Math 300 Section 2 Midterm 2 Fall 2017

Name:__________________________

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	$\underbrace{\left(\frac{1}{1+1}\right)1+1}_{3/2}$	$\underbrace{\underbrace{\left(\frac{2}{2+1}\right)\frac{3}{2}}_{1}+1}_{2 = \frac{4}{2}}$	$\underbrace{\frac{3}{4}2}_{}+1 = \frac{5}{2}$		$\frac{n+1}{2}$

Claim: $\boxed{x_n \overset{(*)}{=} \frac{n+1}{2}}$

Proof by induction:

Case $n=1$: $x_1 = 1 = \frac{1+1}{2}$ ✓

$\uparrow$ given

Assume that $(*)$ holds for n.

$$x_{n+1} = \frac{n}{n+1} \cdot \underbrace{x_n}_{} + 1 = \frac{n}{2} + 1 = \frac{n+2}{2} = \frac{(n+1)+1}{2}.$$

|| Ind. Hyp. $(*)$

So formula (*) hold for $n+1$ as well. Hence hold for all n, by P.M.I
$\frac{n+1}{2}$
$\geq$ QED.

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.

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

$f(x) = e^{3x}$, $f'(x) = 3e^{3x}$, $f''(x) = 3\cdot 3 e^{3x} = 3^2 e^{3x}$

$$\boxed{f^{(n)}(x) \overset{(**)}{=} 3^n e^{3x}.}$$

$e^{3x} \cdot 5^n = \text{RHS}$

$$\text{LHS} = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k} \underbrace{3^k e^{3x}}_{\overset{(**)}{=} f^{(k)}(x)} = e^{3x} \underbrace{\sum_{k=0}^{n} \binom{n}{k} 2^{n-k} \cdot 3^k}_{5^n = (+)}$$

$$\sum_{k=0}^{n} \binom{n}{k} 2^{n-k} 3^k = \underbrace{\binom{n}{0}}_{1} 2^n + \binom{n}{1} 2^{n-1} 3 + \cdots + \binom{n}{n-1} 2^1 3^{n-1} + \underbrace{\binom{n}{n}}_{1} 3^n$$

$$(\underset{2}{a} + \underset{3}{b})^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

So $(+) = 5^n$. So eq (*) holds.
By the Binomial Theorem

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!

Recall: Prop: (i) The linear congruence

$$(*) \qquad ax \equiv c \pmod{n}$$

has a solution, if and only if

$d := \gcd(a, n) \mid c$.

($\Leftrightarrow$ $ax + ny = c$ has a solution)

(ii) If x_0 is a particular solution of $(*)$ then the general solution is

$$x_0, \; x_0 + \frac{n}{d}, \; \frac{kn}{d} \dots, \; x_n + \frac{(d-1)n}{d}$$

modulo n. $0 \le k \le d-1$ So there are precisely d congruence classes in $\mathbb{Z}_n$ solving $(*)$.

$(*)$ $25x \equiv 35 \pmod{45}$

$d := \gcd(\underset{5^2}{25}, \underset{5 \cdot 3^2}{45}) = 5 \mid 35$. So a solution exists, and there are thus precisely $d = 5$ congruence classes solving $(*)$

in $\mathbb{Z}_{45}$,

We solve the Linear Diophantine eq.

$$25x + \underbrace{45}_{n}y = 35 \quad \text{using E.E.A.}$$

$\boxed{n \text{ in the Prop}}$

First solve $25x + 45y = \gcd(25, 45) = 5$.

$45y_i + 25x_i = r_i$

y_i	x_i	r_i	q_i
1	0	45	—
0	1	25	—
1	−1	20	1
−1	2	5	1
		0	

gcd(45, 25)

$(-1)45 + 25 \cdot 2 = 5$. Multiply by 7

So

$$25 \cdot \underbrace{14}_{2\cdot 7} + 45(-7) = \underbrace{5 \cdot 7}_{35}$$

$x_0 = 14$ is a particular solution to

$$25x \equiv 35 \pmod{45}.$$

The general solution mod 45 (in $\mathbb{Z}_{45}$) is

$[14]$, $\underbrace{[14 + \frac{M}{d}]}_{[14+9]}$ ($M=45$, $d=5$), $[14+2\cdot 9]$, $[14+3\cdot 9]$, $[14+4\cdot 9]$ $\underbrace{}_{36}$ $50 = 5$

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.

$[80]\,[x] \overset{(*)}{\equiv} [1]$ in $\mathbb{Z}_{253}$,

A sol'n exists if and only if $\underbrace{\gcd(80, 253)}_{=1}\,\big|\, 1$, which is the case.

$80 = 2^3\cdot 10 = 2^4\cdot 5$

$(*)$ is equivalent to the Diophantine eq

$$80X + 253y = 1.$$

$$253\,y_i + 80\,x_i = r_i$$

y_i	x_i	r_i	q_i
1	0	253	
0	1	80	
1	-3	13	3
-6	19	2	6
37	$\underbrace{-3-6\cdot 19}_{-117}$	$\boxed{1} = \gcd$	6

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

So $[80]\,\underbrace{[-117]}_{\equiv 136} \equiv 1 \pmod{253}$

5. $[80]^{-1} = [136]$ in $\mathbb{Z}_{253}$.

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

$$[x]^{14} + 12[x]^{12} \equiv [3]. \quad (\text{mod } 5 \cdot 13). \quad (*)$$

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

$65 = 5 \cdot 13$. Strategy:

Suppose that x is a solution.

Write $b := x^{14} + 12x^{12}$. Then

$b \equiv 3 \pmod{5 \cdot 13}$,

So $b \equiv 3 \pmod 5$

and $b \equiv 3 \pmod{13}$,

Conversely: Suppose that

$[a_1]$ is a solution in $\mathbb{Z}_5$ of

(1) $[x]^{14} + 12[x]^{12} \equiv [3] \pmod 5$

and $[a_2]$ is a solution in $\mathbb{Z}_{13}$ of

(2) $[x]^{14} + 12[x]^{12} \equiv [3] \pmod{13}$

Then there exists a unique soln

$[x]$ in $\mathbb{Z}_{5\cdot 13}$, such that

$x \equiv a_1 \pmod 5$

$x \equiv a_2 \pmod{13}$.

Then in $\mathbb{Z}_5$

$$[x]^{14}+12[x]^{12}=[a_1]^{14}+12[a_1]^{12}\underset{\substack{\uparrow\\ \text{by the}\\ \text{choice of } a_1}}{=}[3]$$

Similarly in $\mathbb{Z}_{13}$.

So x solve (*).

For each pair $([a_1],[a_2])$ in $\mathbb{Z}_5\times\mathbb{Z}_{13}$ such that $[a_1]$ is a solution of (1) and $[a_2]$ is a solution of (2) we get a unique $[x]$ in $\mathbb{Z}_{5\cdot 13}$ solving (*) by the C.R.T. Any solution is of this form. So $\boxed{\#\text{ solutions of } (*) = \#\text{ Solutions of (1) in } \mathbb{Z}_5 \text{ times } \#\text{ Solution of (2) in } \mathbb{Z}_{13}}$

<u>In $\mathbb{Z}_5$:</u>

(1) $\quad [x]^{14}+12[x]^{12}\equiv[3] \pmod 5$

In $\mathbb{Z}_5$ $[x]^5=[x]$, by F.L.T. So

$$[x]^{14}=[x]^5[x]^5\cdot[x]^4=[x]^6=\underbrace{[x]^5}_{[x]}\cdot[x]=[x]^2,$$

$$[x]^{12}=[x]^5[x]^5[x]^2=[x]^4\underset{\text{F.L.T}\nearrow}{=}\begin{cases}[1] & \text{if } [x]\neq[0]\\ [0] & \text{if } [x]=0\end{cases}$$

$[0]$ is not a sol'n of (1). Assume $[x] \neq [0]$
So LHS of (1) is

$$[x]^2 + \underbrace{[12]}_{\text{is } [2]}[1] = [3] \quad \text{in } \mathbb{Z}_5$$

$$[x]^2 = [1] \quad \text{in } \mathbb{Z}_5$$

So $\boxed{[x] = [1] \text{ or } [-1].}$ TWO SOLN in $\mathbb{Z}_5$

<u>In $\mathbb{Z}_{13}$</u>;

(2) $$[x]^{14} + 12[x]^{12} \equiv [3] \pmod{13}$$

$[x] = [0]$ is not a sol'n. Assume $[x] \neq [0]$, so $\underbrace{[x]^{13-1}}_{[x]^{12}} = [1]$ by FLT

$$[x]^{14} = \underbrace{[x]^{13}}_{\equiv [x] \text{ FLT}}[x] = [x]^2$$

The LHS of (2) is

$$[x]^2 + [-1]\cdot[1] \equiv [3]$$

$$[x]^2 \equiv [4] \pmod{13}$$

$$\boxed{[x] = [2] \text{ or } [-2].}$$ TWO SOLUTIONS

So the # soln to original in $\mathbb{Z}_{5\cdot 13}$

so $\boxed{2 \cdot 2 = 4.}$

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

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

Justify your answer. $\gcd(41, 23) = 1$

We will use the C.R.T. to convert (1) and (2) to a single congruence (mod $41 \cdot 23$).

<u>Solution:</u>

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

Plug into (2) to get

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

$$-41y \equiv 20 - 17 = 3$$

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

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

As in Prob 4, we use the E.E.A to find $[41]^{-1} = [9]$ in $\mathbb{Z}_{23}$. So

$[y] = [-9 \cdot 3] = [-27] = [-4]$.

So $y = -4 + 23z$, z an integer.

$x = 17 - 41(-4 + 23z) = \underbrace{17 + 164}_{181} + 23 \cdot 41(-z)$

So $x \equiv 181 \pmod{23 \cdot 41}$.

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.

So the general solution, by the CRT, is $\{x \in \mathbb{Z} : x \equiv 181 \pmod{23 \cdot 41}\}$.

We need to show that R is Reflexive, Symmetric, and Transitive.

Reflexive: $xRx \iff \underbrace{x - x}_{=0}$ is an integer

Indeed 0 is an integer. So xRx holds for every $x \in \mathbb{R}$.

Symmetric; Assume that xRy. We need to show yRx.

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

So R is symmetric.

Transitive:

suppose that xRy and yRz.
We need to show xRz.

$$(xRy \text{ and } yRz) \Leftrightarrow (x-y \in \mathbb{Z} \text{ and } y-z \in \mathbb{Z}) \Rightarrow$$

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

Q.E.D.