Math 300 Section 2 Midterm 2 Fall 2017

Name: Solution

1. (15 points) Define the sequence x_n of rational numbers as follows. $x_1 = 1$, and

$$x_{n+1} = \left(\frac{n}{n+1}\right) x_n + 1, \text{ for all } n \geq 1.$$

Find an expression for x_n and prove, by induction, that the expression is correct.

n	1	2	3	4	----	n
x_n	1	$\underbrace{\frac{1}{2}\cdot 1+1}_{\frac{3}{2}}$	$\underbrace{\frac{2}{3}\cdot\frac{3}{2}+1}_{2 = \frac{4}{2}}$	$\underbrace{\frac{3}{4}\cdot 2+1}_{\frac{5}{2}}$		$\frac{n+1}{2}$

We claim that $x_n \overset{\circledast}{=} \frac{n+1}{2}$.

<u>Proof by Induction</u>: Initial case $n=1$:

$x_1 = 1 = \frac{1+1}{2}$.

Induction hypothesis: Assume $\circledast$ holds. We need to prove that $x_{n+1} = \frac{n+2}{2}$.

$$x_{n+1} \underset{\text{definition}}{=} \left(\frac{n}{n+1}\right)\cdot x_n + 1 \underset{\text{Induction hyp } \circledast}{=} \left(\frac{n}{n+1}\right)\cdot\left(\frac{n+1}{2}\right) + 1 = \frac{n}{2} + 1 = \frac{n+2}{2}.$$

Hence, the statement follows by the principle of mathematical induction.

2. (15 points) Let $f(x) = e^{3x}$ and denote by $f^{(n)}(x)$ its n-th derivative. Prove the following identity for all positive integers n.

$$\sum_{k=0}^{n} \binom{n}{k} 2^{n-k} f^{(k)}(x) = 5^n e^{3x}.$$

$f^{(k)}(x) = 3^k e^{3x}$. Hence,

$$\sum_{k=0}^{n} \binom{n}{k} 2^{n-k} f^{(k)}(x) \overset{*}{=} \left(\sum_{k=0}^{n} \binom{n}{k} 2^{n-k} 3^k \right) e^{3x}$$

Now, $5^n = (2+3)^n \underset{\uparrow}{=} \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} 3^k$. Hence, the right

Binomial Theorem

hand side of $*$ is $5^n e^{3x}$. QED.

3. (15 points) Determine the number of congruence classes which solve the linear congruence $25x \equiv 35 \pmod{45}$ and find all of them. Justify your answer!

Translate to a diophantine equation

$$25X + 45y = 35.$$

$\gcd(\underset{5^2}{\underset{\parallel}{25}}, \underset{5\cdot 3^2}{\underset{\parallel}{45}}) = 5$ and $5 \mid 35$. Hence solutions exist. Furthermore, if x_0 is a solution, then so are $X = X_0 + \underbrace{9}_{\frac{45}{\gcd(25,45)}}K$, $K \in \mathbb{Z}$. Modulo 45 we get 5 distinct solutions that way ($0 \le K \le 4$).

We find a particular solution x_0 of $5X + 9y = 7$

Find a solution $\tilde{x}_0$ of $5X + 9y = \underbrace{\gcd(5,9)}_{1}$ by the Extended Euclidean Alg

$$9y_i + 5x_i = r_i$$

y_i	x_i	r_i	q_i
1	0	9	
0	1	5	
1	-1	4	1
-1	2	1	1

$$5\underset{\tilde{x}_0}{\underset{\parallel}{\boxed{2}}} + 9(-1) = 1$$

So $x_0 = 7 \cdot \tilde{x}_0 = 14$

Check: $5 \cdot 14 + 9(-7) = 70 - 63 = 7$ ✓

The 5 solutions are

$$14,\ \underbrace{14+9}_{23},\ \underbrace{14+18}_{32},\ \underbrace{14+27}_{41},\ \underbrace{14+36}_{\equiv 5} \pmod{45}$$

4. (15 points) Use the Extended Euclidean Algorithm (E.E.A) to find the inverse of [80] in $\mathbb{Z}_{253}$. Credit will be given only for an answer using the E.E.A.

$$80x + 253y = \underline{1}$$

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

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

So, $[-117] = [136] = [80]^{-1} \pmod{253}$.

5. (15 points) Use the Chinese Remainder Theorem in order to determine (only) the **number** of congruence classes in $\mathbb{Z}_{65}$ solving the congruence

$$[x]^{14} + 12[x]^{12} \equiv [3]. \quad (\dagger)$$

You do not need to actually solve the congruence. Justify your answer.

$65 = 5 \cdot 13$

If $[a_1] \in \mathbb{Z}_5$ is a solution of $[x]^{14} + [12][x]^{12} \equiv [3] \pmod 5$ (*)

and $[a_2] \in \mathbb{Z}_{13}$ " " " " $[x]^{14} + [12][x]^{12} \equiv [3] \pmod{13}$

and $b \in \mathbb{Z}$, $b \overset{(1)}{\equiv} a_1 \pmod 5$ and $b \overset{(2)}{\equiv} a_2 \pmod{13}$, (**)

then $b^{14} + 12 b^{12} \equiv 3 \pmod 5$ and $\pmod{13}$.

Hence, by the Chinese Remainder Theorem (C.R.T) (uniqueness part) $b^{14} + 12b^{12} \equiv 3 \pmod{\underbrace{5 \cdot 13}_{65}}$.

For each pair $([a_1], [a_2])$ in $\mathbb{Z}_5 \times \mathbb{Z}_{13}$ there exist a unique $[b] \in \mathbb{Z}_{65}$ satisfying (1) and (2), by C.R.T. Hence, the number of solutions of $(\dagger) \pmod{65}$ is the product:

(number of solutions of (*)) $\cdot$ (number of solution of (**)).

Fermat's Little Theorem

Solution of (*): $\pmod 5$ $[x]^5 = [x]$. If $[x] \neq [0]$, then $[x]^4 = [1]$.

$[0]$ is not a solution. Assume $[x] \neq [0]$. Then

$[3] = [x]^{14} + [12][x]^{12} = \underbrace{[x]^5[x]^5[x]^4}_{[x]^2} + [2]\underbrace{([x]^4)^3}_{[1]} = [x]^2 + [2]$

So $\boxed{[x]^2 = [1]}$.

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

So we get two sol'ns $\pmod 5$:

Solution of (**): $\pmod{13}$ $[0]$ not a sol'n. Assume $[x] \neq [0]$.

$[3] = [x]^{14} + [12][x]^{12} \overset{F.L.T}{=} \underbrace{[x]^{13}}_{[x]}[x] + [-1][1] = [x]^2 - [1]$. So $\boxed{[x]^2 = [4]}$

So $[x] = \pm[2]$ (use table). Again 2 solutions $\pmod{13}$.

Conclusion: There are $2 \cdot 2 = 4$ solutions in $\mathbb{Z}_{65}$.

6. (15 points) Find all integers x solving the simultaneous congruences

$$x \equiv 17 \pmod{41}, \qquad (1)$$
$$x \equiv 20 \pmod{23}. \qquad (2)$$

Justify your answer. 23 is a prime, $23 \nmid 41$, so $\gcd(23,41)=1$. The Chinese Remainder Theorem states that there exist a unique congruence class $[x] \pmod{23\cdot 41}$, such that x satisfies (1) and (2). We find a particular sol'n as follows.

(1)' $x + 41y = 17$

$x = 17 - 41y \equiv 20 \pmod{23}$

$-3 \equiv 41y \pmod{23}$

$[y] = [-3]\cdot[41]^{-1}$ in $\mathbb{Z}_{23}$

Find $[41]^{-1}$: $a\cdot 41 + b\cdot 23 = 1$

a_i	b_i	r_i	q_i
1	0	41	
0	1	23	
1	-1	18	1
-1	2	5	1
4	-7	3	3
-5	9	2	1
9	-16	1	1

So, $[41]^{-1} = [9]$ in $\mathbb{Z}_{23}$

$[y] = [-27] = [-4]$ in $\mathbb{Z}_{23}$. Let $y_0 = -4$.

$x \equiv 17 - 41\cdot(-4) \equiv 181 \pmod{23\cdot 41}$

General Sol'n: $\boxed{x = 181 + k\cdot 23\cdot 41, \quad k \in \mathbb{Z}}$

7. (15 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.

We need to show that R is symmetric, reflexive, and transitive.

The negative of an integer is an integer

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

Reflexive: $x-x=0 \in \mathbb{Z}$, so xRx holds.

Transitive: We need to show

$$xRy \text{ AND } yRz \Rightarrow xRz.$$

This translates to

$$(x-y \in \mathbb{Z}) \text{ AND } (y-z) \in \mathbb{Z} \Rightarrow (x-z \in \mathbb{Z})$$

Indeed, if $(x-y) \in \mathbb{Z}$ and $(y-z) \in \mathbb{Z}$, then

$$\underbrace{(x-y)+(y-z)}_{= x-z} \in \mathbb{Z},$$ so $x-z \in \mathbb{Z}$, since the sum of two integers is an integer.