Review Problems (with Solutions) for Midterm Exam II
MTH 299 Spring 2014

1. *Disprove the statement*: There is a real root of equation $\frac{1}{5}x^5 + \frac{2}{3}x^3 + 2x = 0$ on the interval $(1, 2)$.

2. *Prove:* there exists a real number x such that $\dfrac{x^2 + 3x - 3}{2x + 3} = 1$.

3. Let $f(x) = x^3 - 3x^2 + 2x - 4$. Prove that there exists a real number r such that $2 < r < 3$ and $f(r) = 0$.

4. Prove that there is no smallest positive rational number.

5. Prove that there is no largest prime.

   Hint: Use proof by contradiction and consider $n = p_1 ... p_k + 1$, where $p_i, i = 1, ..., k$ are all the possible prime numbers, as per your assumption.

6. Let x be an irrational real number. Prove that either x^2 or x^3 is irrational.

   Solution: Assume, by way of contradiction, that x is irrational and x^2 and x^3 are both rational. Then, there exist $p, q, r, s \in \mathbb{Z} - \{0\}$ such that $x^2 = \frac{p}{q}$ and $x^3 = \frac{r}{s}$. Thus, $x = \frac{x^3}{x^2} = \frac{rq}{sp}$, which implies that $x \in \mathbb{Q}$. This contradicts the assumption. Thus, x^2 and x^3 cannot both be rational, i.e., either x^2 or x^3 is irrational. $\square$

7. Prove that $\sqrt{5}$ is irrational. (You can use the fact that $5 \mid x^2$ if and only if $5 \mid x$.)

   Solution: Assume to the contrary that $\sqrt{5} \in \mathbb{Q}$. Thus, $\exists p, q \in \mathbb{Z} - \{0\}$ such that $\sqrt{5} = \frac{p}{q}$. Assume also that the fraction is in reduced form, i.e., p and q have no common factors. Thus, $p^2 = 5q^2$. Therefore $5 \mid p^2$ and consequently $f \mid p$. Thus, $\exists k \in \mathbb{Z}$ such that $p = 5k$. Substituting this into the above equation and dividing both sides by 5, one arrives at $5k^2 = q^2$, which implies that $5 \mid q^2$ and therefore $5 \mid q$. This contradicts our assumption that p and q have no common factors. Since the assumption that $\sqrt{5}$ is rational leads to a contradiction, we can conclude that $\sqrt{5}$ is irrational. $\square$

8. Prove that if $x, y \in \mathbb{Z}$, then $x^2 - 4y \neq 2$.

   Solution: Assume, by way of contradiction, that there exist $z, y \in \mathbb{Z}$ such that $x^2 - 4y = 2$. Then, $x^2 = 2(2y + 1)$, thus x^2 is even (since $2y + 1 \in \mathbb{Z}$). Therefore, x must be even, i.e., $\exists k \in \mathbb{Z}$ such that $x = 2k$. Substituting this into the original equation, one arrives at $4(k^2 - y) = 2$, which implies that $4 \mid 2$. Thus, we have arrived at a contradiction. Therefore, if $x, y \in \mathbb{Z}$, then $x^2 - 4y \neq 2$. $\square$

9. Use induction to prove that

$$1 + 3 + 6 + \cdots + \frac{n(n+1)}{2} = \frac{n(n+1)(n+2)}{6}$$

   for all $n \in \mathbb{N}$.

   Solution: This statement is obviously true for $n = 1$ since $\frac{1(2)(3)}{6} = 1$. So assume there is some $k \geq 1$ for which

$$1 + 3 + 6 + \cdots + \frac{k(k+1)}{2} = \frac{k(k+1)(k+2)}{6}.$$

Adding $\frac{(k+1)(k+2)}{2}$ to both sides gives

$$\begin{aligned}1+3+6+\cdots+\tfrac{k(k+1)}{2}+\tfrac{(k+1)(k+2)}{2} &= \tfrac{k(k+1)(k+2)}{6}+\tfrac{(k+1)(k+2)}{2}\\ &= \tfrac{k(k+1)(k+2)+3(k+1)(k+2)}{6}\\ &= \tfrac{(k+1)(k+2)(k+3)}{6},\end{aligned}$$

which is the desired equality for $k+1$. The result then follows by the principle of induction. $\square$

10. Prove that

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}>\sqrt{n+1}$$

for all $n \in \mathbb{N}$ with $n \geq 3$. (Note that $1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}>1+\frac{1}{\sqrt{4}}+\frac{1}{\sqrt{4}}=2$.)

Solution: Since $1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}>1+\frac{1}{\sqrt{4}}+\frac{1}{\sqrt{4}}=2=\sqrt{3+1}$, the inequality holds for $n=3$.

Assume that the inequality holds for some $k \geq 3$, that is,

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}>\sqrt{k+1}.$$

Then we have

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}>\sqrt{k+1}+\frac{1}{\sqrt{k+1}}. \tag{1}$$

Since

$$k^2+4k+4>k^2+3k+2,$$

it follows that

$$(k+2)^2>(k+1)(k+2).$$

Hence,

$$(k+1)+1>\sqrt{k+1}\sqrt{k+2}.$$

Dividing both sides by $\sqrt{k+1}$ we have

$$\sqrt{k+1}+\frac{1}{\sqrt{k+1}} \geq \sqrt{k+2}.$$

So by (1) we get that

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}>\sqrt{k+2}.$$

That is, the inequality holds for $k+1$.

By the Principle of Mathematical Induction, the inequality holds for every integer $n \geq 3$. $\square$

11. Use the Strong Principle of Mathematical Induction to prove that for each integer $n \geq 13$, there are nonnegative integers x and y such that $n=3x+4y$.

Solution: When $n=13$, we have $13=3(3)+4(1)$, which verifies the base case. Proving by strong induction, we assume that there is some integer $k \geq 13$ such that for every integer $i \in \{13,\ldots,k\}$ there are nonnegative integers x, y such that $i=3x+4y$. We will use cases to prove that this implies the result for $k+1$.

Case 1: $k=13$. This case follows from the identity $k+1=14=3(2)+4(2)$.

Case 2: $k = 14$. This follows from writing $k + 1 = 15 = 3(5) + 4(0)$.

Case 3: $k \geq 15$. Then $(k+1) - 3 = k - 2$ is an integer between 13 and k, so by the inductive hypothesis there are nonnegative integers x, y such that $(k + 1) - 3 = 3x + 5y$. This gives

$$k + 1 = 3(x + 1) + 5y.$$

Since $x + 1$ and y are nonnegative, this proves the result in this case, and finishes the proof. $\square$

12. Let R be a relation defined on $\mathbb{N}^2$ by $(a, b)R(c, d)$ if $ad = bc$. Prove or disprove that a relation R is an equivalence relation and describe the elements in the equivalence class $[(1, 2)]$.

Solution: This is an equivalence relation. Indeed, if $(a, b) \in \mathbb{N}^2$ we obviously have $ab = ba$, which shows $(a, b)R(a, b)$.

To see the relation is symmetric, assume $(a, b)R(c, d)$. Then $ad = bc$, and this implies $cb = da$, which is exactly the statement $(c, d)R(a, b)$.

For transitivity, assume $(a, b)R(c, d)$ and $(c, d)R(e, f)$. Then $ad = bc$ and $cf = de$. Since none of these integers are zero, we can divide to get

$$\frac{a}{b} = \frac{c}{d}, \frac{c}{d} = \frac{e}{f}.$$

Hence $\frac{a}{b} = \frac{e}{f}$ and so $af = be$. This is exactly the statement $(a, b)R(e, f)$. $\square$

The equivalence class $[(1, 2)]$ is the set $\{(x, 2x) \mid x \in \mathbb{N}\}$.

13. For (a, b) and $(c, d) \in \mathbb{R}^2$, define $(a, b) \sim (c, d)$ if $\lfloor a \rfloor = \lfloor c \rfloor$ and $\lfloor b \rfloor = \lfloor d \rfloor$, where $\lfloor x \rfloor$ is the greatest integer less than or equal to x. Prove or disprove that a relation $\sim$ is an equivalence relation in $\mathbb{R}^2$.

Solution: This is an equivalence relation. To see it is reflexive, let $(a, b) \in \mathbb{R}^2$. Then $\lfloor a \rfloor = \lfloor a \rfloor$ and $\lfloor b \rfloor = \lfloor b \rfloor$, so $(a, b) \sim (a, b)$.

For symmetry, assume $(a, b) \sim (c, d)$. Then $\lfloor a \rfloor = \lfloor c \rfloor$ and $\lfloor b \rfloor = \lfloor d \rfloor$, which implies

$$\lfloor c \rfloor = \lfloor a \rfloor, \lfloor d \rfloor = \lfloor b \rfloor$$

and hence $(c, d) \sim (a, b)$.

To see transitivity, suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then focusing on the first components, we have $\lfloor a \rfloor = \lfloor c \rfloor$ and $\lfloor c \rfloor = \lfloor e \rfloor$. This implies $\lfloor a \rfloor = \lfloor e \rfloor$. The same argument shows $\lfloor b \rfloor = \lfloor f \rfloor$, and hence $(a, b) \sim (e, f)$. $\square$

14. A relation R is defined on the set of positive rational numbers by aRb if $\frac{a}{b} \in \{3^k : k \in \mathbb{Z}\}$. Prove that a relation R is an equivalence relation and describe the elements in the equivalence class $[2]$.

Solution: This is reflexive because $\frac{a}{a} = 1 = 3^0$. To see it is symmetric, assume aRb, and so $\frac{a}{b} = 3^k$ for some $k \in \mathbb{Z}$. Then $\frac{b}{a} = 3^{-k}$ and so bRa. For transitivity, assume aRb and bRc, so $\frac{a}{b} = 3^k$ and $\frac{b}{c} = 3^l$ for some integers k, l. Then multiplying gives $\frac{a}{c} = 3^{k+l}$ and so aRc. $\square$

The equivalence class of 2 is $\{2 \cdot 3^k \mid k \in \mathbb{Z}\}$.

15. (a) Fill in the following addition and multiplication tables for $\mathbb{Z}_4$.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

(b) For each of the following modular arithmetic equations, use the tables above to either find *all* solutions or explain why it has no solution. The coefficients and variables should be taken in $\mathbb{Z}_4$.

i. $[3]\,x + [1] = [2]$ This has one solution $x = [3]$.

ii. $[2]\,x + [2] = [3]$ This has no solutions because $[2]\,x = [3]$ has no solutions.

iii. $[2]\,x + [1] = [3]$ This has two solutions $x = [1]$ and $x = [3]$.

16. Let $[a]\,, [b] \in \mathbb{Z}_{13}$ and $[a] \neq [0]$. Prove that the equation $[a]\,x + [b] = 0$ always has *exactly one* solution.

Solution: Let $[a] \in \mathbb{Z}_{13}$, and assume this is non-zero. In a moment we will prove there is an integer r such that

$$[r]\,[a] = [1]\,.$$

Supposing this is the case, a solution x to $[a]\,x + [b] = 0$ is $x = [r]\,[-b]$. To prove this solution is the only one, suppose x' is a second solution, so $[a]\,x + [b] = [a]\,x' + [b] = [0]$. Subtracting these equations gives

$$[a]\,(x - x') = [0]\,.$$

Since 13 is prime, this means that 13 divides a or $x - x' = [0]$. We have assumed $[a] \neq 0$, so it must be the case that $x = x'$.

Now we prove the existence of $[r]$ above. This can be shown in several ways. For example, one way is to look at the multiplication table for $\mathbb{Z}_{13}$ and notice that every non-zero $[a]$ has a [1] in its column. However, we will give an alternative approach that is not as tedious as doing 169 products.

Lemma. The map $f : \mathbb{Z}_{13} \to \mathbb{Z}_{13}$ defined by $f([b]) = [ab]$ is an injection.

Proof. Suppose $[ab] = [ab']$ for some $b, b' \in \mathbb{Z}$. Then $[a(b - b')] = [0]$, which implies $a(b - b')$ is a multiple of 13. Since 13 is prime we must have either $13|a$ or $11|(b - b')$. But $[a] \neq 0$, so $13|(b - b')$ which implies $[b] = [b']$. □

Returning to the existence of $[r]$, note that the domain and codomain of f are the same finite set. Since f is injective, it follows that f must be surjective as well. So there is some $[r] \in \mathbb{Z}_{11}$ such that $f([r]) = [1]$; that is, $[r]\,[a] = [1]$. □

17. Let $[a]\,, [b] \in \mathbb{Z}_{13}$, and assume $[a] \cap [b] \neq \emptyset$. Prove that $[a] = [b]$.

Solution: Let $a, b \in \mathbb{Z}$ and suppose $[a]\,, [b] \in \mathbb{Z}_{13}$ have non-empty intersection. This means that there is some $r \in \mathbb{Z}$ such that $r \in [a]$ and $r \in [b]$, so we can write $r = a + 13k$ and $r = b + 13l$ for some integers k, l. This gives

$$a = b + 13(l - k).$$

We will show $[a] \subseteq [b]$; the proof that $[b] \subseteq [a]$ is similar. Let $a' \in [a]$. Then there is some $m \in \mathbb{Z}$ such that $a' = a + 13m$. Combining this with the above gives $a' = b + 13(m + l - k)$, and so $a' \in [b]$.

□

18. Let $[a], [b] \in \mathbb{Z}_{11}$ and $[a] \neq [0]$. Prove that the equation $[a]x + [b] = 0$ always has *exactly one* solution.

    Solution: The solution is the same as for $\mathbb{Z}_{13}$ above.

19. Let $[a], [b] \in \mathbb{Z}_{11}$, and assume $[a] \cap [b] \neq \emptyset$. Prove that $[a] = [b]$.

    Solution: The solution is the same as for $\mathbb{Z}_{13}$ above.

20. Fill in the blanks in part(a).

    (a) Let A and B be sets. A relation $R \subset A \times B$ defines a function from A to B if

    (1) $\forall a \in A$, $\exists b \in B$ such that ______________ and

    (2) $\forall a \in A$, $\forall b_1, b_2 \in B$, if $(a, b_1) \in R$ and $(a, b_2) \in R$, then

    ______________.

    Solution:
    $(a, b) \in R$ and $b_1 = b_2$

    (b) Let A be a set. Prove that there exists a unique relation R on A such that R is an equivalence relation on A and R is a function from A to A.

    Solution:
    Proof: Let $R = \{(a, a) \mid a \in A\}$. Since

    (1) for each $a \in A$, there is an $a \in A$ such that $(a, a) \in A$ and
    (2) if $(a, b_1) \in R$ and $(a, b_2) \in R$, then $b_1 = b_2 = a$,

    the relation R defines a function from A to A. Moreover, R is an equivalence relation since it is reflexive, symmetric, and transitive since each element is only related to itself. This proves existence.

    To prove uniqueness, suppose that R' is an equivalence relation on A and that R' defines a function from A to A. We prove that $R' = R$, where R is the relation above.

    Since R' is an equivalence relation on A, for each $a \in A$ we have that $(a, a) \in R'$ by the reflexive property. Thus, $R \subseteq R'$.

    Suppose that $(a, b) \in R'$. Since R' is a function and since $(a, a) \in R'$, we have that $a = b$. Therefore $(a, b) = (a, a) \in R$. Thus, $R' \subseteq R$. And therefore, $R = R'$. $\square$

21. Let A and B be sets. Suppose that $f : A \to B$ is a function. Let $C, D \subseteq B$. Prove that

    $$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D).$$

    Solution:
    Proof: Suppose that $a \in f^{-1}(C \cap D)$. Then $f(a) \in C \cap D$. Therefore, $f(a) \in C$ and $f(a) \in D$. And so, $a \in f^{-1}(C)$ and $a \in f^{-1}(D)$. Therefore, $a \in f^{-1}(C) \cap f^{-1}(D)$. This proves that $f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$.

    Suppose that $a \in f^{-1}(C) \cap f^{-1}(D)$. Then $a \in f^{-1}(C)$ and $a \in f^{-1}(D)$. Therefore, $f(a) \in C$ and $f(a) \in D$. Therefore, $f(a) \in C \cap D$. And therefore, $a \in f^{-1}(C \cap D)$. This prove that $f^{-1}(C) \cap f^{-1}(D) \subseteq f^{-1}(C \cap D)$.

    Hence, $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$. $\square$

22. Let $\mathbb{Z}_7 = \{[0], [1], \ldots, [6]\}$ be the set of congruence classes of integers modulo 7 together with the operations of addition and multiplication of congruence classes. Suppose that $f : \mathbb{Z}_7 \to \mathbb{Z}_7$ is the function defined by the rule

$$f([x]) = [2x + 1] \text{ for each } x \in \mathbb{Z}.$$

(a) Prove that f is a bijection.

Solution #1:

We compute the image $[x]$ for each $[x] \in \mathbb{Z}_7$:

$[x]$	$f([x])$
[0]	[1]
[1]	[3]
[2]	[5]
[3]	[0]
[4]	[2]
[5]	[4]
[6]	[6]

Thus, the range of f is $\mathbb{Z}_7$; therefore f is onto. Since no two distinct elements of the domain have the same image, f is one-to-one. Therefore, f is a bijection.

Solution #2: Let $g : \mathbb{Z}_7 \to \mathbb{Z}_7$ be the function defined by $g([x]) = [4x + 3]$. Then $f(g([x]) = f([4x + 3]) = [2(4x + 3) + 1] = [8x + 7] = [x]$ since $8 \equiv 1 \pmod 7$ and $7 \equiv 9 \pmod 7$. And $g(f([x])) = g([2x+1]) = [4(2x+1)+3] = [8x+7] = [x]$ since $8 \equiv 1 \pmod 7$ and $7 \equiv 9 \pmod 7$. These two calculations prove that $f \circ g = \iota_{\mathbb{Z}_7}$ and $g \circ f = \iota_{\mathbb{Z}_7}$. Therefore, $g = f^{-1}$. (This solves part (b) below, as well.) Since f has an inverse, f is a bijection.

(b) Prove that there exists integers a and b such that f^{-1} is given by the rule

$$f^{-1}([x]) = [ax + b] \text{ for each } x \in \mathbb{Z}.$$

Solution:

Let $a = 4$ and $b = 3$. And define $g([x]) = [4x + 3]$. We compute the image of $[x]$ for each $[x] \in \mathbb{Z}_7$:

$[x]$	$g([x])$
[0]	[3]
[1]	[0]
[2]	[4]
[3]	[1]
[4]	[5]
[5]	[2]
[6]	[6]

Since the table above is the same as the previous table with the columns switched, $g = f^{-1}$. $\square$