CSC165H1 Problem Set 2 (due 10/25/17)

Jacob Nazarenko, James Currier, Mark Abdullah

October 25, 2017

1. (a) We want to show that

$$\forall n \in \mathbb{N}^+,\ Composite(n^2 + 3n + 2)$$

Proof. Let n be an arbitrary positive natural number. Then we know that

$$n \geq 1$$
$$n + 1 \geq 2 > 1$$
$$n + 2 \geq 3 > 1$$

Therefore,

$$(n + 1)(n + 2) = (n^2 + 3n + 2) \geq 6 > 1$$

Let us now define $\neg Prime(p)$:

$$\neg Prime(p) : p \leq 1 \vee (\exists d \in \mathbb{N},\ d \mid p \wedge d \neq 1 \wedge d \neq p)$$

We know that

$$(n^2 + 3n + 2) = (n + 2)(n + 1)$$

Therefore,

$$(n + 1) \mid (n^2 + 3n + 2)$$
$$(n + 2) \mid (n^2 + 3n + 2)$$

We also know the following:

$$(n + 1) \neq (n^2 + 3n + 2)$$
$$(n + 2) \neq (n^2 + 3n + 2)$$
$$(n + 1) \neq 1$$
$$(n + 2) \neq 1$$

Therefore, $(n^2 + 3n + 2)$ is not prime.

Because $n \geq 1$, we know that

$$(n^2 + 3n + 2) \geq 6 > 1$$

We have therefore proven the statement true. ■

(b) We want to show that
$$\forall n \in \mathbb{N}^+,\ Composite(n^2 + 6n + 5)$$

Proof. Let n be an arbitrary positive natural number. Then we know that

$$n \geq 1$$
$$n + 5 \geq 6 > 1$$
$$n + 1 \geq 2 > 1$$

Therefore,
$$(n + 1)(n + 5) = (n^2 + 6n + 5) \geq 12 > 1$$

Now consider our previous definition of $\neg Prime(p)$.

We know that
$$(n^2 + 6n + 5) = (n + 1)(n + 5)$$
so we also know that

$$(n + 5) \mid (n^2 + 6n + 5)$$
$$(n + 1) \mid (n^2 + 6n + 5)$$

where the following is also true:

$$(n + 5) \neq (n^2 + 6n + 5)$$
$$(n + 1) \neq (n^2 + 6n + 5)$$
$$(n + 5) \neq 1$$
$$(n + 1) \neq 1$$

Therefore, by our previous definition of $\neg Prime(p)$, we have that $(n^2 + 6n + 5)$ is not prime.

We also have that
$$(n^2 + 6n + 5) \geq 11 > 1$$

Therefore, we have proven the statement true. ∎

2. For all the following proofs in 2:
Let $a, b \in \mathbb{N}$. Assume they are not both zero.

(a) We want to show that
$$\exists m \in \mathcal{L}, \forall n \in \mathcal{L}, m \leq n$$

Proof. The set L is an infinite set defined as:

$$\mathcal{L} = \{n \in \mathbb{N}^+ : \exists x, y \in \mathbb{Z}, n = ax + by\}$$

Define $\mathcal{L}'$ as:
$$\mathcal{L}' = \{n \in \mathcal{L} : n \leq a + b\},$$

the finite set of linear combinations of a and b that are less than or equal to $a + b$. We know $\mathcal{L}'$ is finite because it only contains positive integers bounded to at most $a + b$. We also know $\mathcal{L}'$ is non-empty because it contains at least a or b. Using the fact that any non-empty, finite set of real numbers has a minimum element, we can conclude $\mathcal{L}'$ has a minimum element. Since every element in $\mathcal{L}$ is greater than or equal to any element $\mathcal{L}'$, this minimum holds for $\mathcal{L}$ as well. ■

(b) We want to show that

$$\forall k \in \mathbb{N}^+, \exists x, y \in \mathbb{Z}, mk = ax + by$$

Proof. Let m be the minimum element in $\mathcal{L}$. Assume $m \in \mathcal{L}$ such that $\exists x, y \in \mathbb{Z}, m = ax_1 + by_1$. Let x_1 and y_1 be such values.
Let $k \in \mathbb{N}^+$, let $x = x_1 k$, and let $y = y_1 k$. From our assumption, we know m is a linear combination of a and b:

$$\begin{aligned} m &= ax_1 + by_1 \\ mk &= ax_1 k + by_1 k \\ mk &= ax + by \end{aligned}$$

We've proven that mk is also a linear combination of a and b, and that it is therefore in the set $\mathcal{L}$. ■

(c) In order to prove this statement, we must first prove that we may assume the following for the set $\mathcal{L}$ with minimum element m:

$$\forall c \in \mathcal{L},\ c \geq 0 \wedge c \geq m$$

To prove this, let c be an element of $\mathcal{L}$. We know that by the definition of the set $\mathcal{L}$, c must be non-negative, as all of the elements of $\mathcal{L}$ must be positive natural numbers. Therefore, the lowest value that any element of $\mathcal{L}$ can have is 1. If $c \geq 1$, then c must be non-negative. Also, we know that m is defined as an element that is no larger than any other element of $\mathcal{L}$. Therefore, we know that $m \leq c$ for any element c of $\mathcal{L}$, and we have proven this assumption true. We may now proceed to prove the following statement by contradiction:

$$\forall c \in \mathcal{L},\ \exists k \in \mathbb{Z},\ km = c$$

Proof. (by contradiction) Assume that there is at least one element of the set $\mathcal{L}$ that is not a multiple of m (this is the negation of the above statement):

$$\exists c \in \mathcal{L},\ \forall k \in \mathbb{Z},\ km \neq c$$

Let there be such a value c in $\mathcal{L}$ that makes the expression above true. In this case, we know by the Quotient-Remainder Theorem that

$$\exists q, r \in \mathbb{Z},\ qm + r = c$$

For the purposes of this proof, let $q = k$ from above. If we follow our assumption that c is not a multiple of m, then we know that $0 < r < m$. However, r cannot be between 1 and m because if it were, the number $km + r$ could not be expressed solely as a linear combination of a and b. This is because r would have to be less than m, and would therefore have to be less than both a and b. We have therefore reached a contradiction. r cannot be equal to m, or the whole number would be divisible by m, so it must actually be equal to 0. We have thereby proven the original statement to be true. ■

(d) We want to show that

$$m \mid a \wedge m \mid b$$

Proof. Let $m = ax + by$ be the minimum element in $\mathcal{L}$. Using the Quotient Remainder Therom, we can express a as follows,

$$\exists k, r \in \mathbb{Z}, a = mk + r,\ \text{where } 0 \leq r < m$$

$$
\begin{aligned}
r &= a - mk \\
r &= a - (ax + by)k \\
r &= a - kax - kby \\
r &= a(1 - kx) + b(-ky)
\end{aligned}
$$

Therefore r is a non-negative linear combination, as $0 \leq r$, but since m is the smallest positive linear combination and $r < m$, hence $r = 0$. Therefore $m \mid a$.

Similarily, using the Quotient Remainder Therom, we can express b as follows,

$$\exists k_1, r_1 \in \mathbb{Z}, b = mk_1 + r_1, \text{ where } 0 \leq r_1 < m$$

$$
\begin{aligned}
r_1 &= b - mk_1 \\
r_1 &= b - (ax + by)k_1 \\
r_1 &= b - k_1 by - k_1 ax \\
r_1 &= b(1 - k_1 y) + a(-k_1 x)
\end{aligned}
$$

Therefore r_1 is a non-negative linear combination, as $0 \leq r_1$, but since m is the smallest positive linear combination and $r_1 < m$, hence $r_1 = 0$. Therefore $m \mid b$. ■

(e) We want to show that

$$\forall n \in \mathbb{N}, n \mid a \wedge n \mid b \implies n \mid m$$

Proof. Let $m = ax + by$ be the minimum element in $\mathcal{L}$. Let $n \in \mathbb{N}$.
Assume $n \mid a$, such that $\exists k_1 \in \mathbb{Z}, a = k_1 n$
Assume $n \mid b$, such that $\exists k_2 \in \mathbb{Z}, a = k_2 n$
Since m in a linear combination,

$$m = ax + by$$

By our hypothesis,

$$
\begin{aligned}
m &= k_1 nx + k_2 ny \\
m &= (k_1 x + k_2 y)n
\end{aligned}
$$

Since n is a factor of m, $n \mid m$. ■

(f) We want to show that

$$m = gcd(a, b)$$

Proof. Let $m = ax + by$ be the minimum element in $\mathcal{L}$.
By the claim in 4e, we know that any natural number that divides a and b must also divide m. Therefore the $gcd(a, b)$ must also divide m.

$$gcd(a, b) \leq m$$

By the claim in 4d, we know m is a common divisor of a and b, and so the greatest common divisor of a and b cannot be less than any other common divisor, in this case m.

$$gcd(a, b) \not< m$$

Thus $gcd(a, b) = m$ ■

(g) We want to show that

$$\forall c \in \mathbb{Z}, gcd(a, b) = 1 \wedge a \mid bc \implies a \mid c$$

Proof. Let $m = ax + by$ be the minimum element in $\mathcal{L}$.
Assume $gcd(a, b) = 1$
Assume $a \mid bc$, such that $\exists k_1 \in \mathbb{Z}, bc = ak_1$
Want to show $a \mid c$, such that $\exists k_2 \in \mathbb{Z}, c = ak_2$. Let $k_2 = cx + k_1 y$
From the claim in 4f, we know $gcd(a, b) = m$, and equivalently $1 = ax + by$

$$\begin{aligned} 1 &= ax + by \\ c &= c(ax + by) \\ c &= cax + cby \end{aligned}$$

From our hypothesis, we know $bc = ak_1$

$$\begin{aligned} c &= cax + ak_1 y \\ c &= a(cx + k_1 y) \\ c &= ak_2 \end{aligned}$$

We've proven $a \mid c$. ■

3. (a) We want to show that

$$\text{The set } P = \{p \mid Prime(p) \wedge p \equiv 3 \ (mod\ 4)\} \text{ is infinite}$$

Proof. (by contradiction) Assume that the set is finite. This means that there is a finite number of primes $\{p_1, p_2, \ ... \ , p_k\}$ that are also congruent to 3 (mod 4).

By the definition of congruence, we know that for any $p_i \in P$,

$$4 \mid p_i - 3$$

This means that if we divide p_i by 4, we will get a remainder of 3, and consequently means that

$$4 \mid p_i + 1$$

By the definition of divisibility, this means that

$$\exists k_1 \in \mathbb{Z}, \ 4k_1 = p_i + 1$$

Let a natural number N be defined as the following:

$$N = 4(p_1 \times p_2 \times \ ... \ \times p_k) - 1$$

By our previous statement, we can see that because $N + 1 = 4(p_1 \times p_2 \times \ ... \ \times p_k)$, we have that

$$4 \mid N + 1 \quad \text{and} \quad 4 \mid N - 3$$

Therefore, by our previous statements,

$$N \equiv 3 \ (mod\ 4)$$

We know that there must be a prime number that divides N, but this number cannot be in the set $\{p_1, p_2, \ ... \ , p_k\}$, because if it were, it would divide $N - 4(p_1 \times p_2 \times \ ... \ \times p_k)$, a linear combination of N and itself which is equal to -1, and there is no prime number that can divide -1. Hence, we can conclude that N itself is a prime number.

Therefore, we have reached a contradiction, because we have shown that N is congruent to 3 (mod 4), that N is a prime number itself, and that it is not one of the prime numbers in the set P. Therefore, we can conclude that the set P is infinite, and that there are infinitely many prime numbers congruent to 3 (mod 4). We have proven the original statement. ■

4. (a) We want to show that

$$\exists n_0 \in \mathbb{R}^{\geq 0},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow 0.5n^2 \geq 2n + 1650$$

Proof.
Take $n_0 = 60$

Let $n \in \mathbb{N}$

Assume $n \geq n_0$

$$\begin{aligned} n &\geq 60 \\ n^2 &\geq 60n \\ \frac{1}{2}n^2 &\geq 30n \\ \frac{1}{2}n^2 &\geq 2n + 28n \end{aligned}$$

Since $n \geq 60$, $28n \geq 28(60) = 1680$

So,

$$\frac{1}{2}n^2 \geq 2n + 1680$$

Since $1680 \geq 1650$,

$$\frac{1}{2}n^2 \geq 2n + 1650$$

■

(b) We want to show that

$$\forall a, b \in \mathbb{R}^{\geq 0},\ \exists n_0 \in \mathbb{N},\ \forall n \in \mathbb{R}^{\geq 0},\ n \geq n_0 \Rightarrow 0.5n^2 \geq an + b$$

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

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

Let $n \in \mathbb{N}$

Assume $n \geq n_0$

$$\begin{aligned}
n &\geq a + \sqrt{a^2 + 2b} \\
n - a &\geq \sqrt{a^2 + 2b} \\
(n - a)^2 &\geq a^2 + 2b \\
n^2 - 2an + a^2 &\geq a^2 + 2b \\
n^2 - 2an &\geq 2b \\
n^2 &\geq 2an + 2b \\
0.5n^2 &\geq an + b
\end{aligned}$$

■