CSC165H1: Problem Set 1

Due October 4 before 10 p.m.

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_set1.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

- Final expressions 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 $a \neq b$.
- When rewriting logical formulas into equivalent forms (e.g., simplifying a negated formula or removing implication operators), you must **show all of the simplification steps involved**, not just the final result. We are looking for correct use of the various simplification rules here.
- You may not define your own predicates or sets for this problem set; please work with the definitions provided in the questions, or from the course notes.

1. **[4 marks] Truth tables and formulas.** Consider the following formula:

$$(p \vee q) \Rightarrow r$$

   (a) **[2 marks]** Write the truth table for the formula. (No need to show your calculations).

   (b) **[2 marks]** Write a logically equivalent formula that doesn't use $\Rightarrow$ or $\Leftrightarrow$, in other words it uses only $\wedge, \vee$, or $\neg$. Show how you derived the result.

2. **[10 marks] congruence**

Find a natural number m congruent to $5 \pmod 7$, and another natural number n congruent to $2 \pmod 7$. Find what the product mn is congruent to $\pmod 7$, and then make a statement about the congruence of the product of any pairs of natural numbers that have the same congruences as the m and n you found, $\pmod 7$.

   (a) **[5 marks]** Write a predicate formula that expresses your statement in the form of a universally quantified implication. If you believe the statement, prove it true. If you disbelieve the statement, prove it false.

   (b) **[5 marks]** Write the converse of your formula from the previous part. If you believe the converse, prove it true. If you disbelieve the converse, prove it false.

3. **[4 marks] one-to-one pigeonholes**

The **pigeonhole principle** says, informally, that if n pigeons roost in fewer than n pigeonholes, at least one pigeonhole will be crowded with more than 1 pigeon.

To make this precise, we first formalize the notion of un-crowded for $f : D \mapsto R$:

$$\text{OneToOne}(f)\text{: } \forall x, y \in D, x \neq y \Rightarrow f(x) \neq f(y), \text{ where } f : D \mapsto R,\ |D|, |R| \in \mathbb{N}^+.$$

Let $F = \{f \mid f : D \mapsto R \wedge |D| > 0 \wedge |R| > 0\}$ The pigeonhole principle says that:

$$\forall f \in F, \text{OneToOne}(f) \Rightarrow |D| \leq |R|$$

   (a) **[4 marks]** Use the pigeonhole principle to prove that if $n \geq 2$ people go to the same party, there are at least 2 people who shake hands with the same number of other people. **Hint**: Take the set of people at the party as your domain, define a function that evaluates how many people each person shook hands with.

You may also use the pigeonhole principle in subsequent questions in this assignment.

4. **[21 marks] modular arithmetic with primes**

Let a, p be natural numbers with p prime and $\gcd(a, p) = 1$. Let $T = \{1, \ldots, p-1\}$, the positive integers less than p.

Define $r_p(x)$ as the remainder after division of x by p.

Prove each of the following claims. You may use the result of an earlier claim to help prove a later claim, for example Claim (e) might help prove Claim (f). You may even use an earlier claim you haven't proven to help prove a later claim.

   (a) **[3 marks] Claim:** $\{r_p(an) \mid n \in T\} \subseteq T$. **Hint**: Consider the material in *Characterizations* in the course notes.

(b) **[3 marks] Claim**: If n_1 and n_2 are distinct numbers in T, then $r_p(an_1) \neq r_p(an_2)$. **Hint**: Consider the material in *Characterizations* in the course notes.

(c) **[3 marks] Claim**: $|\{r_p(an) \mid n \in T\}| = |T|$.

(d) **[3 marks] Claim**: $\{r_p(an) \mid n \in T\} = T$. **Hint**: For finite sets A and B if $A \subseteq B$ then $|B| = |B \setminus A| + |A|$.

(e) **[3 marks] Claim**: $\Pi_{i=1}^{i=p-1} r_p(ai) = \Pi_{i=1}^{i=p-1} i$.

(f) **[3 marks] Claim**: $r_p(a^{p-1}) = 1$. **Hint**: You may assume, as a consequence of Example 2.18, that if for $i \in \{1, 2, \ldots, k\}$ $a_i \equiv b_i \pmod{p}$, then $\Pi_1^k a_i \equiv \Pi_1^k b_i \pmod{p}$. You may also assume, as an extension of Example 2.14, that for any $k > 1$, if prime $p \nmid b_1 \wedge p \nmid b_2 \wedge \cdots \wedge p \nmid b_k$, then $p \nmid (b_1 \times b_2 \times \cdots \times b_k)$.

(g) **[3 marks] Claim**: If a is an arbitrary natural number that isn't divisible by 5, then $r_5(a^{100}) = 1$.

5. **[6 marks] primes**

Since, as shown in the course notes, there are infinitely many primes, it is not possible for a consecutive sequence of composite (non-prime) natural numbers to stretch on forever. However, arbitrarily long prime-free sequences exist. On the other hand, for any natural number we can always set an upper bound on how far away the next prime can be.

Prove each of the following statements. You may use the Prime predicate.

(a) **[3 marks] Claim**: For any $k \in \mathbb{N}$ there is some $n \in \mathbb{N}$ such that $n, n+1, \ldots, n+k$ are composite. **Hint**: Think about $(k+2)!$.

(b) **[3 marks] Claim**: For any positive natural number n there exists a prime p with $n < p < n! + 2$. **Hint**: Think about $n!$, and the proof of Theorem 2.3, that there are infinitely many primes.