1. (a) Give the negation, contrapositive, and converse of the following statement avoiding the word 'not' in your final answers. Then determine which of the statements are true (no proof required):

ORIGINAL: "$\forall a, n \in \mathbb{N}$, if $ax \equiv 2 \pmod{n}$ for some $x \in \mathbb{Z}$, then a is even or n is even."

(4 pts) NEGATION:

$a = 9$
$n = 7$
$9x \equiv 2 \pmod 7$ is possible with $x = 1$ and a and n are odd

$\exists\, a, n \in \mathbb{N}$ such that $ax \equiv 2 \pmod{n}$ for some $x \in \mathbb{Z}$ AND a is ODD AND n is ODD.

(3 pts) CONTRAPOSITIVE:

$\forall a, n \in \mathbb{N}$ if a is ODD AND n is ODD, then $ax \not\equiv 2 \pmod{n}$ for any $x \in \mathbb{Z}$.

(3 pts) CONVERSE:

counterexample

$a = 6$
$n = 3$
a even or b even is TRUE AND $6x \equiv 2 \pmod 3$ IS NOT POSSIBLE

$\forall a, n \in \mathbb{N}$ if a is even or n is even, then $ax \equiv 2 \pmod{n}$ for some $x \in \mathbb{Z}$.

F

(solvable only if gcd(a,n) divides 2)

(3 pts) CIRCLE **ALL THAT ARE TRUE**:

ORIGINAL   NEGATION   CONTRAPOSITIVE   CONVERSE

(b) (3 pts) Suppose that P and Q are TRUE statements and R and S are FALSE statements. Determine the truth values of the following statements.

i. $(\overset{T}{P} \text{ or } \overset{F}{R})$ and $(\overset{T}{Q} \text{ and } \overset{F}{S})$	TRUE	FALSE
ii. $\overset{T}{P} \Rightarrow \neg(\overset{F}{R} \text{ or } \overset{T}{Q})$	TRUE	FALSE
iii. $\overset{F}{R} \Rightarrow (\overset{T}{P} \text{ and } \overset{T}{Q})$	TRUE	FALSE

Vacuously

Q and S is FALSE
So $(P \text{ or } R)$ and $\underbrace{(Q \text{ and } S)}_{F}$ is FALSE

$\neg\underbrace{(\overset{F}{R} \text{ or } \overset{T}{Q})}_{T}$ is FALSE

So $\underset{T}{P} \Rightarrow \underbrace{\neg(R \text{ or } Q)}_{F}$ is FALSE

(c) (6 pts) Give a counterexample (explain why it is a counterexample)

i. Every monotone function from $\mathbb{R}$ to $\mathbb{R}$ is surjective.

$\boxed{f(x) = 5}$ or any constant function

ii. Every function from the set $A = \{1, 2, 3\}$ to $B = \{1, 2, 3\}$ is a bijection.

$f(1) = 1$
$f(2) = 1$
$f(3) = 1$

$f: A \to B$ is not a bijection

2. (a) (8 pts) Using the definitions of even and odd, give a **proof by contradiction** for the statement: For all $x, y \in \mathbb{Z}$, if $x^2 + y + 5$ is odd, then x is odd or y is even.

pf) Assume $x, y \in \mathbb{Z}$ such that x^2+y+5 is odd

AND x is even AND y is odd.

By def'n of even and odd $\exists k, m, n \in \mathbb{Z}$ such that

$x^2+y+5 = 2k+1$, $x = 2m$ and $y = 2n+1$. By substitution,

$(2m)^2 + (2n+1) + 5 = 2k+1$. So

$4m^2 + 2n + 6 = 2k+1$

$2(2m^2+n+3) = 2k+1$ $\rightarrow\leftarrow$ (even $\neq$ odd).

Hence x is odd or y is even.//

(b) (10 pts) Let $f : \mathbb{R} \to \mathbb{R}$ and define $g : \mathbb{R} - \{-1\} \to \mathbb{R}$ by $g(x) = 3f\left(\frac{x}{x+1}\right) - 1$.

Prove that if f is one-to-one, then g is one-to-one.

pf) Assume f is 1-1.

Let $g(x_1) = g(x_2)$ for some $x_1, x_2 \in \mathbb{R} - \{-1\}$.

By the given def'n, $3f\left(\frac{x_1}{x_1+1}\right) - 1 = 3f\left(\frac{x_2}{x_2+1}\right) - 1$

Simplifying $3f\left(\frac{x_1}{x_1+1}\right) = 3f\left(\frac{x_2}{x_2+1}\right)$

$f\left(\frac{x_1}{x_1+1}\right) = f\left(\frac{x_2}{x_2+1}\right)$

Since f is 1-1, $\frac{x_1}{x_1+1} = \frac{x_2}{x_2+1}$

By algebra, $x_1(x_2+1) = x_2(x_1+1)$

$\cancel{x_1 x_2} + x_1 = \cancel{x_2 x_1} + x_2$

Thus, $x_1 = x_2$//

3. (18 pts)

Suppose $f : A \to B$ and $g : B \to C$ are functions and define $h : A \to C$ by $h(x) = g(f(x))$ for all $x \in A$. Assume all the sets A, B and C are the set of real numbers $\mathbb{R}$ (labeled differently just for easy reference in your proof).

Two of the statements below are TRUE and two of the statements are FALSE. Correctly circle which are TRUE and which are FALSE.

(a) If f and g are decreasing, then h is decreasing.	TRUE	FALSE
(b) If f and g are surjective, then h is surjective.	TRUE	FALSE
(c) If g is bounded, then h is bounded.	TRUE	FALSE
(d) If f is bounded, then h is bounded.	TRUE	FALSE

- Provide counterexamples for both the statements that you said were false.

(a) $f(x) = -2x$, $g(x) = -3x$ so $h(x) = g(f(x)) = -3(-2x) = 6x$
$f: \mathbb{R} \to \mathbb{R}$ $\quad g: \mathbb{R} \to \mathbb{R}$ $\quad h: \mathbb{R} \to \mathbb{R}$

(d) $f(x) = \sin(x)$ $\quad g(x) = \begin{cases} \frac{1}{x}, & x \neq 0 \\ 0, & x = 0 \end{cases}$
$f: \mathbb{R} \to \mathbb{R}$ $\quad g: \mathbb{R} \to \mathbb{R}$

- Give a proof for ONE of the statements you said was true, you can pick whichever you want. (If you attempt to prove both, clearly indicated which one you want me to grade. Otherwise, I will average the grades on your two proofs. If you give completely correct proofs for both true statements, I will award 2 bonus points.)

(b) pf Assume f and g are onto.
Let $y \in C$. Since g is onto, $\exists b \in B$ s.t. $g(b) = y$.
Since f is onto, $\exists x \in A$ s.t. $f(x) = b$.
By substitution, $g(f(x)) = y$, so $h(x) = y$ for some $x \in A$ //

(c) pf Assume g is bnded. By def'n of bounded, $\exists M \in \mathbb{R}$ such that $|g(b)| \leq M$ for all $b \in B$.
If $x \in A$, then $h(x) = g(f(x))$ by the given def'n. Since f is a function, $f(x) = b$ for some $b \in B$.
Thus, $|h(x)| = |g(b)| \leq M$. So $|h(x)| \leq M$ for all $x \in A$ //

4. (8 pts) Your poorly designed robot has two walking functions.
It can either take large steps of exactly 33 inches forward or back, or it can take short steps of exactly 27 inches forward or back. Thus, the only distances that the robot can travel exactly are the distances that can be expressed as $33x + 27y$ for some integers x and y.

(a) Using appropriate reference to a theorem from class, describe ALL the distances that the robot can exactly travel.

$33x+27y=c$ is only possible, with $x,y \in \mathbb{Z}$, when $\gcd(33,27)$ divides c by the LDE thm. So we need $\boxed{3 \mid c}$

(b) Find one solution, $x, y \in \mathbb{Z}$, to the equation $33x + 27y = 9$.
(Hint: We have a systematic algorithm to do this.)

$33 = 1 \cdot 27 + 6$
$27 = 4 \cdot 6 + 3$
$6 = 2 \cdot 3$

So
$3 = 27 - 4 \cdot 6$
$3 = 27 - 4(33-27)$
$3 = 27 - 4(33) + 4(27)$
$3 = 33(-4) + 27(5)$
$\times 3$ $\quad \downarrow \times 3 \quad \downarrow \times 3$
$9 = 33(-12) + 27(15)$

one sol'n
there are ∞'ly many others

$\boxed{x = -12} \quad \boxed{y = 15}$

5. (12 pts) Let $k \in \mathbb{Z}$ with $k \geq 0$. Using induction on n, prove that for all integers $n \geq 0$,

From homework $\longrightarrow$
$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

pf) Let $k \in \mathbb{Z}$, $k \geq 0$ be arbitrary. We use induction on n.

$\boxed{\text{BASE}}$ For $n=0$, $\sum_{i=0}^{n} \binom{i}{k} = \binom{0}{k} = \begin{cases} 1, & \text{if } k=0; \\ 0, & \text{if } k>0. \end{cases}$

and $\binom{n+1}{k+1} = \binom{1}{k+1} = \begin{cases} 1, & \text{if } k=0; \\ 0, & \text{if } k>0. \end{cases}$ ✓

$\boxed{\text{IND STEP}}$ Assume $\sum_{i=0}^{m} \binom{i}{k} = \binom{m+1}{k+1}$ for some $m \in \mathbb{Z}$, $m \geq 0$.

$\sum_{i=0}^{m+1} \binom{i}{k} = \binom{m+1}{k} + \sum_{i=0}^{m} \binom{i}{k}$ (pulling out the last term)

$= \binom{m+1}{k} + \binom{m+1}{k+1}$ (by induction hypothesis)

$= \binom{m+2}{k+1}$ (by Pascal's identity).

$= \binom{(m+1)+1}{k+1}$ //

6. (a) (8 pts) Prove that for all $n \in \mathbb{N}$, if 6 divides n, then 9 divides $3^n + 2^n - 1$.

pf) By def'n, $6 | n$ means $\exists k \in \mathbb{Z}$ such that $n = 6k$.

Thus, $3^n + 2^n - 1 = 3^{6k} + 2^{6k} - 1 = 9^{3k} + 8^{2k} - 1$.

Since $9 \equiv 0 \pmod 9$ and $8 \equiv -1 \pmod 9$, by the replacement theorem, $9^{3k} + 8^{2k} - 1 \equiv 0^{3k} + (-1)^{2k} - 1 \pmod 9$

$\equiv 0 \pmod 9$

Hence, 9 divides $3^n + 2^n - 1$ //

(b) (4 pts) Find a counterexample to the statement:
For all $n \in \mathbb{N}$, $x^2 \equiv 1 \pmod n$ if and only if $x \equiv 1 \pmod n$ or $x \equiv -1 \pmod n$.
(Hint: You may have to try a few different values for n before you come up with a counterexample, it will help to peek at the next part).

$\boxed{n = 8}$ $x^2 \equiv 1 \pmod 8$ for $x \equiv 1 \pmod 8$, $x \equiv -1 \pmod 8$ and $x \equiv 3 \pmod 8$

because $3^2 \equiv 9 \equiv 1 \pmod 8$.

(c) (10 pts) Let p be a prime number.
Prove that $x^2 \equiv 1 \pmod p$ **if and only if** $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$.
(Hint: It might help to rewrite it as a divisibility problem for one of the directions.)

pf)

($\Leftarrow$) Assume $x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$.

$\boxed{\text{CASE 1}}$ If $x \equiv 1 \pmod p$, then, by the replacement theorem, $x^2 \equiv 1^2 \equiv 1 \pmod p$.

$\boxed{\text{CASE 2}}$ If $x \equiv -1 \pmod p$, then, again by the replacement theorem, $x^2 \equiv (-1)^2 \equiv 1 \pmod p$.

($\Rightarrow$) Assume $x^2 \equiv 1 \pmod p$.

By def'n of congruence, $p | (x^2 - 1)$.

Factoring, $p | (x+1)(x-1)$.

Since p is a prime, $p | (x+1)$ or $p | (x-1)$. (as proven in class)

Thus, $x \equiv -1 \pmod p$ or $x \equiv 1 \pmod p$. //