CS 131 – Fall 2019, Assignment 4
Problems 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?

Solution. Given: $A \cap C \subseteq B$, $a \in C$
Goal: $a \notin A \setminus B$

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

Solution. $a \notin A \backslash B$ is equivalent to $\neg(a \in A \wedge a \notin B)$ which by DeMorgan's law is $(a \notin A \vee a \in B)$ which is simply $(a \in A \to a \in B)$.

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

Solution. Given: $A \cap C \subseteq B$, $a \in C$
Goal: $a \in A \to a \in B$

A direct proof strategy will be:
Given: $a \in A$, $A \cap C \subseteq B, a \in C$
Goal: $a \in B$

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

Solution. Suppose $a \in A$. Then since $a \in C$, $a \in A \cap C$. But since $A \cap C \subseteq B$ it follows that $a \in B$. Thus it cannot be the case that a is an element of A but not B, so $a \notin A \backslash B$.

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

Solution. The contrapositive statement we are trying to prove is: if a is not divisible by 3, then a^2 is not divisible by 3.

So suppose a is not divisible by 3. Then we have two cases: $a = 3k+1$ for some k, or $a = 3k+2$ for some k.

- Case 1: $a = 3k + 1$ for some k. Then $a^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$ which is not divisible by 3.
- Case 2: $a = 3k + 2$ for some k. Then $a^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$ which is also not divisible by 3.

In either case 3 does not divide a^2.

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.

Solution. Since $\sqrt{3} = \frac{m}{n}$, $3 = \frac{m^2}{n^2}$, or $3n^2 = m^2$. Since 3 divides m^2, 3 divides m by the previous problem.

b) Prove that n is divisible by 3.

Solution. Since 3 divides m, $m = 3k$ for some integer k. Then $3n^2 = 9k^2$. Simplifying this, we get $n^2 = 3k^2$.

Again by the previous problem, we find that n is divisible by 3.

c) Reach a contradiction.

Solution. Both m and n are divisible by 3 but we assumed in the beginning that they have no common divisor. This is 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: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Solution. We need to prove two facts: $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$, and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

First we will show that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Take an arbitrary $x \in A \cup (B \cap C)$. Our goal now is to show that $x \in (A \cup B) \cap (A \cup C)$. $x \in A \cup (B \cap C)$ is equivalent to $(x \in A) \vee (x \in B \cap C)$ which is equivalent to $(x \in A) \vee (x \in B \wedge x \in C)$ which by a distributive law is equivalent to $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$.

This in turn is equivalent to $(x \in A \cup B) \wedge (x \in A \cup C)$ which is equivalent to $x \in (A \cup B) \cap (A \cup C)$.

Hence, $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

The proof for $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ is analogous.

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

Solution. Similarly to the previous part we need to prove that $(A \cup B)^c \subseteq A^c \cap B^c$ and $A^c \cap B^c \subseteq (A \cup B)^c$.

To show $(A \cup B)^c \subseteq A^c$, take any $x \in (A \cup B)^c$. By definition, $x \notin A \cup B$.

We will now prove by contradiction that $x \notin A$. Suppose $x \in A$. Then $(x \in A) \vee (x \in B)$ is also true. By definition of set union, $x \in A \cup B$. However, we know that $x \notin A \cup B$. Therefore, we reach a contradiction.

Simimilarly, we can show that $x \notin B$.

Then by definition of the complement $x \in A^c$ and $x \in B^c$. But then $x \in A^c \cap B^c$.

Therefore $(A \cup B)^c \subseteq A^c \cap B^c$.

To show $A^c \cap B^c \subseteq (A \cup B)^c$, take an arbitrary $x \in A^c \cap B^c$. Then $x \in A^c \wedge x \in B^c$. Applying the definition of the complement, $x \notin A \wedge x \notin B$. By DeMorgan's law, this is equivalent to $\neg(x \in A \vee x \in B)$. Then $\neg(x \in A \cup B)$ and consequently $x \in (A \cup B)^c$. So, $A^c \cap B^c \subseteq (A \cup B)^c$.

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.

Solution. Assume, for purposes of contradiction, that $r_1 \neq r_2$. Since r_1 is a remainder, there exists q_1 such that $b = aq_1 + r_1$. Since r_2 is a remainder, there exists q_2 such that $b = aq_2 + r_2$. Therefore, $aq_1 + r_1 = aq_2 + r_2$. We will now do a proof by cases.

- Case I: $r_1 > r_2$. Then $r_1 - r_2 = a(q_2 - q_1)$. On other hand, since $r_1 < a$ and $r_2 \geq 0$, $r_1 - r_2 < a$. And since $r_1 > r_2$, $r_1 - r_2 > 0$. But this is impossible, because $a(q_2 - q_1)$ is an integer multiple of a, and thus cannot be greater than 0 and less than a. This case leads to a contradiction.
- Case II: $r_2 > r_1$. By the same exact argument, this case also leads to a contradiction.
- Case III: $r_1 = r_2$. This case contradicts by assumption.

We have thus shown that every possible case leads to a contradiction. This completes the proof.

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).

Solution.

Claim 1. S is nonempty.

Proof. To prove this claim, we need to show that S contains at least one element. We will prove this fact by cases. First, consider the case when $b \geq 0$. Then $b \in S$, because for $q = 0$, $b = a \cdot q + b$. Now consider the case when $b < 0$. Let $t = b - ab$. Note that $t \geq 0$, because $t = b - ab = b(1 - a)$; and $b(1 - a)$ is nonnegative because b is negative and $(1 - a)$ is nonpositive (since $a \geq 1$). Note also that for $q = b$, $b = aq + t$. Therefore, $t \in S$. ■

Note that S is a subset of nonnegative integers, by definition of S. Therefore, since it is nonempty by the claim above, it contains an element that is smaller than all other values in S. Call this element m. There exists q such that $b = aq + m$.

Claim 2. $m < a$.

Proof. Indeed, suppose for purposes of contradiction that $m \geq a$. Let $m' = m - a$. Then $m' \geq 0$ and there exists q' such that $b = aq' + m'$: namely, $q' = q + 1$ (because $b = aq + m = aq + a + (m - a) = a(q + 1) + (m - a) = aq' + m'$). Thus, $m' \in S$. But $m' < m$, which contradicts the assumption that m is smaller than all other values in S. ■

Thus, $m \geq 0$ (because $m \in S$), $m < a$ (by the claim above), and there exists q such that $b = aq + m$ (because $m \in S$). Therefore, m is a remainder.