CSC165H1: Problem Set 2

Due Friday February 7 before 4pm

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 that are technically correct but poorly written will not receive full marks. Please read over your solutions carefully before submitting them.
- 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 Set 0 must be completed individually.
- Solutions must be typeset electronically, and submitted as a PDF with the correct filename. **Hand-written 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(s) should not be larger than 9MB. You might exceed this limit if you use a word processor like Microsoft Word to create a PDF; 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!
- Submissions must be made *before* the due date on MarkUs. You may use *grace tokens* to extend the deadline; please see the Homework page for details on using grace tokens.
- The work you submit must be that of your group; you may not use or copy from the work of other groups, or external sources like websites or textbooks.

Additional instructions

- You may not define your own propositional operators, predicates, or sets for this problem set. Work with the symbols we have introduced in lecture, and any definitions provided in the questions.
- In your proofs you can always use *definitions* we have covered in the course. You may **not** use any external facts about these definitions unless they are explicitly stated in the question.

  However, you *may* make statements about these definitions without proof when they concern only specific integers, e.g., "7 is odd" or "13 is prime".
- You are *not* required to submit translations of statements you're proving in predicate logic unless we explicitly ask for it. However, if you are doing a **disproof**, then you *must* submit a translation of the negation of the statement in predicate logic (following the same guidelines as Problem Set 1).

1. **[12 marks] Number theory.** Prove each of the following statements. For each one, you may use the statements from previous question parts (including part (a)) as "external facts" in your proofs. You may also use the following facts, as long as you clearly refer to them:

$$\forall a, b \in \mathbb{Z},\ 2 \nmid a \land 2 \nmid b \Rightarrow 2 \mid a - b \qquad \text{(Fact 1)}$$
$$\forall a, b, c \in \mathbb{Z},\ a \mid b \land b \mid c \Rightarrow a \mid c \qquad \text{(Fact 2)}$$
$$\forall p \in \mathbb{N},\ Prime(p) \Rightarrow \big(\forall k, d \in \mathbb{Z}^+,\ d \mid p^k \Rightarrow d = 1 \lor p \mid d\big) \qquad \text{(Fact 3)}$$
$$\forall n_0 \in \mathbb{N},\ \exists n \in \mathbb{N},\ n > n_0 \land Prime(n) \qquad \text{(Fact 4)}$$

(a) [**Do not hand in—this question part is not graded.**] Prove that for every pair of integers d and n, d does not divide any number between nd and $(n+1)d$, exclusive.

(b) Prove that for every prime p and positive integer k, $\gcd(p^k, n) = 1$ for every positive integer n between p^k and $p^k + p$, exclusive.

(c) Prove that for every positive integer m, there are infinitely many natural numbers n such that $\gcd(n, n+m) = 1$.

For this part, you *must* include a translation of the above statement into predicate logic, using the same structure for "infinitely many" that we saw in the Course Notes and on Problem Set 1.

Hint: Fact 4 ("infinitely many primes") allows you to choose a prime number that is as large as you want.

(d) Prove that every prime gap is equal to 1 or is divisible by 2. (Refer to Problem Set 1 for the definition of "prime gap".)

Updated Jan 30: you may use the domain $\mathbb{Z}^+$ instead of $\mathbb{N}$ for prime gaps in this question.

2. **[16 marks] The floor function.**

Recall the definition of the **floor** function $\lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}$, where $\lfloor x \rfloor$ returns the greatest integer that is less than or equal to x.

Prove or disprove each of the following statements. For each one, you may use the True statements from previous question parts as "external facts" in your proofs. You may also use the following facts about floor, as long as you clearly refer to them:

$$\forall x \in \mathbb{R},\ 0 \leq x - \lfloor x \rfloor < 1 \tag{Fact 1}$$

$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{R},\ \ \lfloor x + y \rfloor = x + \lfloor y \rfloor \tag{Fact 2}$$

(a) $\forall n \in \mathbb{N},\ \exists k \in \mathbb{N},\ \forall x \in \mathbb{R},\ \ \lfloor nx \rfloor - n \lfloor x \rfloor \leq k.$

(b) $\exists k \in \mathbb{N},\ \forall n \in \mathbb{N},\ \forall x \in \mathbb{R},\ \ \lfloor nx \rfloor - n \lfloor x \rfloor \leq k.$

(c) $\forall y \in \mathbb{R}^{\geq 0},\ \forall n \in \mathbb{Z}^+,\ n > y \Rightarrow \big(\exists \epsilon \in \mathbb{R}^{\geq 0},\ 0 \leq \epsilon < 1 \wedge y = (n+\epsilon)^2 - n^2\big)$

Hints: the quadratic formula may be helpful in your rough work; Also, $x - y = \dfrac{x^2 - y^2}{x + y}$.

(d) The function $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ defined as $f(x) = x^2 - (\lfloor x \rfloor)^2$ is onto.[1]

Refer to Worksheet 2 for the definition of onto; note that we originally defined it for functions $\mathbb{R} \to \mathbb{R}$, but here we adapt the definition for $\mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ instead.

[1] This statement can be proved/disproved using properties of continuity from calculus, but we haven't covered that in this course, and so such arguments aren't allowed for this problem set.

3. **[11 marks] Properties of functions**.

Please review the definitions of **even** and **odd functions** from Problem Set 1.

Prove or disprove each of the following statements.

(a) For every function $f : \mathbb{R} \to \mathbb{R}$, f is both even and odd if and only if it is the constant 0 function.

(b) Every function $f : \mathbb{R} \to \mathbb{R}$ can be written as a sum of an even function and an odd function.
Formally, for functions $f_1, f_2 : \mathbb{R} \to \mathbb{R}$, their sum is a function $(f_1 + f_2) : \mathbb{R} \to \mathbb{R}$ defined as $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ for all $x \in \mathbb{R}$.

(c) Every function $f : \mathbb{R} \to \mathbb{R}$ can be written as the product of an even function and an odd function.
The product of two functions is defined analogously to their sum (except using $\times$ instead of $+$).