Math 300 Section 2 Midterm 2 Spring 2016

Name:_____

1. (15 points) Define the sequence x_n as follows. $x_1 = 1$, $x_2 = 5$, and

$$x_n = x_{n-1} + 2x_{n-2}, \text{ for all } n \geq 3.$$

Find an expression for x_n and prove, by induction, that the expression is correct. Hint: Compute the difference $x_n - 2^n$ for the first few terms.

n	1	2	3	4
x_n	1	5	7	17
$x_n - 2^n$	-1	1	-1	1

The emerging patern is $x_n - 2^n = (-1)^n$.

$\Leftrightarrow$ $x_n = 2^n + (-1)^n$.

We will prove, by induction, that $x_n = 2^n + (-1)^n$. (*)

<u>Initial Step:</u> The cases $n=1$ and $n=2$ are verified by the table above.

<u>Induction Step:</u> Assume that $n \geq 2$ and that equality (*) holds for all integers k in the range $1 \leq k \leq n$. We need to prove $x_{n+1} \overset{(**)}{=} 2^{(n+1)} + (-1)^{n+1}$.

$$x_{n+1} \underset{\boxed{\text{Def of the sequence}}}{=} x_n + 2x_{n-1} \underset{\boxed{\text{Induction Hypothesis}}}{=} \left(2^n + (-1)^n\right) + 2\left(2^{n-1} + (-1)^{n-1}\right) =$$

$$= \underbrace{2^n + 2^n}_{2^{n+1}} + \underbrace{(-1)^n + 2(-1)^{n-1}}_{(-1)^{n-1} = (-1)^{n+1}} = 2^{n+1} + (-1)^{n+1}.$$

We established Equality (**). Hence, Equality (*) follows, by the principle of STRONG Mathematical Induction.

Q.E.D

2. (15 points) Let p be a prime.

(a) 7 points Prove that $\binom{p}{k} \equiv 0 \pmod{p}$, for $0 < k < p$.

By definition,

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}.$$

We know that $\binom{p}{k}$ is an integer.

Hence, $\underbrace{p!}_{= p(p-1)\cdots 1} = \binom{p}{k} \cdot k!\,(p-k)!$

Now p divides $p!$. Hence $p \mid \binom{p}{k} \cdot k!\,(p-k)!$.

$k! = 1 \cdot 2 \cdots k$. So $p \nmid k!$, since $k < p$.

Similarly, $p \nmid (p-k)!$, since $p-k < p$.

Hence, since p is a prime, $p \mid \binom{p}{k}$, by the prop. below (take $a = \binom{p}{k}$, $b = k!$, $c = (p-k)!$). QED.

<u>Prop:</u> Let a, b, c be integers and p a prime. If $p \mid abc$, then $p \mid a$ or $p \mid b$ or $p \mid c$.

8 points

(b) Use induction on n to prove that $n^p \equiv n \pmod{p}$, for all positive integers n (Fermat's Little Theorem). Credit will be given only for a proof by induction. Hint: In the induction step you will need the Binomial Theorem and part 2a.

Proof by induction on n.

Case $n = 1$: $1^p = 1 \equiv 1 \pmod{p}$. ✓

Induction Step: Assume that $n^p \equiv n \pmod{p}$.

We need to prove that

$$(n+1)^p \equiv n+1 \pmod{p}.$$

$$(n+1)^p = n^p + \underbrace{\binom{p}{1} n^{p-1}}_{\equiv 0 \pmod{p}} + \cdots + \underbrace{\binom{p}{k} n^{p-1}}_{\equiv 0 \pmod{p}} + \cdots + \underbrace{\binom{p}{p-1} n^1}_{\equiv 0 \pmod{p}} + 1^p$$

The Binomial Theorem

$\equiv 0 \pmod{p}$ ← for $0 < k < p$

$$\equiv n^p + 1^p \equiv n+1 \pmod{p}$$

By part (a) by the Induction Hypothesis.

Hence, $(n+1)^p \equiv n+1 \pmod{p}$ as well.

The congruence $n^p \equiv n \pmod{p}$ follows, for all n, by the Principle of Mathematical Induction.

3. (15 points) Determine the number of congruence classes which solve the linear congruence $9x \equiv 6 \pmod{15}$ and find all of them. Justify your answer!

$d := \gcd(\underset{3^2}{\underset{\shortparallel}{9}}, \underset{3\cdot 5}{\underset{\shortparallel}{15}}) = 3$ and $3 \mid 6$.

Hence, the linear congruence has 3 congruence classes (mod 15), which solve it, by Theorem 3.54.

If x_0 is a particular sol'n, then $[x_0]$, $[x_0+5]$, and $[x_0+10]$ are the 3 solutions (mod 15), by Theorem 3.54 again.

We find a particular solution x_0 by solving the linear Diophantine equation

$$9x + 15y \overset{(*)}{=} 6$$

$$\Longleftrightarrow$$

$$3x + 5y = 2$$

Note that $3 \cdot 2 + 5(-1) = \underline{1}$

So $\boxed{x_0 = 4}$, $y_0 = -2$ is a particular sol'n of $(*)$.

The general sol'n is

$$\boxed{x \equiv 4 \text{ or } 9 \text{ or } 14 \pmod{15}.}$$

Partial credit:
Particular sol'n: 7 pt. Number of sol'n + Just: 4 pt. All soln: 4 pt

4. (15 points) Find all integers x solving the congruence $x^{12} \equiv 5x \pmod{13}$. Justify your answer.

$p = 13$ is a prime.

If $x \equiv 0 \pmod{13}$, then clearly x is a solution.

If $x \not\equiv 0 \pmod{13}$, then $x^{12} \equiv 1 \pmod{13}$, by Fermat's Little Theorem and so $1 \equiv 5x \pmod{13}$.

This congruence has a unique sol'n in $\mathbb{Z}_{13}$ since $\gcd(5,13)=1$.

$x_0 = (-5) \equiv 8 \pmod{13}$ is a solution.

Hence, the general solution of $x^{12} \equiv 5x \pmod{13}$ is $x \equiv 0 \pmod{13}$, or $x \equiv 8 \pmod{13}$.

5. (15 points) Find the inverse of $[25]$ in $\mathbb{Z}_{41}$.

$\gcd(\underbrace{25}_{5^2}, 41) = 1$

Solve the congruence

$$25x \equiv 1 \pmod{41}.$$

So the Diophantine Equation

$$25x + 41y \equiv 1$$
$$41y + 25x \equiv 1$$

$41y_i + 25x_i = r_i$

y	x	r	q
1	0	41	
0	1	25	
1	-1	16	1
-1	2	9	1
2	-3	7	1
-3	5	2	1
11	-18	1	3

$\gcd(41,25)$

$y_0 = 11$, $x_0 = -18 \equiv 23 \pmod{41}$.

So $[25]^{-1} = [23] \pmod{41}$

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

$$x \equiv 2 \pmod 5, \quad (1)$$
$$x \equiv 18 \pmod{24}. \quad (2)$$

Justify your answer.

$\gcd(5,24)=1$, hence, there <u>exists</u> a <u>unique</u> congruence class, modulo $\underbrace{5\cdot 24}_{120}$, which simulaneously solves (1) and (2), by the Chinese Remainder Theorem.

If x_0 is a particular solution, then the general solution is $x = x_0 + 120\cdot m$, $m \in \mathbb{Z}$.

We find next a particular sol'n:

(1)' $x + 5y = 2$. Plug into (2) to get
$x = 2 - 5y$

(2)' $2 - 5y \equiv 18 \pmod{24}$.

$5y \equiv 2 - 18 \equiv -16 \equiv 8 \pmod{24}$

$[y] = \underbrace{[5]^{-1}}_{\substack{\parallel \\ [5]}} \cdot [8] = [40] = [16]$.

$y_0 = 16$, $x_0 = 2 - 80 = -78 \equiv 42 \pmod{120}$.

So $\boxed{x \equiv 42 \pmod{120}}$.

7. (15 points) Let R be the relation on the integers $\mathbb{Z}$ given by xRy if and only if $x^2 + x + 1 \equiv y^2 + y + 1 \pmod 5$.

(a) Show that R is an equivalence relation.

R is reflexisive, since $x^2+x+1 \equiv x^2+x+1 \pmod 5$, for all $x \in \mathbb{Z}$.

R is symmetric, since congruence mod 5 is symmetric and so

$$\left[x^2+x+1 \equiv y^2+y+1 \pmod 5\right] \Leftrightarrow \left[y^2+y+1 \equiv x^2+x+1 \pmod 5\right].$$

R is transitive, since congruence mod 5 is transitive. Hence, if

$x^2+x+1 \equiv y^2+y+1 \pmod 5$ and

$y^2+y+1 \equiv z^2+z+1 \pmod 5$, then

$x^2+x+1 \equiv z^2+z+1 \pmod 5$.

4 pts

(b) Find a pair of integers (x, y), such that $x \not\equiv y \pmod 5$ and xRy.

(mod 5)

x	0	1	2	3	4
x^2+x+1	[1]	[3]	[2]	[3]	[1]

So $1 \not\equiv 3 \pmod 5$, but $1 R 3$ holds.

Similarly $0 \not\equiv 4 \pmod 5$, but $0 R 4$ holds.

3 points

(c) The equivalence relation R determines a partition of $\mathbb{Z}$ into equivalence classes with respect to R. Determine the number of equivalence classes in this partition and find a representative for each equivalence class. Justify your answer!

If $x \equiv y \pmod 5$, then $x^2+x+1 \equiv y^2+y+1 \pmod 5$, and so xRy holds.

The table in part (b) shows that

(a) If $x \equiv 0 \pmod 5$ or $x \equiv 4 \pmod 5$, then $0Rx$.

(b) If $x \equiv 1 \pmod 5$ or $x \equiv 3 \pmod 5$, then $1Rx$.

(c) If $x \equiv 2 \pmod 5$, then $2Rx$.

Since every $x \in \mathbb{Z}$ falls in cases (a) OR (b) OR (c), then there are at most $\boxed{3}$ R-equivalence classes.

The table in part b shows that

$0 \not R 1$, $0 \not R 2$, and $1 \not R 2$. Hence, the equivalence classes of 0, 1, and 2 are pairwise distinct, and there are $\boxed{3}$ equivalence classes, one for each value of $[x^2+x+1] \pmod 5$.