CSC165H1: Problem Set 2 Sample Solutions

Due October 25 2017 before 10pm

Note: solutions are incomplete, and meant to be used as guidelines only. We encourage you to ask follow-up questions on the course forum or during office hours.

1. **[6 marks] divisibility...**

Composite(n): "n is greater than 1 and not prime." for $n \in \mathbb{N}$. Prove the statements below.

(a) **[3 marks]**

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

Solution

The statement to be proved is given in the question:

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

Proof: Let $n \in \mathbb{N}$. To be composite n^2+3n+2 must be greater than 1 and non-prime. n^2+3n+2 may be factored as:

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

Since $n \in \mathbb{N}^+$, $n+2 \geq 3 > 1$ and $n+1 \geq 2 > 1$. Thus $n^2 + 3n + 2$ has a factor, $n + 2$, which is greater than 1 and less than $n^2 + 3n + 2$ itself, so it is non-prime. Also $n^2 + 3n + 2$ is greater than 1, hence composite. ■

- 0.5 marks for re-capitulating predicate
- 1 mark for introducing n
- 1.5 marks for showing that $n^2 + 3n + 2$ is composite

(b) **[3 marks]**

$$\forall n \in \mathbb{N}^+, \text{Composite}(n^2 + 6n + 5)$$

Solution

The statement to be proved is given in the question:

$$\forall n \in \mathbb{N}^+, \text{Composite}(n^2 + 6n + 5)$$

Proof: Let $n \in \mathbb{N}$. To be composite n^2+6n+5 must be greater than 1 and non-prime. n^2+6n+5 may be factored as:

$$n^2 + 6n + 5 = (n + 1)(n + 5)$$

Since $n \in \mathbb{N}^+$, $n+5 \geq 6 > 1$ and $n+1 \geq 2 > 1$. Thus $n^2 + 6n + 5$ has a factor, $n + 5$, which is greater than 1 and less than $n^2 + 6n + 5$ itself, so it is non-prime. Also $n^2 + 6n + 5$ is greater than 1, hence composite. ■

- 0.5 marks for re-capitulating predicate
- 1 mark for introducing n

- 1.5 marks for showing that $n^2 + 6n + 5$ is composite

2. **[21 marks] more gcd!**

Let $a, b \in \mathbb{N}$, assume they are not both 0. Define $\mathcal{L} = \{n \in \mathbb{N}^+ : \exists x, y \in \mathbb{Z}, n = ax + by\}$. Prove the claims below, being sure to first state the claim you are proving in predicate logic, and then to write the complete proof. You may use the result of earlier claims in proving later ones, for example you might use claim (f) to help prove claim (g). **Anti-hint**: You may **not** use Claims (1)–(6) from Tutorial 4, since you are proving some of them!

(a) **[3 marks] Claim**: $\mathcal{L}$ has a minimum element m, i.e. m is no larger than any other element of $\mathcal{L}$. You may use, without proof, the fact that any non-empty, finite set of real numbers has a minimum element[1]

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement in order to pare down the statement to be proved.

$$\exists m \in \mathcal{L}, \forall n \in \mathcal{L}, m \leq n$$

Proof: Let a, b and $\mathcal{L}$ be as in the question statement. Then $a + b > 0$, since it is the sum of two natural numbers that are not both 0. Let $x_0 = y_0 = 1$, and $a + b = x_0 a + y_0 b \in \mathcal{L}$. Thus $\mathcal{L}' = \{n : n \in \mathcal{L} \wedge n \leq z + b\}$ is non-empty and has, at most, $a + b$ elements. Let m be a minimal element of this finite, non-empty set of real numbers. Since m is a minimum of all elements of $\mathcal{L}$ that are no larger than $a + b$, it is also no larger than any element of $\mathcal{L}$ that is larger than $a + b$. Hence m is a minimum for $\mathcal{L}$. ■

- 0.5 marks for statement, allowing them to reference $a, b, \mathcal{L}$, and m, already introduced
- 1 mark for introducing variables
- 1.5 mark for showing $\mathcal{L}$ must have a minimal element

(b) **[3 marks] Claim**: Any multiple km, where $k \in \mathbb{N}^+$, is an element of $\mathcal{L}$.

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement, and m, the minimal element of $\mathcal{L}$ introduced in the previous question.

$$\forall k \in \mathbb{N}^+, km \in \mathcal{L}$$

Proof: Let $a, b, \mathcal{L}$ be as in the question statement, and m be the minimal element of $\mathcal{L}$ introduced in the first part of this question. Let $k \in \mathbb{N}^+$.. Then $\exists x_0, y_0 \in \mathbb{Z}, m = x_0 a + y_0 b$, so let x_0, y_0 be such values. Let $x_1 = kx_0, y_1 = ky_0$, and $km = x_1 a + x_1 b$ is an element of $\mathcal{L}$. ■

- 0.5 marks for statement
- 1 mark for introducing variables
- 1.5 marks for showing that a multiple of m is a positive linear combination of a and b.

(c) **[3 marks] Claim**: Any element $c \in \mathcal{L}$ is a multiple of m. **Hint**: Show that you may assume that c is non-negative, no smaller than m, and then use the Quotient-Remainder Theorem to derive a contradiction.

[1] Notice that this is **not** necessarily true of infinite sets, for example $\mathbb{Z}$ or $(0, 1)$, nor is it true of the empty set.

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement, and m, the minimal element of $\mathcal{L}$ introduced in the previous question:

$$\forall c \in \mathcal{L}, \exists k \in\in \mathbb{N}, c = qm$$

Proof (by contradiction): Assume the statement is false, that is:

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

Let $a, b, \mathcal{L}$ be as in the question statement, and m be the minimal element of $\mathcal{L}$ introduced in the first part of this question. Let $c \in \mathcal{L}$, so $\exists x_1, x_0, y_1, y_0$ such that $c = x_1 a + y_1 b$ and $m = x_0 a + y_0 b$. Let x_1, y_1, x_0, y_0 be such values. Then, by the Quotient-Remainder Theorem $\exists q, r \in \mathbb{Z}, c = qm + r$ and $m > r \wedge r \geq 1$, since $r = 0$ is excluded by the assumption that $qm \neq c$. Let q, r be such values. Thus $r = (x_1 - qx_0)a + (y_1 - qy_0)b$. So $r \in \mathcal{L}$ but $r < m \longrightarrow\longleftarrow$ contradiction: m is a minimal element of $\mathcal{L}$. ■

(d) **[3 marks] Claim:** m divides a and m divides b.

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement, and m, the minimal element of $\mathcal{L}$ introduced in the previous question:

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

Proof: Let $a, b, \mathcal{L}$ be as in the question statement, and m be the minimal element of $\mathcal{L}$ introduced in the first part of this question. If $a = 0$, then $a = 0 \cdot m$ and $m \mid a$. Otherwise $1 \cdot a + 0 \cdot b \in \mathcal{L}$, and $m \mid a$ by the previous question. Similarly, $m \mid b$. ■

(e) **[3 marks] Claim:** Any natural number n that divides both a and b also divides m.

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement, and m, the minimal element of $\mathcal{L}$ introduced in the previous question:

$$\forall n \in \mathbb{N}^+, (n \mid a \wedge n \mid b) \Rightarrow n \mid m$$

Proof: Let $a, b, \mathcal{L}$ be as in the question statement, and m be the minimal element of $\mathcal{L}$ introduced in the first part of this question. Let $n \in \mathbb{N}^+$, and assume $n \mid a \wedge n \mid b$. Then exists $k_1, k_2 \in \mathbb{Z}, a = k_1 n \wedge b = k_2 b$. Let k_1, k_2 be such values. Since $m \in \mathcal{L}$, $\exists x_0, y_0 \in \mathbb{Z}, m = ax_0 + by_0$, so let x_0, y_0 be such values. Then $m = k_1 x_0 n + k_2 y_0 n = (k_1 x_0 + k_2 y_0)n$, and $n \mid m$. ■

(f) **[3 marks] Claim:** m is the greatest common divisor of a and b.

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement, and m, the minimal element of $\mathcal{L}$ introduced in the previous question:

$$(m \mid a \wedge m \mid b) \wedge [\forall n \in \mathbb{N}, (n \mid a \wedge n \mid b) \Rightarrow n \leq m]$$

Proof: Let $a, b, \mathcal{L}$ be as in the question statement, and m be the minimal element of $\mathcal{L}$ introduced in the first part of this question. Let $n \in \mathbb{N}$ and assume $n \mid a \wedge n \mid b$.

We have shown above that $m \mid a \wedge m \mid b$ and that $n \mid m$. Let $k \in \mathbb{Z}, m = kn$, and notice that since $m \in \mathbb{N}^+$ that $n \neq 0$, so $n \in \mathbb{N}^+$. Also, since $m, n \in \mathbb{N}+$ we must have $k \in \mathbb{N}^+$, $k \geq 1$, so,

$$m = kn \geq 1 \cdot n = n$$

So $m = \gcd(a, b)$. ■

(g) **[3 marks] Claim:** If a and b are **coprime**, i.e. $m = \gcd a, b = 1$, and $c \in \mathbb{Z}$, and $a \mid bc$, then a divides c. **Hint:** $a \mid c$ is equivalent to $c \equiv 0 \pmod{a}$, and 2(f) should be helpful here.

Solution

I reference a, b and $\mathcal{L}$ as introduced in the question statement, and m, the minimal element of $\mathcal{L}$ introduced in the previous question:

$$(m = \gcd(a, b) = 1 \wedge a \mid bc) \Rightarrow a \mid c$$

Proof: Let $a, b, \mathcal{L}$ be as in the question statement, and m be the minimal element of $\mathcal{L}$ introduced in the first part of this question. Assume $m = 1$. Let $c \in \mathbb{Z}$ and assume $a \mid bc$.

From the first part of this question we know $\exists x_0, y_0 \in \mathbb{Z}, m = ax_0 + by_0 = 1$, so let x_0, y_0 be such values. Also, by assumption, $existsk \in \mathbb{Z}, bc = ak$, so let k be such a value. Then,

$$\begin{aligned} ax_0 + by_0 &= 1 \\ cax_0 + cby_0 &= c \quad \text{(multiply by } c\text{)} \\ cax_0 + akby_0 &= c \quad \text{(since } bc = ak\text{)} \\ a(cx_0 + kby_0) &= c \end{aligned}$$

So $a \mid c$. ■

3. **[3 marks] a prime example...**

Theorem 2.3 established that there are infinitely many prime numbers. It seems pretty clear all but one prime number are odd. You can go further:

(a) **[3 marks]** Prove that that the set $P = \{p \mid Prime(p) \wedge p \equiv 3 \pmod{4}\}$ is infinite.

Hint: Think about the **technique** of Theorem 2.3, and also that there are other arithmetic manipulations other than adding one, such as multiplying by 4 or even subtracting 1.

Solution

One way to express that a subset of $\mathbb{N}$ is infinite is to show that there is always an element greater than any given natural number

$$\forall n \in \mathbb{N}, \exists p \in \mathbb{N}, Prime(p) \wedge p \equiv 3 \pmod{4} \wedge p > n$$

Proof: Let $n \in \mathbb{N}$. Let $P_n = \{p : p \leq n \wedge Prime(p) \wedge p \equiv 3 \pmod{4}\}$. There are two cases to consider:

Case $n < 3$: Then let $p' = 3$. Then $p' > n$, $Prime(p')$, and $p' \equiv 3 \pmod{4}$.

Case $n \geq 3$: Then P_n is non-empty and we can form the product of its elements, $k = p_1 \times \cdots \times p_k$. Then $r = 4k - 1 \equiv 3 \pmod{4}$. Since $3 \mid k$ we must have $r \geq 4 \times 3 - 1 = 11$, and thus r

has 1 or more prime factors. None of these prime factors are in P_n, since any prime in P_n is a factor of k and hence a factor of $4k$. Any factor of both r and $4k$ must divide their difference, 1, and no prime does that.

By construction r is odd, so all its prime factors must be odd numbers, hence congruent to either 1 or 3 $\pmod 4$. At least one of them must be congruent to 3 $\pmod 4$, since otherwise their product, r would be congruent to 1 $\pmod 4$. ■

4. **[7 marks] Function growth.** Now let's leave numbers and talk about functions. Consider the following definition:[2]

Definition 1. Let $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$. We say that g **is eventually dominated by** f if and only if there exists $n_0 \in \mathbb{R}^{\geq 0}$ such that every natural number n greater than or equal to n_0 satisfies $g(n) \leq f(n)$.

We can express this definition in a predicate $Edom(f, g)$: "g is eventually dominated by f", where $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$, in the following way:

$$EDom(f, g) : \exists n_0 \in \mathbb{R}^{\geq 0},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow g(n) \leq f(n)$$

(a) **[3 marks]** Let $f(n) = 0.5n^2$ and $g(n) = 2n + 1650$. Prove that g is eventually dominated by f. Do **NOT** use part (b) to prove this part; we want to see you construct a proof with concrete numbers rather than the variables you'll use in part (b).

Hint: pay attention to the order of the quantifiers. The first line of your proof should introduce the variable n_0, and give it a concrete value.

Solution

We want to prove that

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

Proof: Let $n_0 = 60$, and let $n \in \mathbb{N}$, and assume $n \geq n_0$. We want to prove that $0.5n^2 \geq 2n + 1650$. Start with our assumption:

$$\begin{aligned} n &\geq n_0 = 60 \\ 0.5n^2 = (0.5n \times n) &\geq 30n \\ &= 2n + 28n \\ &\geq 2n + 28n \\ &\geq 2n + 28(60) = 2n + 1680 \\ &\geq 2n + 1650 \quad ■ \end{aligned}$$

- 0.5 marks for statement
- 1 mark for introducing variables
- 1.5 marks for proving the inequality

(b) **[4 marks]** Prove the following statement, which is a generalization of the previous part:

$$\forall a, b \in \mathbb{R}^{\geq 0},\ g(n) = an + b \text{ is eventually dominated by } f(n) = 0.5n^2.$$

Hint: you don't need to pick the "best" n_0 here, just pick one that works and makes the proof's calculations easy for you to work with! Which variables can n_0 depend on?

[2] The symbol $\mathbb{R}^{\geq 0}$ denotes the set of all nonnegative real numbers, i.e., $\mathbb{R}^{\geq 0} = \{x \mid x \in \mathbb{R} \wedge x \geq 0\}$.

Solution

Translated statement, expanded:

$$\forall a, b \in \mathbb{R}^{\geq 0},\ \exists n_0 \in \mathbb{R}^{\geq 0},\ \forall n \in \mathbb{N},\ n \geq n_0 \Rightarrow an + b \leq \frac{1}{2}n^2$$

Proof: Let $a, b \in \mathbb{R}^{\geq 0}$. Let $n_0 = \max(2a + 2b, 1)$, and let $n \in \mathbb{N}$. Assume that $n \geq n_0$. We want to prove that $an + b \leq n^2$. Notice that since $n \geq n_0 \geq 1$, we know $bn \geq b$.

By our assumption:

$$\begin{array}{rcl} n & \geq & 2(a+b) \\ 0.5n & \geq & (a+b) \\ 0.5n^2 & \geq & (a+b)n = an + bn \\ & \geq & an + b \quad \blacksquare \end{array}$$

- 0.5 marks for statement
- 1 mark for introducing variables
- 1.5 marks for proving the inequality