CSC165H1: Problem Set 2

Due Sunday February 10 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. **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(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

- Final expressions in predicate logic must have negation symbols ($\neg$) applied **only** to predicates or propositional variables, e.g., $\neg p$ or $\neg Prime(x)$. To express "a is not equal to b," you can write $a \neq b$.
- 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, e.g., for divisibility and greatest common divisor. You may **not** use any external facts about these definitions unless they are explicitly stated in the question.

  However, you *may* make statements without proof about these definitions when they concern only specific integers, e.g., "7 is odd".

1. **[10 marks] Difference of Squares**. Let $n \in \mathbb{Z}^+$. We say that n is a **difference of squares** if it is of the form $p^2 - q^2$ for some positive integers p and q. We can capture this definition in the following predicate, defined over $\mathbb{Z}^+$:

$$\mathit{DifferenceOfSquares}(n): \quad \exists p, q \in \mathbb{Z}^+,\ n = p^2 - q^2$$

   (a) Translate the following statement into predicate logic: "Every difference of squares is odd or divisible by four."

   You may use the *DifferenceOfSquares* predicate in your translation, but you must expand the definition of divisibility (including in how you express "odd").

   (b) Prove the statement from part (a). Use the definition of divisibility; do *not* use any external facts about divisibility, except that you may use the Quotient-Remainder Theorem[1] to identify cases for your proof.

   (c) **(Corrected Jan 31)**[2] Prove or disprove the following statement:

$$\forall x, y \in \mathbb{Z}^+,\ \mathit{DifferenceOfSquares}(x) \land \mathit{DifferenceOfSquares}(y) \Rightarrow \mathit{DifferenceOfSquares}(x + y)$$

   If you want to disprove this statement, first write the negation of the statement in predicate logic. You may, but are not required to, use part (a) in your proof/disproof.

[1] pg. 50 of the Course Notes

[2] The original statement had a domain of $\mathbb{Z}$, which is inconsistent with the definition of our *DifferenceOfSquares* predicate.

2. **[14 marks] Greatest common divisor and divisibility**. Review the definition of the *greatest common divisor* of two integers on pg. 58 in the Course Notes (you'll also do a worksheet on this in Week 4).

   You may use the following external facts about divisibility in all parts of this question, as long as you clearly state when you use each one:[3]

$$\forall a, b, c \in \mathbb{N},\ a \mid b \land b \mid c \Rightarrow a \mid c \qquad \text{(Fact 1)}$$

$$\forall a, b, d \in \mathbb{Z},\ d \mid a \land d \mid b \Rightarrow \big(\forall p, q \in \mathbb{Z},\ d \mid (pa + qb)\big) \qquad \text{(Fact 2)}$$

$$\forall a, b \in \mathbb{Z},\ 2 \nmid a \land 2 \nmid b \Rightarrow 2 \nmid ab \qquad \text{(Fact 3 } \textbf{(NEW Jan 31)}\text{)}$$

   Note: We will *not* be marking translations into predicate logic for this question, but we still strongly recommend doing this as a first step for each proof/disproof.

   (a) Prove that for all integers a, m, and n, $\gcd(m, n) = \gcd(n, m - an)$.
   Hint: in your proof, let $e = \gcd(m, n)$, and prove that e is the greatest common divisor of n and $m - an$ using the definition of gcd.

   (b) Prove or disprove: for all integers a, m, and n, $\gcd(m, n) = \gcd(m, m - an)$.

   (c) **(Updated Jan 31)**[4] Prove that for all integers m and n, if m is odd then $\gcd(m, n) = \gcd(m, 2n)$.

   (d) Let $f : \mathbb{N} \to \mathbb{N}$ be the function $f(n) = n^2 + n + 1$. Prove that for all $n \in \mathbb{N}$, $\gcd(f(n), f(n + 1)) = 1$. You may use the True statements from the previous parts of this question in your proof.

[3] (**Jan 31**) We added one more additional fact you can use (Fact 3) in your proofs. See the FAQ for a few more details.

[4] We modified this statement from the original, because it's not necessary to assume that n is odd to prove the conclusion.

3. **[10 marks] Eventually bounded**. Let $f : \mathbb{N} \to \mathbb{R}^{\geq 0}$. We say that f is **eventually bounded** if and only if

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

Note: We will *not* be marking translations into predicate logic for this question, but we still strongly recommend doing this as a first step for each proof/disproof.

(a) Prove that the function $f(n) = \dfrac{1}{n+1}$ is eventually bounded.

(b) Prove that every *strictly decreasing* function $f : \mathbb{N} \to \mathbb{R}^{\geq 0}$ is eventually bounded. Note that we use the same definition of *strictly decreasing* as in Problem Set 1, except the function's domain and range are different here.

(c) For any two functions $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$, we define their **product function** to be the function $f \times g : \mathbb{N} \to \mathbb{R}^{\geq 0}$ as follows:

$$(f \times g)(n) = f(n) \cdot g(n), \qquad \text{where } n \in \mathbb{N}$$

Prove that for every two eventually bounded functions $f_1, f_2 : \mathbb{N} \to \mathbb{R}^{\geq 0}$, the function $f_1 \times f_2$ is also eventually bounded.