MHF3202
HW3

Oliver Deng

February 24, 2025

Question 1

Lemma 0.0.1 Given an $x \in \mathbb{Z}$, it must be written as only one of two forms $x = 2c$ or $x = 2c + 1$ for some $c \in \mathbb{Z}$

Proof: Suppose that $x \in \mathbb{Z}$.
By the division algorithm, we have unique integers c and r such that $x = 2c + r$, since $x \in \mathbb{Z}$, and we also have that $0 \leq r < 2$.
r must be either 0 or 1, but not both, since r is unique, so x can either be written as $x = 2c$ or $x = 2c + 1$. ☺

Proof: Suppose $x \in \mathbb{Z}$.

First, we show that if x is even, then it is not odd.
Suppose x is even.
If x is even, then by definition it can be written as $x = 2m$ for some $m \in \mathbb{Z}$.
By lemma 0.0.1, x cannot cannot then be written in the form $x = 2m + 1$.
Hence, x cannot be odd by definition of odd numbers.

Conversely, we show that if x is not odd, then it is even.
Suppose that x is not odd.
If x is not odd, then it cannot be written in the form $x = 2k + 1$ for some $k \in \mathbb{Z}$.
By lemma 0.0.1, x must be written in the form $x = 2k$.
Hence, by definition, x is even. ☺

Question 2

Lemma 0.0.2 For any $x, n \in \mathbb{N}$ with $x > 2$, $x^n - 1 = (1 + x + x^2 + x^3 + \ldots + x^{n-1})(x - 1)$

Proof: Fix $n,\ x \in \mathbb{N}$ arbitrarily with $x > 2$.
Observe that $x(1 + x + x^2 + x^3 + \ldots + x^{n-1}) = x + x^2 + x^3 + x^4 + \ldots + x^n$ and $-1(1 + x + x^2 + x^3 + \ldots + x^{n-1}) = -1 - x - x^2 - x^3 - \ldots - x^{n-1}$.
By distribution, $(1 + x + x^2 + x^3 + \ldots + x^{n-1})(x - 1) = x + x^2 + x^3 + x^4 + \ldots + x^n - (1 + x + x^2 + x^3 + \ldots + x^{n-1}) = x^n - 1$.
By choice of n and $x > 2$ arbitrary our conclusion follows. ☺

Proof: Suppose $x \in \mathbb{N}$ with $x > 2$, and let $n \in \mathbb{N}$.
By the difference of squares, $(x^{2n} - 1) = (x^n - 1)(x^n + 1)$.
By lemma 0.0.2, we have that

$$x^{2n} - 1 = (x^n + 1)(x^n - 1) = (1 + x + x^2 + x^3 + \ldots + x^{n-1})(x - 1)(x^n + 1). \tag{0.0.1}$$

Notice that since the produce and sum of integers is an integer, there is a $a \in \mathbb{Z}$ such that $a = (1 + x + x^2 + x^3 + \ldots + x^{n-1})(x^n + 1)$.
So by equation 0.0.1,

$$x^{2n-1} = (x - 1)(1 + x + x^2 + x^3 + \ldots + x^{n-1})(x^n + 1) = (x - 1)a.$$

Hence, since $a \in \mathbb{Z}$, $x - 1 \mid x^{2n} - 1$ by definition of divisibility. ☺

Question 3

Proof: Suppose that $x \in \mathbb{Z}$ is odd.
Then $x = 2k + 1$ for some $k \in \mathbb{Z}$, by the definition of an odd number.

Then, $x^2+3x+2 = (2k+1)^2+3(2k+1)+2 = (4k^2+4k+1)+(6k+3)+2 = 4k^2+10k+6 = 2(2k^2+5k+3)$.
Thus, $x^2+3x+2 = 2n$, where $n = 2k^2+5k+3 \in \mathbb{Z}$.
Hence, by the definition of an even number, x^2+3x+2 is even. 😊

Question 4

Proof: Let $x \equiv 3 \pmod 5$, where $z \in \mathbb{Z}$.
By definition of congruence of integers, $5 \mid (x-3)$.
Then, by definition of divisibility, $x-3 = 5m$ for some $m \in \mathbb{Z}$.
Adding 3 to both sides, this turns into $x = 5m+3$.

Case 1: $k = 1$

Fix $n = 4$.

Then $x^n = x^4$.

Observe that $x^4 = (5m+3)^4 = 625m^4 + 1500m^3 + 1350m^2 + 540m + 81$.

We can rewrite this as $x^4 = 5(125m^4 + 300m^3 + 270m^2 + 108m + 16) + 1$.

Subtracting 1 from both sides, we get $x^4 - 1 = 5(125m^4 + 300m^3 + 270m^2 + 108m + 16)$.

This is equivalent to $x^4 - 1 = 5j$ for the integer $j = 125m^4 + 300m^3 + 270m^2 + 108m + 16$.

By definition of divisibility, we have that $5 \mid x^4 - 1$.

Hence, by definition of congruence of integers, $x^4 \equiv 1 \pmod 5$, and $x^n \equiv 1 \pmod 5$ is satisfied.

Case 2: $k = 2$

Fix $n = 3$.

Then $x^n = x^3$.

Observe that $x = (5m+3)^3 = 125m^3 + 225m^2 + 135m + 27$.

We can rewrite this as $x^3 = 5(25m^3 + 45m^2 + 27m + 5) + 2$.

Subtracting 2 from both sides, we get $x^3 - 2 = 5(25m^3 + 45m^2 + 27m + 5)$.

This is equivalent to $x^3 - 2 = 5l$ for the integer $l = 25m^3 + 45m^2 + 27m + 5$.

By definition of divisibility, we have that $5 \mid x^3 - 2$.

Hence, by definition of congruence of integers, $x^3 \equiv 2 \pmod 5$, and $x^n \equiv 2 \pmod 5$ is satisfied.

Case 3: $k = 3$

Fix $n = 1$.

Then $x^n = x^1 = x$.

Since $x = 5m+3$, we can subtract 3 from both sides to get $x - 3 = 5m$.

By definition of divisibility, we have that $5 \mid x - 3$.

Hence, by definition of congruence of integers, $x \equiv 3 \pmod 5$, and $x^n \equiv 3 \pmod 5$ is satisfied.

Case 4: $k = 4$

Squaring both sides of $x^3 \equiv 2 \pmod 5$ from case 2, we get $x^6 \equiv 4 \pmod 5$ from a result in the textbook.

Hence, if we fix $n = 6$, $x^n \equiv 4 \pmod 5$ is satisfied.

Hence, by our cases, for each integer k, $0 < k < 5$, there exists n such that $x^n \equiv k \pmod 5$. 😊

Question 5

Proof: Let $x, y \in \mathbb{R}^+ = (0, \infty)$.
Suppose that $x \leq y$.
Subtracting from both sides, we get $x - y \leq 0$.
We can rewrite this as $\sqrt{x}^2 + \sqrt{y}^2 \leq 0$.
Factoring this as a difference of squares, we get $(\sqrt{x} + \sqrt{y})(\sqrt{x} - \sqrt{y}) \leq 0$.
Since $x \neq 0$ and $y \neq 0$, we know that $\sqrt{x} + \sqrt{y} \neq 0$, and so we can divide both sides of $(\sqrt{x} + \sqrt{y})(\sqrt{x} - \sqrt{y}) \leq 0$ to get $\sqrt{x} - \sqrt{y} \leq 0$.
Adding $\sqrt{y}$ to both sides yields $\sqrt{x} \leq \sqrt{y}$.
Hence $\sqrt{x} \leq \sqrt{y}$. 😊

Question 6

Proof: Let $x, y \in \mathbb{R}^+$.
Observe that $0 \leq (x - y)^2$.
This is equal to $0 \leq x^2 - 2xy + y^2$.
Adding $4xy$ to both sides, we get $4xy \leq x^2 + 2xy + y^2$.
This is equal to $4xy \leq (x + y)^2$.
We can take the square root of both sides, and based on the result from Problem 5, we get $2\sqrt{xy} \leq x + y$.
Hence, $2\sqrt{xy} \leq x + y$. 😊

Question 7

Proof: Let $a, b, c \in \mathbb{Z}$, and suppose $a \mid b$ and $b \mid c$.
Then, by the definition of divisibility, we have $d, e \in \mathbb{Z}$ such that $a = bd$ and $b = ce$.
Substituting, we get $a = (ce)d = c(ed) = cf$, where $f = ed \in \mathbb{Z}$.
Hence, by the definition of divisibility, $a \mid b$. 😊

Question 8

Claim: a must be an element of the set $S = \{-1, 0, 1\}$ if $a^2 \mid a$.

Proof: Suppose by way of contradiction that $a \in \mathbb{Z}$ is not an element of $S = \{-1, 0, 1\}$.
Suppose $a^2 \mid a$.
Then by definition of divisibility, $a = a^2 m$ for some $m \in \mathbb{Z}$.
We can divide both sides by a^2 since $a \neq 0$, which yields $\frac{1}{a} = m$.
However, this is a contradiction, since if $a \notin S$, then either $0 < \frac{1}{a} < 1$ or $-1 < \frac{1}{a} < 0$ which means that it is not an integer, even though m is an integer. 😊

Note

I wasn't sure of the exact wording you wanted so I proved it both ways if that's okay.

Claim: If a is an element of the set $S = \{-1, 0, 1\}$, then $a^2 \mid a$.

Proof: Let $a \in S = \{-1, 0, 1\}$.

Case 1: $a = -1$

Suppose $a = -1$.

Then $a^2 = 1$.

Observe, $a^2 = 1 = -1(-1) = a(-1)$.

Then by definition of divisibility, $a^2 \mid a$.

Case 2: $a = 0$

Suppose $a = 0$.

Then $a^2 = 0$.

Observe, $a^2 = 0 = 0(0) = a(0)$.

Then by definition of divisibility, $a^2 \mid a$.

Case 3: $a = 1$

Suppose $a = 1$.

Then $a^2 = 1$.

Observe, $a^2 = 1 = 1(1) = a(1)$.

Then by definition of divisibility, $a^2 \mid a$.

😊

Question 9

Proof: Let $a, b \in \mathbb{Z}$.
Observe that $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
Subtracting $a^3 + b^3$ from both sides, we get $(a+b)^3 - (a^3 + b^3) = 3a^2b + 3ab^2 = 3(a^2b + ab^2)$.
Then, $(a+b)^3 - (a^3 + b^3) = 3k$, where $k = a^2b + ab^2 \in \mathbb{Z}$.
By definition of divisibility, $3 \mid (a+b)^3 - (a^3 + b^3)$.
Hence, by definition of congruence of integers, $(a+b)^3 \equiv a^3 + b^3 \pmod 3$. 😊

Question 10

Proof: Let $a, b \in \mathbb{Z}$.
Observe that $(a+b)^2 = a^2 + 2ab + b^2$.
Subtracting $a^2 + b^2$ from both sides, we get $(a+b)^2 - (a^2 + b^2) = 2ab$.
Then, $(a+b)^2 - (a^2 + b^2) = 2k$ for $k = ab \in \mathbb{Z}$.
By definition of divisibility, $2 \mid (a+b)^2 - (a^2 + b^2)$.
Hence, by definition of congruence of integers, $(a+b)^2 \equiv a^2 + b^2 \pmod 2$, and $n = 2$, so we have existence.

Next, suppose $\forall a, b \in \mathbb{Z}, (a+b)^2 \equiv a^2 + b^2 \pmod n$, where $n \in (\mathbb{N} \setminus \{1\})$.
Suppose by way of contradiction that $n > 2$.
By definition of congruence of integers, $n \mid ((a+b)^2 - (a^2 + b^2))$.
Then, by definition of divisibility, $(a+b)^2 - (a^2 + b^2) = nm$ for some $m \in \mathbb{Z}$.
Expanding, we get $a^2 + 2ab + b^2 - a^2 - b^2 = mn$, which simplifies to $2ab = mn$.
However, if we choose $a = b = 1$, then $2 = mn$.
Then $\frac{2}{n} = m$, and since $n > 2$, $0 < \frac{2}{n} < 1$, and $\frac{2}{n} \notin \mathbb{Z}$.
However, this is a contradiction, since $m \in \mathbb{Z}$, and we have uniqueness. 😊