CS 131 – Fall 2019, Prof. Tsourakakis
Assignment 4 must be submitted by Friday October 4, 2019 5:00pm, on Gradescope.

Problem 1. Suppose $A \cap C \subseteq B$, and $a \in C$. Prove that $a \notin A \setminus B$.

a) As we have seen in class, explain what is given to you, and what is the goal?

b) Express $a \notin A \backslash B$ as a conditional law by applying DeMorgan's law.

c) Formulate a direct proof strategy. Be specific about the set of logical premises, and the goal.

d) Use the direct proof strategy to give a proof of the theorem.

Problem 2. Let a be an integer. Prove by contraposition that if a^2 is divisible by 3, then a is divisible by 3.

Problem 3. In this problem we will prove by contradiction that $\sqrt{3}$ is irrational.

For the purpose of reaching a contradiction, we assume $\sqrt{3}$ is rational. That is, there exist an integer m and a natural number n such that $\sqrt{3} = \frac{m}{n}$.

Moreover, if m and n have a common divisor > 1, $\frac{m}{n}$ can always be simplified. So, also assume $\frac{m}{n}$ is already in the lowest terms.

a) Prove that m is divisible by 3.

b) Prove that n is divisible by 3.

c) Reach a contradiction.

Problem 4. Recall that sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$. Also recall that $A \subseteq B$ if and only if for all x, $x \in A \to x \in B$. Finally, recall that A^c denotes the set of all elements that are not in A. $A^c = \{x : x \notin A\}$.

Venn diagrams might help you visualize the problem.

a) Prove a "distributive law" for sets: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

b) Prove a "De Morgan's law" for sets: $(A \cup B)^c = A^c \cap B^c$.

Problem 5. In this problem, you will prove that division with remainder is well-defined. That is, you will prove that for any two integers $a > 0$ and b, there exists a unique remainder after the division of b by a. We will do the proof in two parts: first by proving that there is at most one remainder, and then by proving that there exists at least one remainder. The conclusion will be that there exists a unique remainder.

Assume a and b are both integers and $a > 0$. Define a *remainder* after the division of b by a to be a value r such that $r \geq 0$, $r < a$, and there exists an integer q for which $b = aq + r$.

a) Prove uniqueness. That is, if r_1 and r_2 are both remainders after the division of b by a, then $r_1 = r_2$. You can use without proof reasonable facts about integer multiplication, addition, subtraction, and $>$, but don't assume anything about integer division. In particular, you can use the fact that there are no integer multiples of a that are greater than 0 and less than a.

b) Let $S = \{$ integer $s \geq 0$: $\exists$ integer q such that $b = aq + s\}$. You can use without proof the following fact: every nonempty subset of nonnegative integers contains an element that is smaller than all other values in the subset. (This fact is actually part of the definition of nonnegative integers.) Prove that S contains a remainder after the division of b by a (that is, there is at least one remainder).