1. (a) (12 pts) Let $f : A \to B$ and $g : B \to C$ be functions, where $A, B, C \subseteq \mathbb{R}$. For the definitions below, identify the definition (tell me the name of what is being defined) and give the negation of the statement

i. $\forall x_1, x_2 \in A$, if $x_1 < x_2$, then $f(x_1) > f(x_2)$. NAME OF DEF'N: $\boxed{f \text{ decreasing}}$

NEGATION: $\boxed{\exists x_1, x_2 \in A \text{ s.t. } x_1 < x_2 \text{ AND } f(x_1) \leq f(x_2)}$

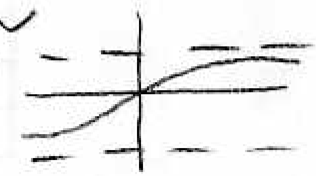
ii. $\exists M \in \mathbb{R}$ such that $\forall x \in \mathbb{R}$, $|f(x)| \leq M$. NAME OF DEF'N: $\boxed{f \text{ bounded}}$

NEGATION: $\boxed{\forall M \in \mathbb{R},\ \exists x \in \mathbb{R} \text{ s.t. } |f(x)| > M}$

(b) (4 pts) Give a specific counterexample to the statement:
Every injective function from $\mathbb{R}$ to $\mathbb{R}$ is not bounded.

$\boxed{f(x) = \arctan(x)}$

INJECTIVE ✓
BOUNDED ✓



(c) Consider the statement:
For all $n, a, b \in \mathbb{N}$, if $ab \equiv 0 \pmod{n}$, then $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.

i. (4 pts) Give a specific counterexample to the statement.

$\boxed{a = 2 \quad b = 3 \quad n = 6}$

$2 \cdot 3 \equiv 0 \pmod{6}$
$2 \not\equiv 0 \pmod{6}$
$3 \not\equiv 0 \pmod{6}$

ii. (3 pts) Give a condition on n that makes the statement true.

$\boxed{n \text{ is a prime}}$

(d) (8 pts) Use congruence arithmetic to simplify and solve for an integer x such that $0 \leq x < 7$ and $6^{411}x + 8^{911} + 2 \equiv 23^6 \pmod{7}$. (You must show your work to get credit).

Replacement $\rightarrow$ $(-1)^{411}x + 1^{911} + 2 \equiv 2^6 \pmod{7}$

Simplify $\rightarrow$ $-x + 1 + 2 \equiv 2^6 \pmod{7}$

Fermat's Little Thm $\rightarrow$ $-x + 3 \equiv 1 \pmod{7}$

Simplify $\rightarrow$ $-x \equiv -2 \pmod{7}$

Cancellation $\gcd(-1, 7) = 1$ $\rightarrow$ $\boxed{x \equiv 2 \pmod{7}}$

2. (a) (12 pts) Let A, B, and C be sets.
Using a formal, and properly structure, subset proof with proper reference to definitions, logic and de'Morgan's law, prove $A \cap (B - (A \cap C)) \subseteq B \cap (A - C)$.

Let $x \in A \cap (B - (A \cap C))$. By def'n, $x \in A$ AND $x \in B - (A \cap C)$.

So $x \in A$ AND $x \in B$ AND $x \in (A \cap C)^c$. Hence, $x \in A$ AND $x \in B$

AND $(x \in A^c \cup C^c)$, by de Morgan's law. Since $x \in A$, $x \in A^c$ is false

it must be the case that $x \in C^c$ to make $x \in A^c$ or $x \in C^c$ true.

Thus, $x \in A$ AND $x \in B$ AND $x \in C^c$.

Since $x \in A$ and $x \in C^c$, by def'n, $x \in A - C$.

Hence, $x \in B$ AND $x \in A - C$, so $x \in B \cap (A - C)$. //

(b) Let $f : A \to B$ and $g : B \to C$ be functions.
Define $h : A \to C$ by $h(x) = g(f(x))$ for all $x \in A$.

i. (6 pts) Give a specific counterexample (give me your functions and sets) to the statement: If h is surjective, then f is surjective.

$A = \{1\}$ $\quad B = \{2, 3\}$ $\quad C = \{4\}$

$\underbrace{f(1) = 2}_{\text{NOT SURJECTIVE}}$ ✓ $\quad g(2) = 4$ $\quad g(3) = 4$ $\quad \underbrace{h(1) = g(f(1)) = g(2) = 4}_{\text{surjective}}$ ✓

ii. (5 pts) Consider the following theorem. *Theorem:* If h is injective, then f is injective.
Now is your chance to be a proof grader. Of the three "proofs" below, only ONE is correct. Which is the correct proof? And why?

('Proof' 1) Assume $h(x_1) = h(x_2)$. By definition of h, $g(f(x_1)) = g(f(x_2))$. Since h is injective, $x_1 = x_2$, so $f(x_1) = f(x_2)$. Since we have $f(x_1) = f(x_2)$ and $x_1 = x_2$, f is injective.
('Proof' 2) Assume $x_1 = x_2$ for $x_1, x_2 \in A$. Since f and g are well-defined, $f(x_1) = f(x_2)$ and $g(f(x_1)) = g(f(x_2))$. Thus, $h(x_1) = h(x_2)$. Since h is injective, we have $x_1 = x_2$, so f is injective.
('Proof' 3) Assume $f(x_1) = f(x_2)$. Since g is well-defined, $g(f(x_1)) = g(f(x_2))$. Thus, $h(x_1) = h(x_2)$. Since h is injective, $x_1 = x_2$. Hence, f is injective.

ANSWER AND EXPLANATION:

$\boxed{\text{Proof 3 is correct}}$ to show f is injective

we must start with $f(x_1) = f(x_2)$ and prove $x_1 = x_2$

3. (a) (12 pts) By using a precisely worded induction proof, prove $3^n > 2^{n+1}$ for all integers $n \geq 2$.

$\boxed{\text{BASE STEP}}$ For $n=2$, $3^n = 9$ and $2^{n+1} = 2^3 = 8$

and $3^2 = 9 > 8 = 2^{2+1}$.

$\boxed{\text{IND STEP}}$ Assume $3^k > 2^{k+1}$ for some integer $k \geq 2$.

Thus, $3^{k+1} = 3 \cdot 3^k > 3 \cdot 2^{k+1}$ (multiplying ind. hyp. by 3)

Since $3 > 2$, $3 \cdot 2^{k+1} > 2 \cdot 2^{k+1} = 2^{k+2}$.

Hence, by transitivity, $3^{k+1} > 2^{k+2}$.

By the principle of mathematical induction, $3^n > 2^{n+1}$ $\forall n \in \mathbb{Z}, n \geq 2$ //

(b) (9 pts) $\forall a, b, c, d \in \mathbb{N}$, prove if $\gcd(a+b, c) = 2d$, $\gcd(a, b) = 28$, and $14|c$, then $7|d$.

Since $14|c$, $\exists k \in \mathbb{Z}$ s.t. $c = 14k$.

Since $\gcd(a,b) = 28$, $28|a$ and $28|b$, so $\exists m, n \in \mathbb{Z}$ s.t. $a = 28m$ and $b = 28n$.

By the LDE Theorem, $\exists x, y \in \mathbb{Z}$ s.t. $(a+b)x + cy = 2d$.

By substitution, $(28m + 28n)x + 14ky = 2d$

$\Rightarrow 14[(2m+2n)x + ky] = 2d$

$\Rightarrow 7[(2m+2n)x + ky] = d$.

Thus, $7|d$ //

4. (a) Let a, b and c be integers.

i. (6 pts) Using the definition of even and odd, prove if c^3 is even, then c is even. (Hint: Prove the contrapositive.)

If c is odd, then $\exists k \in \mathbb{Z}$ s.t. $c = 2k+1$.

Hence, $c^3 = (2k+1)^3 = 8k^3 + 3 \cdot 4k^2 + 3 \cdot 2k + 1$
$= 2(4k^3 + 6k^2 + 3k) + 1$

So c^3 is odd //

ii. (10 pts) Using a proof by contradiction, prove if $(2a-1)^2 + (2b-1)^2 = c^3$, then a is odd or b is odd.

Assume $(2a-1)^2 + (2b-1)^2 = c^3$ AND a is even and b is even.

Then $\exists k, l \in \mathbb{Z}$ s.t. $a = 2k$ and $b = 2l$, so

$(4k-1)^2 + (4l-1)^2 = c^3$

$16k^2 - 8k + 1 + 16l^2 - 8l + 1 = c^3$

$8(2k^2 - k + 2l^2 - l) + 2 = c^3$

So c^3 is even $\Rightarrow$ c is even $\Rightarrow$ $c = 2m$ for some $m \in \mathbb{Z}$.

Hence, $8(2k^2 - k + 2l^2 - l) + 2 = 8m^3$ $\rightarrow\leftarrow$.

(b) (9 pts) Prove if p is a prime number and $p > 4$, then $p^2 - 1 \equiv 0 \pmod{12}$.

Since p is a prime and $p > 4$, $2 \nmid p$ and $3 \nmid p$.

Thus, $p = 12q + r$ is not possible with $r = 0, 2, 3, 4, 6, 8, 9$, or 10

because then p would be divisible by 2 or 3.

Hence, $p \equiv 1, 5, 7$, or $11 \pmod{12}$. Now we check these cases:

① If $p \equiv 1 \pmod{12}$, then $p^2 - 1 \equiv 1^2 - 1 \equiv 0 \pmod{12}$

② If $p \equiv 5 \pmod{12}$, then $p^2 - 1 \equiv 25 - 1 \equiv 0 \pmod{12}$.

③ If $p \equiv 7 \pmod{12}$, then $p^2 - 1 \equiv 49 - 1 \equiv 0 \pmod{12}$

④ If $p \equiv 11 \pmod{12}$, then $p^2 - 1 \equiv 121 - 1 \equiv 0 \pmod{12}$

Hence, $p^2 - 1 \equiv 0 \pmod{12}$ //