Math 300 Section 2 Final Exam Spring 2016

Name: Solution Scheme

Justify **all** your work!

1. (a) (5 points) Let the universe of discourse be the real numbers. Prove or disprove the following statement.

$$\exists x\ \forall y\ ((x+y)^2 + 5(x+y) + 6 > 0).$$

The statement is False. We will prove it negation

(*) $\forall x\ \exists y\ \left((x+y)^2 + 5(x+y) + 6 \leq 0\right)$

Indeed, $z^2 + 5z + 6 = (z+2)(z+3) \leq 0$ for $\boxed{-3 \leq z \leq -2}$.

Given x, set $y(x) := -2 - x$. Then

$x + y(x) = x + (-2-x) = -2$ and so

$(x + y(x))^2 + 5(x + y(x)) + 6 = 0.$

Hence, for every x there exist y (take $y(x) = -2-x$) such that $(x+y)^2 + 5(x+y) + 6 \leq 0.$

(b) (5 points) Let the universe of discourse be the positive integers. Write the contrapositive of the following statement.
If $p|ab$, then ($p|a$ OR $p|b$).

If $\underbrace{\text{Not}(p|a \text{ OR } p|b)}_{p\nmid a \text{ AND } p\nmid b}$, then $p \nmid ab$

If $p \nmid a$ AND $p \nmid b$, then $p \nmid ab$.

2. (a) (10 points) Let X be a set, $S \subset X$ a subset, and $S^c := \{x \in X \ : x \notin S\}$ the complementary subset. Assume that $\sharp(S) = \sharp(\mathbb{P})$ and $\sharp(S^c) = \sharp(\mathbb{P})$, i.e., the cardinalities of both S and S^c are equal to the cardinality of the set $\mathbb{P}$ of positive integers. Prove that $\sharp(X) = \sharp(\mathbb{P})$.
Hint: By assumption, there exist bijections $f : S \to \mathbb{P}$ and $g : S^c \to \mathbb{P}$. Use them to construct a bijection $h : X \to \mathbb{P}$. **Prove** that your h is bijective.

both x_1, x_2 belong to S or both belong to S^c.

Define $h(x) = \begin{cases} 2f(x) - 1 & \text{if } x \in S \\ 2g(x) & \text{if } x \in S^c \end{cases}$

Note that $h(x)$ is odd if $x \in S$ and even if $x \in S^c$.

h is injective: Let $x_1, x_2 \in X$ and assume $h(x_1) = h(x_2)$. Then both $h(x_i)$ are even or both are odd. Hence either

~~Let $x_1, x_2 \in X$.~~ If x_1 and $x_2 \in S$, and $h(x_1) = h(x_2)$,

then $2f(x_1) - 1 = 2f(x_2) - 1$, so $f(x_1) = f(x_2)$, and hence $x_1 = x_2$, since f is bijective.

Similarly, if x_1 and $x_2 \in S^c$, and $\underset{2g(x_1)}{\underset{\parallel}{h(x_1)}} = \underset{2g(x_2)}{\underset{\parallel}{h(x_2)}}$

then $g(x_1) = g(x_2)$ and so $x_1 = x_2$, since g is injective.

h is surjective:

Let $y \in \mathbb{P}$. If $y = 2k$, $k \in \mathbb{P}$, then there exist $x \in S^c$ such that $g(x) = k$, since g is surjective. So $y = h(x)$. If y is odd, then

~~If~~ $y = 2k - 1$, $k \in \mathbb{P}$, and there exists $x \in S$ such that $f(x) = k$, since f is surjective.

Hence $h(x) = 2f(x) - 1 = y$.

Another method to prove that h is bijective:

$h^{-1} : \mathbb{P} \to X$ is given by $h^{-1}(n) = \begin{cases} f^{-1}\left(\frac{n+1}{2}\right) & \text{if } n \text{ is odd} \\ g^{-1}(n/2) & \text{if } n \text{ is even.} \end{cases}$

(b) (10 points) Regard the set $\mathbb{Q}$ of rational numbers as a subset of the real numbers $\mathbb{R}$ and let $\mathbb{Q}^c$ be the set of irrational real numbers. Prove that $\sharp(\mathbb{Q}^c) \neq \sharp(\mathbb{P})$ (so that $\mathbb{Q}^c$ is uncountable). Hint: Use part 2a.

Proof by contradition. Assume that $\#(\mathbb{Q}^c) = \#(\mathbb{P})$, we already know that $\#(\mathbb{Q}) = \#\mathbb{P}$ (Theorem 6.66 in the text). Part 2(a) implies that $\#(\mathbb{R}) = \#(\mathbb{P})$. But we know that $\#(\mathbb{R}) \neq \#\mathbb{P}$, by Cantor's Theorem 6.67 in the text. A contradition. Hence, $\#(\mathbb{Q}^c) \neq \#(\mathbb{P})$. Q.E.D

3. (10 points) Use Mathematical Induction to prove that for all $n \geq 1$,

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} \overset{(*)}{=} 2 - \left(\frac{n+2}{2^n}\right).$$

Initial case $n=1$: LHS $= \frac{1}{2}$, RHS $= 2 - \left(\frac{1+2}{2}\right) = \frac{1}{2}$. checks.

Induction step: Assume that $(*)$ holds for n. We need to prove the equality

$$\frac{1}{2} + \cdots + \frac{n}{2^n} + \frac{n+1}{2^{(n+1)}} \overset{(**)}{=} 2 - \left(\frac{n+1+2}{2^{n+1}}\right)$$

$$\text{LHS of } (**) = (\text{LHS of } (*)) + \frac{n+1}{2^{n+1}} \underset{\text{Induction Hyp}}{=} 2 - \left(\frac{n+2}{2^n}\right) + \frac{n+1}{2^{n+1}} =$$

$$= 2 + \underbrace{\left(\frac{n+1}{2^{n+1}} - \frac{2n+4}{2^{n+1}}\right)}_{\frac{-n-3}{2^{n+1}}} = 2 - \left(\frac{n+3}{2^{n+1}}\right) = \text{RHS of } (**).$$

Hence, equality $(*)$ holds for all n, by the principle of mathematical induction. Q.E.D

4. (10 points) Set $\mathbb{P}_n = \{1, 2, \ldots, n\}$, where $n \geq 3$. Consider the permutations $\rho := \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$ and $\sigma := \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}$. Note that ρ is a cyclic shift one position to the right, and σ reverses the order. Compute ρ^{-1} and $\sigma \circ \rho \circ \sigma$. Suggestion: Do it first for $n = 4$ so that $\rho := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

2 pt

Case $n=4$: $\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$\sigma(\overbrace{\rho(\underbrace{\sigma(1)}_{4})}^{1}) = 4$, $\sigma(\overbrace{\rho(\underbrace{\sigma(2)}_{3})}^{4}) = 1$, $\sigma(\overbrace{\rho(\underbrace{\sigma(3)}_{2})}^{3}) = 2$, $\sigma(\rho(\sigma(4))) = 3$

$\sigma \circ \rho \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$. (Note that this is ρ^{-1}).

3 pt

General $n \geq 3$:

$\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n & 1 & 2 & & n-1 \end{pmatrix}$

$\sigma(\overbrace{\rho(\underbrace{\sigma(1)}_{n})}^{1}) = n$, $\sigma(\overbrace{\rho(\underbrace{\sigma(2)}_{n-1})}^{n}) = 1$, $\cdots$ $\sigma(\overbrace{\rho(\underbrace{\sigma(n)}_{1})}^{2}) = n-1$

For $1 < i \leq n$: $\sigma(\overbrace{\rho(\underbrace{\sigma(i)}_{n-i+1})}^{n-i+2}) = i-1$

$\sigma \circ \rho \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & i & & n-1 & n \\ n & 1 & & i-1 & & n-2 & n-1 \end{pmatrix}$. = (Note that this is ρ^{-1})

2 pts

5. (10 points) Find the remainder when 5^{66183} is divided by $\overset{3^2\cdot 11}{\overset{\shortparallel}{99}}$. State any theorem you use and carefully justify your answer!

The Euler number of 99: $\phi(99) = \underbrace{\phi(3^2)}_{3\cdot 2}\underbrace{\phi(11)}_{10} = 60$.

$\gcd(5, 99) = 1$. Hence, $5^{\phi(99)} \equiv 1 \pmod{99}$, by Euler's-Fermat Theorem.

$$5^{66183} = 5^3 \cdot 5^{\overbrace{66180}^{60\cdot 1103}} = 5^3 \cdot (5^{60})^{1103} \equiv 125 \cdot 1^{1103} \equiv 125 \equiv 26$$

(modulo 99).

6. (10 points) Find the multiplicative inverse of 80 in $\mathbb{Z}_{253}$. Justify your answer. A complete answer will involve the Extended Euclidian Algorithm.

Solve:

$80 \cdot x \equiv 1 \pmod{253}$. This corresponds to the linear Diophantine equation $80x + 253y = 1$.

$253 y_i + 80 x_i = r_i$

y_i	x_i	r_i	q_i
1	0	253	
0	1	80	
1	-3	13	3
-6	19	2	6
37	-117	1	6

$253 \cdot 37 + 80(-117) = 1$

So $x = -117 \equiv 136$ (modulo 253).

$[80]^{-1} = [136]$ in $\mathbb{Z}_{253}$.

7. (10 points) Solve the simultaneous congruences

$$3x \equiv 10 \pmod{41} \quad (1)$$
$$x \equiv 20 \pmod{23} \quad (2)$$

Note that $3 \cdot 14 = 42 \equiv 1 \pmod{41}$. So $[14] = [3]^{-1}$ in $\mathbb{Z}_{41}$ and congruence (1) is equivalent to

$$\boxed{x \equiv 140 \equiv 17 \pmod{41}} \quad (1)'$$

(*) $x = 17 + 41y$. Plug into (2) to get

$$17 + 41y \equiv 20 \pmod{23}$$

$$\underbrace{41}_{\equiv 18 \pmod{23}} y \equiv 3 \pmod{23}$$

We solve the congruence $18y \equiv 3 \pmod{23}$

$$23z + 18y = 1$$

z_i	y_i	r_i
1	0	23
0	1	18
1	-1	5
-3	4	3
4	-5	2
-7	9	1

$[9] = [18]^{-1} \mod 23$

$y \equiv [18]^{-1}[3] = [27] = [4]$ in $\mathbb{Z}_{23}$.

So, pluging $y = 4 + 23k$ in (*) we get

$x = 17 + 41(4 + 23k) \equiv 181 \pmod{41 \cdot 23}$.

$$\boxed{x \equiv 181 \pmod{\underbrace{41 \cdot 23}_{943}}}$$

8. (10 points) Consider the relation R on the set of real numbers defined by xRy if and only if $x - y$ is an integer. Prove that R is an equivalence relation.

<u>R is symmetric:</u>

$xRy \iff x-y \in \mathbb{Z} \iff y-x \in \mathbb{Z} \iff yRx$

<u>R is reflexive:</u>

For every real number x, $x-x=0$ is an integer. Hence, xRx for all x.

<u>R is transitive:</u> (xRy and $yRz \Rightarrow xRz$)

If xRy and yRz, then $x-y \in \mathbb{Z}$ and $y-z \in \mathbb{Z}$.

So $\underbrace{(x-y)+(y-z)}_{x-z} \in \mathbb{Z}$. So xRz.

9. (10 points) Prove that there are precisely three congruence classes in $\mathbb{Z}_{280}$, which solve the congruence

$$x^3 \equiv 13 \pmod{280}.$$

You are not asked to find the solutions. State any theorem you use and carefully justify your answer.

$280 = 2^3 \cdot 5 \cdot 7$

The Chinese Remainder Theorem (C.R.T) implies that for $x^3 \equiv 13 \pmod{280}$, if and only if the simultaneous

(1) $x^3 \equiv 13 \equiv 5 \pmod{2^3}$ and

(2) $x^3 \equiv 13 \equiv 3 \pmod 5$ and

(3) $x^3 \equiv 13 \equiv 6 \pmod 7$.

Solutions for (1): Mod 8

x	0	1	2	3	4	5	6	7
x^3	0	1	0	3	0	5	0	7

one solution

Solutions for (2): Mod 5

x	0	1	2	3	4
x^3	0	1	3	2	4

one solution

Solutions for (3): Mod 7

x	0	1	2	3	4	5	6
x^3	0	1	1	6	1	6	6

Three solutions.

The C.R.T implies that there is a unique $[x_1] \in \mathbb{Z}_{280}$, such that $x_1 \equiv 5 \pmod 8$, $x_1 \equiv 2 \pmod 5$, and $x_1 \equiv 3 \pmod 7$.

There is a unique $[x_2] \in \mathbb{Z}_{280}$, such that

$x_2 \equiv 5 \pmod 8$, $x_2 \equiv 2 \pmod 5$, and $x_2 \equiv 5 \pmod 7$.

There is a unique $[x_3] \in \mathbb{Z}_{280}$, such that

$x_3 \equiv 5 \pmod 8$, $x_3 \equiv 2 \pmod 5$, and $x_3 \equiv 6 \pmod 7$

Hence, $\{[x_1], [x_2], [x_3]\}$ is the set of sol'n in $\mathbb{Z}_{280}$.