CSC165H1: Problem Set 2

Due October 25 2017 before 10pm

General instructions

Please read the following instructions carefully before starting the problem set. They contain important information about general problem set expectations, problem set submission instructions, and reminders of course policies.

- Your problem sets are graded on both correctness and clarity of communication. Solutions which are technically correct but poorly written will not receive full marks. Please read over your solutions carefully before submitting them. Proofs should have headers and bodies in the form described in the course note.
- Each problem set may be completed in groups of up to three. If you are working in a group for this problem set, please consult `https://github.com/MarkUsProject/Markus/wiki/Student_Groups` for a brief explanation of how to create a group on MarkUs.

  Exception: Problem Sets 0 and 1 must be completed individually.
- Solutions must be typeset electronically, and submitted as a PDF with the correct filename. **Handwritten submissions will receive a grade of ZERO.**

  The required filename for this problem set is **problem_set2.pdf**.
- Problem sets must be submitted online through MarkUs. If you haven't used MarkUs before, give yourself plenty of time to figure it out, and ask for help if you need it! If you are working with a partner, you must form a group on MarkUs, and make one submission per group. "I didn't know how to use MarkUs" is not a valid excuse for submitting late work.
- Your submitted file should not be larger than 9MB. This may happen if you are using a word processing software like Microsoft Word; if it does, you should look into PDF compression tools to make your PDF smaller, although please make sure that your PDF is still legible before submitting!
- The work you submit for credit must be your own; you may not refer to or copy from the work of other groups, or external sources like websites or textbooks. You may, however, refer to any text from the Course Notes (or posted lecture notes), except when explicitly asked not to.

Additional instructions

- For each proof you write, make sure to first write in predicate logic the precise statement, fully simplified, that you're going to prove. For a disproof, clearly write the fully simplified negation. You do **not** need to show your work for computing negations of statements. Your proof should include a **header**, where names and assumptions are introduced, and a **body**, where statements leading to the conclusion are derived.
- For proofs involving divisibility, primes, and the floor function, you **may not use any external facts other than those mentioned in the questions**. You should not (and will not need to) prove any external facts to complete this problem set.

- For any *concrete numbers*, you may state whether one divides another, or whether a number is prime, without proof. For example, you can write statements "$3 \mid 12$" and "15 is not prime" without justification.

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]**

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

   (b) **[3 marks]**

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

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]

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

   (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.

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

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

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

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.

[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.

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) 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.

(b) 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., $\mathbb{R}^{\geq 0} = \{x \mid x \in \mathbb{R} \wedge x \geq 0\}$.