CSC165H1: Problem Set 2

Due October 25 2017 before 10pm

1.(a) WTS:$\forall n \in \mathbb{N}^+, (n^2+3n+2) > 1 \wedge \neg prime(n^2+3n+2)$

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

- since $n \in \mathbb{N}^+$, $n^2+3n+2 > 2$ so $n^2+3n+2 > 1$
- To show $\neg prime(n^2+3n+2)$ is same to show $n^2+3n+2 \le 1$ or $\exists d \in \mathbb{N}, d|(n^2+3n+2) \wedge d \neq 1 \wedge d \neq (n^2+3n+2)$.Since $n^2+3n+2 > 1$ we want to show$\exists d \in \mathbb{N}, d|(n^2+3n+2) \wedge d \neq 1 \wedge d \neq (n^2+3n+2)$.

  Take d=n+1 since $n \in \mathbb{N}^+, so\ d \in \mathbb{N}$ and $d \neq 1$ and $d \neq (n^2+3n+2)$

  Since (n+1)(n+2)= n^2+3n+2, so $d|(n^2+3n+2)$ ($n+2 \in \mathbb{Z}$ since $n \in \mathbb{N}^+$)

  Hence we have proven $\neg prime(n^2+3n+2)$

We have proven $(n^2+3n+2) > 1 \wedge \neg prime(n^2+3n+2)$ as needed.■

(b) WTS:$\forall n \in \mathbb{N}^+, (n^2+6n+5) > 1 \wedge \neg prime(n^2+6n+5)$

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

- since $n \in \mathbb{N}^+$, $n^2+6n+5 > 5$ so $n^2+6n+5 > 1$
- To show $\neg prime(n^2+6n+5)$ is same to show $n^2+6n+5 \le 1$ or $\exists d \in \mathbb{N}, d|(n^2+6n+5) \wedge d \neq 1 \wedge d \neq (n^2+6n+5)$.Since $n^2+6n+5 > 1$ we want to show$\exists d \in \mathbb{N}, d|(n^2+6n+5) \wedge d \neq 1 \wedge d \neq (n^2+6n+5)$.

  Take d=n+1 since $n \in \mathbb{N}^+, so\ d \in \mathbb{N}$ and $d \neq 1$ and $d \neq (n^2+6n+5)$

  Since (n+1)(n+5)= n^2+6n+5, so $d|(n^2+6n+5)$ ($n+5 \in \mathbb{Z}$ since $n \in \mathbb{N}^+$)

  Hence we have proven $\neg prime(n^2+6n+5)$

We have proven $(n^2+6n+5) > 1 \wedge \neg prime(n^2+6n+5)$ as needed.■

2.(a)WTS:$\exists m \in l, \forall n \in l, n \ge m$

Construct a set A=$\{n \in \mathbb{N}^+ : n \in l \ \wedge\ n \le a+b\}$

- Since $\exists x, y \in \mathbb{Z}, a+b = ax+by, (x=1, y=1)$ and $a+b \in \mathbb{N}^+$ (a, b $\in \mathbb{N}$ and they are not both 0) , so $a+b \in l$, and A is not empty since it has element $a+b$.($a+b \le a+b$)
- Since A=$\{n \in \mathbb{N}^+ : n \in l \ \wedge\ n \le a+b\}$ A is a finite set of real numbers since there are finite positive natural numbers which is smaller than $a+b$

In all A is a non-empty, finite set of real numbers.

Since the fact that any non-empty, finite set of real numbers has a minimum element, A has a minimum element.

Take m be this minimum element. Since $m \in A$, so $m \in l$

Let $n \in l$. I am going to prove $n \ge m$ in two cases:

- $n \le a+b$, then $n \in A$ (since $n \in l \ \wedge\ n \le a+b$),

  thus $n \ge m$ since m is the minimum element of A.
- $n > a+b$,

  since $a+b \in A$, $so\ a+b \ge m$ (since m is the minimum element of A)

  we know $n > a+b\ and\ a+b \ge m$

so $\mathrm{n} \geq \mathrm{m}$

We have proven $\mathrm{n} \geq \mathrm{m}$ as needed. ■

(b)WTS: $\forall \mathrm{k} \in \mathbb{N}^{+}, km \in \mathrm{l}$,where m is introduced in 2(a).

Let $\mathrm{k} \in \mathbb{N}^{+}$

to show $km \in \mathrm{l}$ is to show $\mathrm{km} \in \mathbb{N}^{+}$ *and* $\exists \mathrm{x}, \mathrm{y} \in \mathbb{Z}, \mathrm{km}=\mathrm{ax}+\mathrm{by}$

- Since $\mathrm{k} \in \mathbb{N}^{+}$ and $\mathrm{m} \in \mathbb{N}^{+}$ so $\mathrm{km} \in \mathbb{N}^{+}$
- Since $\mathrm{m} \in \mathrm{l}$, $\exists x_1, y_1 \in \mathbb{Z}, \mathrm{m}=\mathrm{a} x_1+\mathrm{b} y_1$ let x_1, y_1 be that value.

Take x=kx_1,y=ky_1, since $\mathrm{k} \in \mathbb{N}^{+}, x_1, y_1 \in \mathbb{Z}$ so kx_1, k$y_1 \in \mathbb{Z}$

ax+by=a×kx_1+b×ky_1=k$(\mathrm{a}x_1+\mathrm{b}y_1)$=km

we have proven $\mathrm{km} \in \mathbb{N}^{+}$ *and* $\exists \mathrm{x}, \mathrm{y} \in \mathbb{Z}, \mathrm{km}=\mathrm{ax}+\mathrm{by}$ as needed. ■

(c)WTS: $\forall \mathrm{c} \in \mathrm{l}, \exists \mathrm{k} \in \mathbb{Z}, \mathrm{c}=\mathrm{km}$,where m is introduced in 2(a).

We will prove this by contradiction.

Assume $\exists \mathrm{c} \in \mathrm{l}, \forall \mathrm{k} \in \mathbb{Z}, \mathrm{c} \neq \mathrm{km}$

Since $\mathrm{c}, \mathrm{m} \in \mathrm{l}$, so $\mathrm{c}, \mathrm{m} \in \mathbb{Z}^{+}$. thus according to the Quotient-Remainder Theorem, there exist $\mathrm{q}, \mathrm{r} \in \mathbb{Z}$ such that c=qm+r and 0≤ $r<m$ also since $\forall \mathrm{k} \in \mathbb{Z}, \mathrm{c} \neq \mathrm{km}$, so r≠ $\mathbf{0}$, so 0<r<m.

Since $\mathrm{c}, \mathrm{m} \in \mathrm{l}$, $\exists x_1, y_1 \in \mathbb{Z}, \mathrm{c}=\mathrm{a} x_1+\mathrm{b} y_1, \exists x_2, y_2 \in \mathbb{Z}, \mathrm{m}=\mathrm{a} x_2+\mathrm{b} y_2$, let x_1, x_2, y_1, y_2 be that value.

Since c=qm+r so $\mathrm{a}x_1+\mathrm{b}y_1=q(\mathrm{a}x_2+\mathrm{b}y_2)+r,$ hence r=$(x_1-qx_2)a+(y_1-qy_2)b$, *since* $x_1, y_1, x_2, y_2, \mathrm{q} \in \mathbb{Z}$ so $(x_1-qx_2),(y_1-qy_2) \in \mathbb{Z}$ also since 0<r and $\mathrm{r} \in \mathbb{Z}$ so $\mathrm{r} \in \mathbb{N}^{+}$. Hence $\mathrm{r} \in l$, therefore r $\geq \mathrm{m}$ (since m is the minimum element of l). So we get a contradiction with 0<r<m

Hence we have proven $\forall \mathrm{c} \in \mathrm{l}, \exists \mathrm{k} \in \mathbb{Z}, \mathrm{c}=\mathrm{km}$ as needed. ■

(d)WTS: $\mathrm{m}|\mathrm{a} \wedge m| b$,where a,b is introduced in the question and m is introduced in 2(a).

To show $\mathrm{m}|\mathrm{a} \wedge m| b$ is same to show $\exists \mathrm{k} \in \mathbb{Z}, \mathrm{a}=\mathrm{km} \wedge \exists \mathrm{k} \in \mathbb{Z}, \mathrm{b}=\mathrm{km}$

Since $\mathrm{a}, \mathrm{b} \in \mathbb{N}$, and they are not both 0. We can prove the statement in two cases:

For a:

- a=0: take k=0,km=0=a, so $\mathrm{m} | \mathrm{a}$
- a≠ $\mathbf{0}$ so $\mathrm{a} \in \mathbb{N}^{+}$. Take x=1,y=0,(they are both integers) so ax+by=a, hence $\mathrm{a} \in \mathrm{l}$ according to 2(c) , we know that since $\mathrm{a} \in \mathrm{l}, \exists \mathrm{k} \in \mathbb{Z}, \mathrm{a}=\mathrm{km}$, hence $\mathrm{m} | \mathrm{a}$.

For b:

- b=0: take k=0,km=0=b, so $\mathrm{m} | \mathrm{b}$
- b≠ $\mathbf{0}$ so $\mathrm{b} \in \mathbb{N}^{+}$. Take x=0,y=1,(they are both integers) so ax+by=b, hence $\mathrm{b} \in \mathrm{l}$ according to 2(c) , we know that since $\mathrm{b} \in \mathrm{l}, \exists \mathrm{k} \in \mathbb{Z}, \mathrm{b}=\mathrm{km}$, hence $\mathrm{m} | \mathrm{b}$.

Hence we have proven $\mathrm{m}|\mathrm{a} \wedge m| b$ as needed. ■

(e)WTS: $\forall n \in \mathbb{N}, n|a \wedge n|b \Longrightarrow n|m$,where a,b is introduced in the question and m is introduced in 2(a).

Let $n \in \mathbb{N}$,

For n=0 :since $n|a \wedge n|b$ is false, $n|a \wedge n|b \Longrightarrow n|m$ is true.

For $n \neq 0$:we assume $n|a \wedge n|b$, that is $\exists k_1 \in \mathbb{Z}, a = k_1 n$ *and* $\exists k_2 \in \mathbb{Z}, b = k_2 n$, let k_1, k_2 be that value.

We want to show $\exists k \in \mathbb{Z}, m = kn$

Since $m \in l$, $\exists x, y \in \mathbb{Z}, m = ax + by$, let x,y be that value.

Take k=$k_1 x + k_2 y$, since $k_1, k_2, x, y \in \mathbb{Z}$ so $k \in \mathbb{Z}$

kn=$(k_1 x + k_2 y)n = k_1 x \times n + k_2 y \times n$=ax+by=m.

Hence we have proven $n|m$ as needed. ■

(f)WTS: $m|a \wedge m|b \wedge (\forall e \in \mathbb{N}, e|a \wedge e|b \Longrightarrow e \leq m)$,where a,b is introduced in the question and m is introduced in 2(a).

We have proven $m|a \wedge m|b$ in 2(d)

We have proven $\forall e \in \mathbb{N}, e|a \wedge e|b \Longrightarrow e|m$ in 2(e)

Since $e, m \in \mathbb{N}$ and $e|m$ so $e \leq m$

Hence $\forall e \in \mathbb{N}, e|a \wedge e|b \Longrightarrow e \leq m$

We have proven $m|a \wedge m|b \wedge (\forall e \in \mathbb{N}, e|a \wedge e|b \Longrightarrow e \leq m)$ as needed, so m is the greatest common divisor of a and b. ■

(g)WTS: $\forall c \in \mathbb{Z}, (m = 1 \wedge a|bc) \Longrightarrow (a|c)$,where a,b is introduced in the question and m is introduced in 2(a).

Let $c \in \mathbb{Z}$, we assume $m = 1 \wedge a|bc$

Since m=1 and $m \in l$, so $\exists x, y \in \mathbb{Z}, ax + by = m = 1$, let x,y be that value.

Since a|bc, so $\exists k_1 \in \mathbb{Z}, bc = k_1 a$, let k_1 be that value.

We want to prove $a|c$, that is $\exists k \in \mathbb{Z}, c = ka$

Take k=$\frac{k_1}{b}$, since $\frac{k_1}{b} = k_1 \times \frac{1}{b} = k_1 \times \frac{ax+by}{b} = \frac{k_1 ax + k_1 by}{b} = \frac{bcx + k_1 by}{b} = cx + k_1 y$

Since c,x,y, $k_1 \in \mathbb{Z}$, so $cx + k_1 y \in \mathbb{Z}$, hence k$\in \mathbb{Z}$

ka=$\frac{k_1}{b} a = \frac{k_1 a}{b} = \frac{bc}{b} = c$

Hence we have proven $a|c$ as needed■

3.WTS: $\forall n \in \mathbb{N}, \exists p \in P, p > n$

I will prove this by contradiction.

Assume that this statement is false, i.e., that there are finite numbers of P. Let k$\in \mathbb{N}$ be the number of elements of P, and let $p_1, p_2, p_3 \ldots . p_k$ be the elements.($p_1 < p_2 < p_3 \ldots . < p_k$), so $p_1 = 3$

Our statement Q will be "for all n$\in \mathbb{N}$, n is prime and $n \equiv 3 \pmod 4$ if and only if n is one of { $p_1, p_2, p_3 \dots. p_k$}

Define the number p=4($\prod_{i=2}^{k} p_i$)+3 ,hence $p \equiv 3 \pmod 4$ (since $p_2 \times p_3 \dots. \times p_k$ is an integer). Also $p \notin P$ since p is even bigger than p_k . Therefore p must not be a prime. So p is a composite number since p is not a prime and p is bigger than 1.

- I am going to prove:$\forall n \in \mathbb{N}, 4|n \Longrightarrow n \nmid p$ by contradiction
  Let $n \in \mathbb{N}$, we assume $4|n$ that is $\exists k \in \mathbb{Z}, 4k = n$, let k be that value.
  If n|p that is $\exists a \in \mathbb{Z}, na = p$, let a be that value, so p=na=4ak
  So 4($p_2 \times p_3 \dots. \times p_k$)+3=4ak
  Hence 4($p_2 \times p_3 \dots. \times p_k - ak$)=-3
  Hence $p_2 \times p_3 \dots. \times p_k - ak$ $=-\frac{3}{4}$ and that is impossible since $p_2 \times p_3 \dots. \times p_k - ak$ must be an integer, so we get a contradiction.
  Hence we have proven $\forall n \in \mathbb{N}, 4|n \Longrightarrow n \nmid p$ as needed.

- I am going to prove:$\forall n \in \mathbb{N}, n \equiv 2 \pmod 4 \Longrightarrow n \nmid p$ by contradiction
  Let $n \in \mathbb{N}$, we assume $n \equiv 2 \pmod 4$ that is $\exists k \in \mathbb{Z}, 4k + 2 = n$, let k be that value.
  If n|p that is $\exists a \in \mathbb{Z}, na = p$, let a be that value, so p=na=4ka+2a
  So 4($p_2 \times p_3 \dots. \times p_k$)+3=4ak+2a
  Hence 2($2 \times p_2 \times p_3 \dots. \times p_k - 2ak - a$)=-3
  Hence $2 \times p_2 \times p_3 \dots. \times p_k - 2ak - a$ $=-\frac{3}{2}$ and that is impossible
  since $2 \times p_2 \times p_3 \dots. \times p_k - 2ak - a$ must be an integer, so we get a contradiction.
  Hence we have proven $\forall n \in \mathbb{N}, n \equiv 2 \pmod 4 \Longrightarrow n \nmid p$ as needed.

- I am going to prove:$\forall n \in \mathbb{N}, \mathrm{prime}(n) \wedge n \equiv 3 \pmod 4 \Longrightarrow n \nmid p$

That is to prove p is divisable by one of $p_1, p_2, p_3 \dots. p_k$ since for all n$\in \mathbb{N}$, n is prime and $n \equiv 3 \pmod 4$ if and only if n is one of { $p_1, p_2, p_3 \dots. p_k$}.
  For $p_1 = 3$: this is impossible for otherwise 4($p_2 \times p_3 \dots. \times p_k$) is divisible by 3 while $3 \nmid 4$ and $p_2, p_3 \dots. p_k$ are primes that is not equal to 3.
  For $p_2, p_3 \dots. p_k$, this is also impossible for otherwise one of $p_2, p_3 \dots. p_k$ would divide P-4($p_2 \times p_3 \dots. \times p_k$)= 3, while all of $p_2, p_3 \dots. p_k$ is bigger than 3.
  Hence we have proven $\forall n \in \mathbb{N}, \mathrm{prime}(n) \wedge n \equiv 3 \pmod 4 \Longrightarrow n \nmid p$ as needed.

Since $\forall n \in \mathbb{N}, n \equiv 2 \pmod 4 \Longrightarrow n \nmid p$ so $\forall n \in \mathbb{N}, \mathrm{prime}(n) \wedge n \equiv 2 \pmod 4 \Longrightarrow n \nmid p$
And $\forall n \in \mathbb{N}, 4|n \Longrightarrow n \nmid p$
And $\forall n \in \mathbb{N}, \mathrm{prime}(n) \wedge n \equiv 3 \pmod 4 \Longrightarrow n \nmid p$
And p is not a prime
And the fact that any integer greater than 1 is a product of prime
So p must be a product of prime $n_1, n_2 \dots n_t$ while $n_1 \equiv 1 \pmod 4 \wedge n_2 \equiv 1 \pmod 4 \wedge \dots. \wedge$ $n_t \equiv 1 \pmod 4$ (t$\in \mathbb{N}^+$)
According to the [modular multiplication] that says that the product of 2 or more numbers (mod m) is congruent to the product of numbers congruent to them so $p \equiv 1 \pmod 4$

But p=4($p_2 \times\ p_3 \ldots. \times p_k$)+3 ,hence $\mathrm{p} \equiv 3(\mathrm{mod}\ 4)$, so we get a contradiction

So what we assumed at first is false

Hence we have proven $\forall \mathrm{n} \in \mathrm{R}, |\mathrm{P}| > \mathrm{n}$ as needed■

4.(a)WTS: $\exists n_0 \in \mathbb{R}^{\geq 0}, \forall n \in \mathbb{N}, n \geq n_0 \Longrightarrow g(n) \leq f(n)$

Take $n_0 = 1000$, since $1000 \in \mathbb{R}^{\geq 0}$ so $n_0 \in \mathbb{R}^{\geq 0}$

Let $n \in \mathbb{N}$, we assume $n \geq n_0 = 1000$, we want to show $g(n) \leq f(n)$, that is

2n+1650 $\leq 0.5n^2$

2n+1650<250n+250000 $(n \in \mathbb{N})$

$\leq 0.25n^2$+$0.25n^2$ $(n \geq n_0 = 1000\ and\ n \in \mathbb{N})$

$= 0.5n^2$

Hence we have shown $g(n) \leq f(n)$ as needed■

(b) WTS: $\forall \mathrm{a}, \mathrm{b} \in \mathbb{R}^{\geq 0}, \exists n_0 \in \mathbb{R}^{\geq 0}, \forall n \in \mathbb{N}, n \geq n_0 \Longrightarrow g(n) \leq f(n)$

Let $\mathrm{a}, \mathrm{b} \in \mathbb{R}^{\geq 0}$

Take n_0=max$\{4\mathrm{a}, 2\sqrt{b}\}$, since $\mathrm{a}, \mathrm{b} \in \mathbb{R}^{\geq 0}$, so $4\mathrm{a}, 2\sqrt{b} \in \mathbb{R}^{\geq 0}$, so $n_0 \in \mathbb{R}^{\geq 0}$

Let $n \in \mathbb{N}$, we assume $n \geq n_0$, we want to prove $g(n) \leq f(n)$ that is an+b $\leq 0.5n^2$

Since n_0=max$\{4\mathrm{a}, 2\sqrt{b}\}$ and $n \geq n_0$ this implies:

- n $\geq$ 4a, so $n^2 \geq 4\mathrm{a} \times \mathrm{n}$ since $n \geq n_0 \geq 0$
  hence 0.25$n^2 \geq \mathrm{an}$
- n$\geq 2\sqrt{b}$, so $n^2 \geq 4b$ since $n \in \mathbb{N}\ and\ 2\sqrt{b} \geq 0$

  hence 0.25$n^2 \geq b$

In all 0.25$n^2 + 0.25n^2$ $\geq$an+b ,that is an+b $\leq 0.5n^2$

Hence we have shown $g(n) \leq f(n)$ as needed■