CSC165H1: Problem Set 2

Due Wednesday October 25 before 10pm

Question 1

(a)

Proof: Let $n \in \mathbb{N}^+$

$n^2 + 3n + 2$

$= n^2 + \left(2 \cdot \frac{3}{2}\right) n + (\frac{3}{2})^2 - \frac{1}{4}$

$= (n + \frac{3}{2})^2 - \frac{1}{4}$

Since $n \geq 1$

$(n + \frac{3}{2})^2 - \frac{1}{4} \geq 6 > 1$

$n^2 + 3n + 2$

$= (n+1)(n+2)$

Since $(n+1), (n+2) \in \mathbb{Z}$ and $(n+1), (n+2) \notin \{1, n^2 + 3n + 2\}$

$n^2 + 3n + 2$ is not prime ■

(b)

Proof: Let $n \in \mathbb{N}^+$

$n^2 + 6n + 5$

$= n^2 + (2 \cdot 3)n + 3^2 - 4$

$= (n+3)^2 - 4$

Since $n \geq 1$

$(n+3)^2 - 4 \geq 12 > 1$

$n^2 + 6n + 5$

$= (n+1)(n+5)$

Since $(n+1), (n+5) \in \mathbb{Z}$ and $(n+1), (n+5) \notin \{1, n^2 + 6n + 5\}$

$n^2 + 6n + 5$ is not prime ■

Question 2

(a)

Translation: $\exists m \in \mathcal{L}$ s.t. $\forall n \in \mathcal{L}, m \leq n$

Proof: We know that, any non-empty, finite set of real numbers has a minimum element

Let $c, d \in \mathbb{N}^+$

Divide $\mathcal{L}$ into 2 parts: $\mathcal{L}_1, \mathcal{L}_2$

with c be the biggest element in $\mathcal{L}_1$, and d be the smallest element in $\mathcal{L}_2$

and every elements in $\mathcal{L}_1$ are smaller than elements in $\mathcal{L}_2$

Since for any $a, b \in \mathbb{N}$, there must exist some $x, y \in \mathbb{Z}$, which can make ax+by > 0

Then $\mathcal{L}_1$ is not an empty set

Since the smallest value in $\mathcal{L}_1$ must be desirable
Which means $\mathcal{L}_1$ must be finite on its left-side
At the same time in $\mathcal{L}_1$ has a biggest element, c, on its right-side
Which means $\mathcal{L}_1$ must be finite on its right-side
Hence $\mathcal{L}_1$ is a finite set
And $\mathcal{L}_1$ has a minimum element m
Because and every elements in $\mathcal{L}_1$ are smaller than elements in $\mathcal{L}_2$
m is smaller than elements in $\mathcal{L}_2$
Which means $\mathcal{L}$ has a minimum element m ■

(b)

Translation: $(\exists \mathrm{m} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_1, \mathrm{y}_1 \in \mathbb{Z}, \mathrm{m} = \mathrm{ax}_1 + \mathrm{by}_1) \wedge (\forall \mathrm{n} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_2, \mathrm{y}_2 \in \mathbb{Z}, \mathrm{n} = \mathrm{ax}_2 + \mathrm{by}_2 \Longrightarrow \mathrm{n} \geq \mathrm{m}) \wedge (\forall \mathrm{k} \in \mathbb{N}^+, \exists \mathrm{x}_3, \mathrm{y}_3 \in \mathbb{Z}, \mathrm{km} = \mathrm{ax}_3 + \mathrm{by}_3)$

Proof: According to (a) we know $(\exists \mathrm{m} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_1, \mathrm{y}_1 \in \mathbb{Z}, \mathrm{m} = \mathrm{ax}_1 + \mathrm{by}_1) \wedge (\forall \mathrm{n} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_2, \mathrm{y}_2 \in \mathbb{Z}, \mathrm{n} = \mathrm{ax}_2 + \mathrm{by}_2 \Longrightarrow \mathrm{n} \geq \mathrm{m})$
Which means m is the smallest element in $\mathcal{L}$
Let $\mathrm{k} \in \mathbb{N}^+$
Take $\mathrm{x}_3 = \mathrm{kx}_1, \mathrm{y}_3 = \mathrm{ky}_1$
Then $\mathrm{ax}_3 + \mathrm{by}_3 = \mathrm{akx}_1 + \mathrm{bky}_1$
$= \mathrm{k}(\mathrm{ax}_1 + \mathrm{by}_1)$
$= \mathrm{km}$ ■

(c)

Translation: $(\exists \mathrm{m} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_1, \mathrm{y}_1 \in \mathbb{Z}, \mathrm{m} = \mathrm{ax}_1 + \mathrm{by}_1) \wedge (\forall \mathrm{n} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_2, \mathrm{y}_2 \in \mathbb{Z}, \mathrm{n} = \mathrm{ax}_2 + \mathrm{by}_2 \Longrightarrow \mathrm{n} \geq \mathrm{m}) \wedge (\forall \mathrm{c} \in \mathbb{N}^+, (\exists \mathrm{x}_3, \mathrm{y}_3 \in \mathbb{Z}, \mathrm{c} = \mathrm{ax}_3 + \mathrm{by}_3) \Longrightarrow (\exists \mathrm{t} \in \mathbb{Z}, \mathrm{c} = \mathrm{tm})$

Proof: According to (a) we know $(\exists \mathrm{m} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_1, \mathrm{y}_1 \in \mathbb{Z}, \mathrm{m} = \mathrm{ax}_1 + \mathrm{by}_1) \wedge (\forall \mathrm{n} \in \mathbb{N}^+ \text{ s.t. } \exists \mathrm{x}_2, \mathrm{y}_2 \in \mathbb{Z}, \mathrm{n} = \mathrm{ax}_2 + \mathrm{by}_2 \Longrightarrow \mathrm{n} \geq \mathrm{m})$
Which means m is the smallest element in $\mathcal{L}$
Let $\mathrm{c} \in \mathbb{N}^+$
Then we proof by contradiction
Assume $(\exists \mathrm{x}_3, \mathrm{y}_3 \in \mathbb{Z}, \mathrm{c} = \mathrm{ax}_3 + \mathrm{by}_3) \wedge (\forall \mathrm{t} \in \mathbb{Z}, \mathrm{c} \neq \mathrm{tm})$
Then, by Quotient-Remainder Theorem
$\exists \mathrm{r} \in \mathbb{Z}, \mathrm{c} = \mathrm{mt} + \mathrm{r} \wedge 0 < \mathrm{r} < m$
Since $\exists \mathrm{x}_1, \mathrm{y}_1 \in \mathbb{Z}, \mathrm{m} = \mathrm{ax}_1 + \mathrm{by}_1$ and $\exists \mathrm{x}_3, \mathrm{y}_3 \in \mathbb{Z}, \mathrm{c} = \mathrm{ax}_3 + \mathrm{by}_3$
$\mathrm{r} = \mathrm{c} - \mathrm{tm}$
$= \mathrm{ax}_3 + \mathrm{by}_3 - (\mathrm{ax}_1\mathrm{t} + \mathrm{by}_1\mathrm{t})$
$= \mathrm{a}(\mathrm{x}_3 - \mathrm{x}_1\mathrm{t}) + \mathrm{b}(\mathrm{y}_3 - \mathrm{y}_1\mathrm{t})$
Which means r is also a combination of a and b
Since m is the smallest element in $\mathcal{L}$, r > m
which is contradictory to r > m we got before
Hence any element $\mathrm{c} \in \mathcal{L}$ must be a multiple of m ■

(d)

Translation: $(\exists m \in \mathbb{N}^+ \text{ s.t. } \exists x_1, y_1 \in \mathbb{Z}, m = ax_1 + by_1) \land (\forall n \in \mathbb{N}^+ \text{ s.t. } \exists x_2, y_2 \in \mathbb{Z}, n = ax_2 + by_2 \Longrightarrow n \geq m) \land m|a \land m|b$

Proof: According to (a) we know $(\exists m \in \mathbb{N}^+ \text{ s.t. } \exists x_1, y_1 \in \mathbb{Z}, m = ax_1 + by_1) \land (\forall n \in \mathbb{N}^+ \text{ s.t. } \exists x_2, y_2 \in \mathbb{Z}, n = ax_2 + by_2 \Longrightarrow n \geq m)$

Which means m is the smallest element in $\mathcal{L}$

Firstly, we consider a

Case1: a = 0

Since any integer can divide 0

m | a

Case2: a > 0

Assume $\exists c \in \mathbb{N}^+ \text{ s.t. } \exists x_3, y_3 \in \mathbb{Z}, c = ax_3 + by_3$

Take $x_3 = 1, y_3 = 0$

Then c = a

According to (c): any element $c \in \mathcal{L}$ must be a multiple of m

a is a multiple of m

Hence m|a

Case3: a < 0

Assume $\exists c \in \mathbb{N}^+ \text{ s.t. } \exists x_3, y_3 \in \mathbb{Z}, c = ax_3 + by_3$

Take $x_3 = -1, y_3 = 0$

Then c = -a

According to (c): any element $c \in \mathcal{L}$ must be a multiple of m

-a is a multiple of m

Hence m|a

Similarly, we can prove m|b ■

(e)

Translation: $(\exists m \in \mathbb{N}^+ \text{ s.t. } \exists x_1, y_1 \in \mathbb{Z}, m = ax_1 + by_1) \land (\forall c \in \mathbb{N}^+ \text{ s.t. } \exists x_2, y_2 \in \mathbb{Z}, c = ax_2 + by_2 \Longrightarrow c \geq m) \land (\forall n \in \mathbb{N}, (n|a \land n|b) \Longrightarrow n|m)$

Proof: According to (a) we know $(\exists m \in \mathbb{N}^+ \text{ s.t. } \exists x_1, y_1 \in \mathbb{Z}, m = ax_1 + by_1) \land (\forall c \in \mathbb{N}^+ \text{ s.t. } \exists x_2, y_2 \in \mathbb{Z}, c = ax_2 + by_2 \Longrightarrow c \geq m)$

Which means m is the smallest element in $\mathcal{L}$

Since n|a

We know that $\exists t_1 \in \mathbb{Z} \text{ s.t. } a = t_1 n$

Since n|b

We know that $\exists t_2 \in \mathbb{Z} \text{ s.t. } b = t_2 n$

Then $m = ax_1 + by_1$

$= at_1 n + bt_2 n$

$= n(at_1 + bt_2)$

Since $at_1 + bt_2 \in \mathbb{Z}$

We can conclude n|m ■

(f)

Translation: $(\exists m \in \mathbb{N}^+ \text{ s.t. } \exists x_1, y_1 \in \mathbb{Z}, m = ax_1 + by_1) \wedge (\forall c \in \mathbb{N}^+ \text{ s.t. } \exists x_2, y_2 \in \mathbb{Z}, c = ax_2 + by_2 \Longrightarrow c \geq m) \wedge \gcd(a, b) = m$

According to (d) we know that m is a common divisor of a and b

According to (e) we know that any common divisor of a and b also divides m

Which means that any common divisor of a and b is smaller than m

Hence, m is the greatest common divisor of a and b ■

(g)

Translation: $\forall a, b \in \mathbb{N}, \forall c \in \mathbb{Z}, \gcd(a, b) = 1 \wedge a|bc \Longrightarrow a|c$

Proof: We know that, for any integer a, b, c, d, e, k

If $a \equiv b(\text{mod } e)$ and $c \equiv d(\text{mod } e)$

Then $ac \equiv bd(\text{mod } e)$ and $a^k \equiv b^k(\text{mod } e)$

Since gcd(a, b) = 1

We know that $\exists x, y \in \mathbb{Z} \text{ s.t. } ax + by = 1$

Namely ax = 1 – by

a | 1 – by

$1 \equiv by(\text{mod } a)$

$\frac{1}{b} \cdot 1 \equiv \frac{1}{b} \cdot by(\text{mod } a)$

$\frac{1}{b} \equiv y(\text{mod } a)$

Since a | bc

$bc \equiv 0(\text{mod } a)$

Hence $\frac{1}{b} \cdot bc \equiv y \cdot 0(\text{mod } a)$

$c \equiv 0(\text{mod } a)$

Namely a | c ■

Question3

(a)

Proof: Assume that this statement is false

Namely, $P = \{p|\text{Prime}(p) \wedge p \equiv 3(\text{mod}4)\}$ is infinite.

Let $k \in \mathbb{N}$ be the number of primes in P, and let $p_1, p_2, \dots, p_k$ be those prime numbers

Our statement Q will be “$\forall n \in \mathbb{N}, (\text{Prime}(n) \wedge n \equiv 3(\text{mod}4)) \Longleftrightarrow n \in P$”

Q is True because of our assumption that $P = \{p|\text{Prime}(p) \wedge p \equiv 3(\text{mod}4)\}$ is finite, and the definitions of k and $p_1, p_2, \dots, p_k$.

Now we will show that Q is False:

Define the number $s = 4p_1p_2 \dots p_k - 1$

Since $4 \mid 4p_1p_2 \dots p_k$

$s \equiv 3(\text{mod}4)$

Then there must exists some prime c such that c|s

Then we have 4 situations: $c \equiv 0(\text{mod}4), c \equiv 1(\text{mod}4), c \equiv 2(\text{mod}4), c \equiv 3(\text{mod}4)$

Because s is an odd number

c must be an odd number

Then $c \equiv 0(\mathrm{mod}4)$ and $c \equiv 2(\mathrm{mod}4)$ are impossible

If $c \equiv 3(\mathrm{mod}4)$

Then $c \in \{p_1, p_2, \dots, p_k\}$ and $c \mid 4p_1p_2 \dots p_k$

Then $c \mid 4p_1p_2 \dots p_k - 1 - 4p_1p_2 \dots p_k = 1$

Since the only integer which can divide 1 is 1 itself and 1 is not a prime

$c \equiv 3(\mathrm{mod}4)$ is impossible

If $c \equiv 1(\mathrm{mod}4)$

Since we have already proved that

$c \equiv 0(\mathrm{mod}4), c \equiv 2(\mathrm{mod}4), c \equiv 3(\mathrm{mod}4)$ are all impossible

Which means that s can be divided into several primes,

all with remainder 1 when divided by 4

We know that, for any integer a, b, c, d, e, k

$(a \equiv b(\mathrm{mod}\ e) \wedge c \equiv d(\mathrm{mod}\ e)) \Longrightarrow ac \equiv bd(\mathrm{mod}\ e)$

Then $s \equiv 1(\mathrm{mod}4)$, which is contradict to $s \equiv 3(\mathrm{mod}4)$, which we got before

Hence $c \equiv 1(\mathrm{mod}4)$ is impossible

So far we have proved that all possible situations about c, s are wrong when P is finite

Which means $P = \{p | \mathrm{Prime}(p) \wedge p \equiv 3(\mathrm{mod}4)\}$ is infinite ■

Question4

(a)

WTS $\exists n_0 \in \mathbb{R}^+ \mathrm{s.t.} \forall n \in \mathbb{N}, n \geq n_0 \Longrightarrow g(n) \leq f(n)$

Proof: Take $n_0 = 60$

Let h(n) = f(n) – g(n)

Then prove by math induction

Base case: n = 60

g(n) = 1800, f(n) = 1770

$g(n) \leq f(n)$ is True

Induction step: Let $k \in \mathbb{N}$ and $k \geq 60$

Assume $g(k) \leq f(k)$

$h(k) \geq 0$

Which means that $0.5k^2 - 2k + 1650 \geq 0$

$$\begin{aligned} h(k+1) &= 0.5(k+1)^2 - 2(k+1) + 1650 \\ &= 0.5k^2 - 2k + 1650 + k - 1.5 \\ &\geq 0 + k - 1.5 \end{aligned}$$

Since $k \geq 60$

$k - 1.5 > 0$

Which means $h(k+1) \geq 0$

$g(k+1) \leq f(k+1)$ ■

(b)

WTS $\exists n_0 \in \mathbb{R}^+ \mathrm{s.t.} \forall n \in \mathbb{N}, n \geq n_0 \Longrightarrow g(n) \leq f(n)$

Proof: Take $n_0 = a + \sqrt{2b + a^2}$

Let h(n) = f(n) – g(n)

Then prove by math induction

Base case: n = $n_0 = a + \sqrt{2b + a^2}$

$$g(n) = a\left(a + \sqrt{2b + a^2}\right) + b$$

$$= a^2 + b + a\sqrt{2b + a^2}$$

$$f(n) = 0.5(a + \sqrt{2b + a^2})^2$$

$$= 0.5(2a^2 + 2a\sqrt{2b + a^2 + 2b})$$

$$= a^2 + b + a\sqrt{2b + a^2}$$

$g(n) \leq f(n)$ is True

Induction step: Let $k \in \mathbb{N}$ and $k \geq a + \sqrt{2b + a^2}$

Assume $g(k) \leq f(k)$

$h(k) \geq 0$

Which means that $0.5k^2 - ak - b \geq 0$

$$h(k + 1) = 0.5(k + 1)^2 - a(k + 1) - b$$

$$= 0.5k^2 - ak - b + k + 0.5 - a$$

$$\geq 0 + k + 0.5 - a$$

Since $k \geq a + \sqrt{2b + a^2}$

$$0 + k + 0.5 - a \geq 0.5 + \sqrt{2b + a^2} \geq 0$$

Which means $h(k + 1) \geq 0$

$g(k + 1) \leq f(k + 1)$ ■