$

b) $A = \Re,\ R = \{(x,y) | x^2 = y^2\}$

Equivalence Relation with infinitely many equivalence classes.

- Reflexive: $For\ all\ x \in \Re, x^2 = x^2$ .Therefore, $(x,x) \in R$.
- Symmetric: $For\ all\ x,y \in \Re$, if $(x,y) \in R,\ then\ x^2 = y^2$. This implies that $y^2 = x^2$, which in turn implies that $(y,x) \in R$
- Transitive: $For\ all\ x,y,z \in \Re$, if $(x,y) \in R \wedge (y,z) \in R$. Then $x^2 = y^2 = z^2$ which implies that $x^2 = y^2 = z^2$, which in turn implies that $(x,z) \in R$

For each positive real number, we get a distinct equivalence class containing $\{r, -r\}$. We also have an equivalence class $\{0\}$.

c) $A = Z \times Z^*,\ R = \{((a,b),(c,d)) \mid ad = bc\}$, where Z^* are the set of non-zero integers

Equivalence Relation with infinitely many equivalence classes.

- Reflexive: $For\ all\ (a,b) \in Z \times Z^*$, if $a = c$ and $b = d$, then we get $ab = ba$. Therefore, $((a,b),(a,b)) \in R$. Therefore, R is reflexive.
- Symmetric: $For\ all\ (a,b),\ (c,d) \in Z \times Z^*$, if $((a,b),(c,d)) \in R$ then $ad = bc$. This is equivalent to writing $cb = da$. Therefore, $((c,d),(a,b)) \in R$. Therefore, R is symmetric.
- Transitive: $For\ all\ (a,b),\ (c,d),\ (e,f) \in Z \times Z^*$, if $((a,b),(c,d)) \in R$ and $((c,d),(e,f)) \in R$, then $ad = bc \Rightarrow c = \frac{ad}{b}$ and $cf = de \Rightarrow c = \frac{de}{f}$. This implies that: $\frac{ad}{b} = \frac{de}{f} \Rightarrow af = be$. Therefore, $((a,b),(e,f)) \in R$. hence, the transitivity property is satisfied.

Therefore, we see that the relation is satisfied by all tuples whose ratio is the same: $i.e.\ \frac{a}{b} = \frac{c}{d}$. Therefore, the equivalence classes are formed of the fractions $\frac{a}{b}$ in the simplified form, where $gcd(a,b) = 1$. Since there are infinitely many fractions, there are infinitely many equivalence classes.

Question 5

Calculate $7^{15420}\ mod\ 13$.

- 7^0 mod 13 = 1, 7^1 mod 13 = 7, 7^2 mod 13 = 10, 7^3 mod 13 = 5… keep following the pattern, and we get 7^{12} mod 13 = 1, so the pattern repeats for 7^0 up to 7^{12}
- 15420 mod 12 = 0
- 15420 == 12**k* + *j* for some integers
- $7^{15420} == (7^{12})^k * 7^j$
- $7^{15420} == (7^{12})^k * 7^j$ mod 13
- $(1^k * 7^j)$ mod 13 == $(1^k * 7^0)$ mod 13 == 1 == 7^{15420} mod 13

Question 6

Prove that for three integers $a, b\ and\ c$, if c does not divide $a \times b$ then c does not divide a and c does not divide b.

Proof by Contraposition

- Assume that *c* does divide *a* or *c* does divide *b*, then *c* does divide *a*b*.
- Since c divides *a* or *b*, that means that either *a* mod *c = 0*, or *b* mod *c = 0.*
- Modular multiplication: for *x,y*, *x* mod *c * y* mod *c == x*y* mod *c*
- This means that *a*b* mod *c = 0* mod *c*
- This means that *a*b = k * c* for some integer *k*, which means that *c* divides *a*b* by

definition
- Q.E.D.

Question 7

For $f_1, f_2 : A \to B$ and $g : B \to C$, prove that if *g* is injective and $g(f_1(x)) = g(f_2(x))$ for all $x \in A$, then $f_1 = f_2$.

Definition of injective: if g(x) == g(y), then x == y.
Proof by contradiction. Assume that there f_1 != f_2. This means that there is exists some value where $f_1(x) != f_2(x)$. However, we know that $g(f_1(x)) = g(f_2(x))$, and since *g* is injective, that means $f_1(x) == f_2(x)$.

Direct proof version
- *g* is injective, g($f_1(x)$) = g($f_2(x)$) for x ∈ A
- $f_1(x) == f_2(x)$ for x ∈ A
- $f_1 == f_2$