SPRING 2018 MATH 300 FINAL EXAM

Write clearly and legibly. Justify all your answers.
You will be graded for correctness and clarity of your solutions.
You may use one 8.5 x 11 sheet of notes; writing is allowed on both sides. You may use a calculator.
You can use elementary algebra and any result that we proved in class (but not in the homework). You need to prove everything else.
Please raise your hand and ask a question if anything is not clear.
This exam contains 9 pages and is worth a total of 70 points. You have 1 hr and 50 minutes. Good luck

NAME:_________

PROBLEM 1 (8 points) _______

PROBLEM 2 (6 points) _______

PROBLEM 3 (8 points) ________

PROBLEM 4 (12 points) ________

PROBLEM 5 (8 points) ________

PROBLEM 6 (8 points) ________

PROBLEM 7 (12 points) ________

PROBLEM 8 (8 points) ________

Total ____________

f

- **Problem 1** Given sets A, B, C in some universe U prove that

$$(A - (B \cup C))^c = (A - B)^c \cup (A - C)^c.$$

First we shall prove $(A - (B \cup C))^C \subseteq (A-B)^C \cup (A-C)^C$: assume
$x \in (A - B \cup C)^C$, then $x \notin A - (B \cup C)$ so $x \notin A \vee x \in B \cup C$
if $x \notin A$ then $x \notin A - B$ so $x \in (A-B)^C$ so $x \in (A-B)^C \cup (A-C)^C$
if $x \in B \cup C$ then $x \in B$ or $x \in C$; if $x \in B$ then $x \notin A - B$ so again
$x \in (A-B)^C \cup (A-C)^C$; if $x \in C$ then $x \notin A - C$ so $x \in (A-C)^C$ and
therefore $x \in (A-B)^C \cup (A-C)^C$

Now we shall prove $(A-B)^C \cup (A-C)^C \subseteq (A - (B \cup C))^C$:
assume $x \in (A-B)^C \cup (A-C)^C$; then $x \in (A-B)^C$ or $x \in (A-C)^C$;
if $x \in (A-B)^C$ then $x \notin A-B$ so $x \notin A$ or $x \in B$
if $x \notin A$ then $x \notin A - (B \cup C)$ so $x \in (A - (B \cup C))^C$
if $x \in B$ then $x \in B \cup C$ so $x \notin A - (B \cup C)$ so $x \in (A - (B \cup C))^C$
if $x \in (A-C)^C$ the argument is similar

- **Problem 2** Write a statement equivalent to the negation of

$$\exists x \in A \, \forall y \in B \, (x \leq y) \Rightarrow (\exists z \in C \, (z > x) \Rightarrow (z > y \wedge z = y))$$

that does not use the negation symbol $\neg$

My mistake for not using enough parentheses

Some people read it as

$\forall x \in A \; \exists y \in B \; (x \leq y \Rightarrow \cdots\cdots\cdots)$

Negation

$\forall x \in A \; \exists y \in B \quad x \leq y \wedge (\forall z \in C \quad z > x \wedge (x \leq y \vee z \neq y))$

other as

$(\forall x \in A \; \exists y \in B \; x \leq y) \Rightarrow \cdots\cdots$

Negation

$\forall x \in A \; \exists y \in B \; x \leq y \wedge \forall z \in C \; z > x \wedge (z \leq y \vee z \neq y)$

- **Problem 3** Prove or disprove $\forall a \in Z$, $\frac{a^2-a}{2}$ is even if and only if a or $a-1$ are divisible by 4 .

$\frac{a^2-a}{2} = 2k$ for some $k \in Z \iff a \equiv 0$ or $a \equiv 1 \mod 4$ is true

Note $\frac{a^2-a}{2} = 2k$ for some $k \iff a^2-a = 4k \iff a^2-a \equiv 0 \mod k$

First prove $a \equiv 0 \vee a \equiv 1 \mod \Rightarrow a \equiv 0 \mod 4$

if $a \equiv 0 \mod 4$ then $a^2-a \equiv 0^2-0 \equiv 0 \mod 4$
if $a \equiv 1 \mod 4$ then $a^2-a \equiv 1^2-1 \equiv 0 \mod 4$

Then prove $a^2-a \equiv 0 \mod 4 \Rightarrow (a \equiv 0 \vee a \equiv 1 \mod 4)$

By contreposition
if $a \equiv 2 \mod 4$ $a^2-a \equiv 4-2 \equiv 2 \not\equiv 0 \mod 4$
if $a \equiv 3 \mod 4$ $a^2-a \equiv 9-3 \equiv 2 \not\equiv 0 \mod 4$

- **Problem 4** A student is trying to prove that the set A $=\{S|S \subseteq N$ and $|S| = 2\}$ (that is A is the set of all subsets of N that have exactly two elements) is denumerable . Below are some of his attempts to find a bijection f between A and a denumerable set. For each function f that the student has tried to define below say whether it is a well defined function that is a bijection or not. If it is not, explain why.

  - $fA \to N \times N \quad f(\{x, y\}) = (x, y)$

Not well defined; elements of a set are not ordered so is $f(\{1,2\}) = (1,2)$ or $(2,1)$?

  - $fA \to N \times N \quad f(\{x, y\}) = (min(x, y), max(x, y))$

Not surjective since for exemple $(2,1) \notin Im(f)$

  - $fA \to N \quad f(\{x, y\}) = x + y$

Not injective $f(\{1,6\}) = f(\{3,4\})$

- **Problem 5** Consider the sequence $\{a_n\}$ defined by:

  $a_1 = \cancel{0}\ 3$

  $a_2 = 2$

  $a_3 = \cancel{3}\ -3$

  $a_{n+1} = 4a_n - 5a_{n-1} + 2a_{n-2}$ if $n + 1 \geq 4$

  Prove that $\forall n \geq 1$, $a_n = 3n + 4 - 2^{n+1}$

By induction on n

Base case

If $n = 1$ then $3 + 4 - 4 = 3$

If $n = 2$ then $6 + 4 - 8 = 2$

If $n = 3$ then $9 + 4 - 16 = -3$

Induction step: assume the formula above is true for a_{k-2}, a_{k-1} and a_k, for some $k \geq 3$, then $a_{k+1} = 4a_k - 5a_{k-1} + 2a_{k-2} =$

$$= 4\left(3k + 4 - 2^{k+1}\right) - 5\left(3(k-1) + 4 - 2^k\right) + 2\left(3(k-2) + 4 - 2^{k-1}\right)$$

$$= 12k - 15k + 6k + 16 + 15 - 12 - 20 + 8 - 4 \cdot 2^{k+1} + 5 \cdot 2^k - 2^k$$

$$= 3k + 7 - 2 \cdot 2^{k+2} + 2^{k+2} = 3(k+1) + 4 - 2^{k+1+1}$$

- **Problem 6** Solve $3 \cdot 7^{1000} x \equiv 2005 \bmod 10$

$7^{1000} = (49)^{500} \equiv (9)^{500} \equiv (-1)^{500} \equiv 1 \bmod 10$

$2005 \equiv 5 \bmod 10$

$3x \equiv 5 \bmod 10$

by trial and error $x = 5$

So all integer solutions are $x = 5 + 10k \quad k \in \mathbb{Z}$

- **Problem 7** An equivalence relation R on a set A is a subset of $A \times A$ that has the following properties; complete the sentences below :
  - Reflexive, that is $\forall a \in A \quad aRa \quad$ or $(a,a) \in R$
  - Symmetric, that is $\forall a,b \in R \quad aRb \Rightarrow bRa \quad$ or $(a,b) \in R \Rightarrow (b,a) \in R$
  - Transitive, that is $\forall a,b,c \in R \quad (aRb \wedge bRc) \Rightarrow aRc$
    $(a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$

Given that R_1 and R_2 are two equivalence relations on a set A , prove that $R_1 \cap R_2$ is an equivalence relation on A.

We need to show $R_1 \cap R_2$ is reflexive
Given $a \in A$, since $(a,a) \in R_1$ and $(a,a) \in R_2$ then $(a,a) \in R_1 \cap R_2$ so $R_1 \cap R_2$ is reflexive
Given $a,b \in A$ if $(a\ b) \in R_1 \cap R_2$ then $(ab) \in R_1$ so $(ba) \in R_1$ and $(a\ b) \in R_2$ so $(b\ a) \in R_2$, therefore $R_1 \cap R_2$ is symmetric
Given $a,b,c \in A$ if $(a,b) \in R_1 \cap R_2$ and $(b,c) \in R_1 \cap R_2$ then $(a,b) \in R_1$ and $(b,c) \in R_1$ so $(a,c) \in R_1$ and $(a,b) \in R_2 \wedge (b,c) \in R_2$ so $(a,c) \in R_2$
so $(a,c) \in R_1 \cap R_2$ so $R_1 \cap R_2$ is transitive.

If R_1 is $\equiv$ mod 4 in $\mathbb{Z}$ and R_2 is $\equiv$ mod 6 in $\mathbb{Z}$ $\quad a R_1 \cap R_2 b$
$\Leftrightarrow$ 4 div $b-a$ $\wedge$ 6 div $b-a$ so $R_1 \cap R_2$ is $\equiv$ mod 12
since $b - a = 4k = 6h$ for some $h,k \in \mathbb{Z}$ $\Rightarrow 2k = 3h$ so h is even
therefore $h = 2l$ for some $l \in \mathbb{Z}$ and $b - a = 6 \cdot 2\ l$ so $b \equiv a$ mod 12
viceverse if $b \equiv a$ mod 12 $b-a = 12k$ for some $k \in \mathbb{Z}$ so 4 div $b-a$ $\wedge$ 6 div $b-a$, so $a \equiv b$ mod 4 and $a \equiv b$ mod 6

$R_1 \cup R_2$ is not an equivalence relation since
$2 \equiv 6$ mod 4 and $6 \equiv 0$ mod 6 so $(2,6) \in R_1 \cup R_2$ and $(6,0) \in R_1 \cup R_2$
but $2 \not\equiv 0$ mod 4 or 6 So $(2,0) \notin R_1 \cup R_2$

prove that $1^{-1} = 1$ and $(p-1)^{-1} = p-1$ 2
prove that $x^{-1} = x \Rightarrow x = 1 \vee x = \ldots$ 4
$x \cdot x \equiv 1 \mod p$
$(x^2 - 1)$

Give an example that shows 2 is not true if p is not prime

$\cancel{5}^{-1} = 5$ in Z_{12} 3

- **Problem 8** Given $m \in Z, m > 1$, prove that

$$\forall a \in Z, \forall b \in Z, \forall c \in Z,\ a \equiv b \bmod m \Rightarrow ca \equiv cb \bmod m$$

.

Assume $a \equiv b \mod m$ then m div $a-b$ so
$a - b = mk$ for some $k \in Z$ therefore
$ca - cb = m(ck)$ and so $ca \equiv cb \mod m$

Is the converse true ? That is prove or disprove that

$$\forall a \in Z, \forall b \in z, \forall c \in Z,\ ca \equiv cb \bmod m \Rightarrow a \equiv b \bmod m$$

No $c = 0$ is a problem, but even if we let $c \neq 0$
$3 \cdot 2 \equiv 3 \cdot 4 \mod 6$ but $2 \not\equiv 4 \mod 6$

- **Problem 8** Given $m \in Z, m > 1$, recall that for $a \in Z_m$ we denote by a^{-1} the inverse of a in Z_m.
  - Show that $1^{-1} = 1$ and $(m-1)^{-1} = m-1$ in Z_m , that is 1 and $m-1$ are their own inverse in Z_m.

$1 \cdot 1 = 1 \equiv 1 \mod m$

$(m-1)(m-1) = m^2 - 2m + 1 \equiv 1 \mod m$

  - Prove that, if m is prime, 1 and $m-1$ are the only elements of Z_m that are their own inverse (Hint : x is its own inverse if $x^2 \equiv 1$ mod m)

$x^2 \equiv 1 \mod m \iff m \text{ div } x^2 - 1 = (x+1)(x-1) \Rightarrow$ (since m is prime) $m \text{ div } (x+1)$ or $m \text{ div } (x-1) \iff$

$x \equiv -1 \equiv m-1 \mod m$ or $x \equiv 1 \mod m$

  - Give an example to show that, if m is not prime, there maybe elements $a \in Z_m$ such that $a = a^{-1}$ and $a \neq 1$ and $a \neq m-1$

$3 \cdot 3 \equiv 1 \mod 8$ so $3 = 3^{-1}$ in Z_8