Solutions for Week Two

Problem One: Concept Checks

i. What is a universal statement?

A universal statement is a statement of the form "every *x* has [some property]."

ii. How do you prove a universal statement with a direct proof?

Choose an arbitrary *x*, then prove that it has the specified property.

iii. What is an existential statement?

An existential statement is a statement of the form "there is an *x* that has [some property]."

iv. How do you prove an existential statement with a direct proof?

Find an *x* with that property, then prove it has that property.

v. What an an implication?

An implication is a statement of the form "if *P*, then *Q*."

vi. What is an antecedent?

It's the first part of an implication. In "if *P*, then *Q*," the antecedent is *P*.

vii. What is a consequent?

It's the second part of an implication. In "if *P*, then *Q*," the consequent is *Q*.

viii. How do you prove an implication with a direct proof?

Assume the antecedent is true, then prove that the consequent must also be true.

ix. What is a lemma?

It's a smaller statement that's proved as part of a larger proof.

x. What is a proof by cases?

It's a proof where the proof splits into a number of cases and shows that the result must be true in each case.

xi. What is the contrapositive of the statement "if P is true, then Q is true?"

It's the statement "if Q is false, then P is false."

xii. What is the negation of the statement "if P is true, then Q is true?"

It's the statement "P is true and Q is false." It is **not** the statement "if P is true, then Q is false."

xiii. What is the negation of the statement "for all x, $P(x)$ is true?"

It's the existential statement "there is an x where $P(x)$ is false."

xiv. What is the negation of the statement "there is an x where $P(x)$ is true?"

It's the universal statement "for every x, $P(x)$ is false."

Problem Two: Properties of Integers

If n^2 is not a multiple of four, then n is odd. (★)

i. What is the contrapositive of statement (★)?

We can find the contrapositive by exchanging the antecedent and consequent of the implication, then negating each. If we do so, we get this statement: if n is even, then n^2 is a multiple of four.

ii. Prove statement (★) using a proof by contrapositive.

Proof: By contrapositive; we'll instead prove that if n is even, then n^2 is a multiple of four. To do so, consider any even integer n. Since n is even, there must be an integer k such that $n = 2k$. Therefore, we see that $n^2 = (2k)^2 = 4k^2$. This means that there is an integer m, namely, k^2, such that $n^2 = 4m$. Thus n^2 is a multiple of four, as required. ■

iii. What is the negation of statement (★)?

The negation of an implication of the form $P \to Q$ is the statement $P \wedge \neg Q$. Here, this is the statement "n^2 is not a multiple of four, but n is even."

iv. Prove statement (★) using a proof by contradiction.

Proof: Assume for the sake of contradiction that there exists an integer n such that n^2 is not a multiple of four, but n is even. Since n is even, there must be an integer k such that $n = 2k$. Therefore, we see that $n^2 = (2k)^2 = 4k^2$. This means that there is an integer m, namely, k^2, such that $n^2 = 4m$. Therefore, n^2 is a multiple of four, contradicting our earlier statement that n^2 is not a multiple of four. We've reached a contradiction, so our assumption must have been wrong. Therefore, if n^2 is not a multiple of four, then n is odd. ■

v. Let's suppose that n is an arbitrary integer. Can you say anything about remainder you get when you divide n^2 by four? Play around, see what you find, then formalize your result by writing up a formal mathematical proof.

With some exploration we hope you found that every integer's square is either a multiple of four or congruent to one modulo four. There are a couple of different ways that you can go about proving it. One way, which is probably one of the more natural things to try, is to pick an integer n and then look at the remainder modulo four:

Theorem: If n is an integer, then n^2 is either a multiple of four or congruent to one modulo four.

Proof 1: Let n be an arbitrary integer. We consider four cases:

Case 1: n is a multiple of four. Then there is an integer k such that $n = 4k$ for some integer k. This means that $n^2 = (4k)^2 = 16k^2$, so $n^2 = 4(4k^2)$. This means that n^2 is a multiple of four.

Case 2: n is congruent to one modulo four. Then there is an integer k such that $n = 4k + 1$ for some integer k. Then $n^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1$, so n^2 is congruent to one modulo four.

Case 3: n is congruent to two modulo four. Then there's an integer k such that $n = 4k + 2$ for some integer k. We see that $n^2 = (4k+2)^2 = 16k^2 + 16k + 4 = 4(4k^2 + 4k)$ so n^2 is a multiple of four.

Case 4: n is congruent to three modulo four. Then there is an integer k such that $n = 4k + 3$ for some integer k. This means that $n^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1$, so n^2 is congruent to one modulo four.

In all four cases, we see that n^2 is either a multiple of four or congruent to one modulo four, as required. ■

However, we can actually get away with fewer cases if we just look at whether n is odd or even:

Theorem: If n is an integer, then n^2 is either a multiple of four or congruent to one modulo four.

Proof 2: Let n be an arbitrary integer. We consider two cases:

Case 1: n is even. This means that there is an integer k where $n = 2k$. This then tells us that

$$n^2 = (2k)^2 = 4k^2$$

and so n^2 is a multiple of four.

Case 2: n is odd. Then there is an integer k such that $n = 2k + 1$, so we see that

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

and so n^2 is congruent to one modulo four.

This shows that n^2 is either a multiple of four or congruent to one modulo four, as required. ■

vi. According to the US Census Bureau estimates, the population of the United States on January 1, 2016 was 322,761,807. Prove that there are no integers m and n where $m^2 + n^2 = 322{,}761{,}807$.

Proof: Suppose for the sake of contradiction that there are integers m and n such that

$$m^2 + n^2 = 322{,}761{,}807.$$

Notice that 322,761,807 is congruent to three modulo four. Now, each of m^2 and n^2 is either a multiple of four or congruent to one modulo four. We consider three cases.

Case 1: Both m^2 and n^2 are multiples of four. Then there are integers r and s such that $m^2 = 4r$ and $n^2 = 4s$, so $m^2 + n^2 = 4r + 4s = 4(r + s)$, which is not congruent to three modulo four.

Case 2: Exactly one of m^2 and n^2 is a multiple of four and the other is congruent to one modulo four. Without loss of generality, assume $m^2 = 4r$ and $n^2 = 4s + 1$. Then $m^2 + n^2 = 4r + 4s + 1 = 4(r + s) + 1$, which is not congruent to three modulo four.

Case 3: Both m^2 and n^2 are congruent to one modulo four. Then $m^2 = 4r + 1$ and $n^2 = 4s + 1$ for some integers r and s. This means that $m^2 + n^2 = 4r + 1 + 4s + 1 = 4(r + s) + 2$, which is not congruent to three modulo four.

In all three cases, we see that $m^2 + n^2$ is not congruent to three modulo four. But this is impossible – since $m^2 + n^2 = 3{,}805{,}927$, we know that $m^2 + n^2$ is congruent to three modulo four. We've reached a contradiction, so our assumption must have been incorrect. Therefore, there are no integers m and n such that $m^2 + n^2 = 322{,}761{,}807$. ■

Why we asked this question: We chose this question to get you playing around with proof by contradiction, proof by contrapositive, and proof by cases. We hoped that the first four parts of the problem would be a good way to get you playing around with how to take negations and contrapositives and that the proofs in question were sufficiently similar to the ones from lecture that the focus would be on the key techniques rather than on the mathematical gymnastics. Part (v) of this problem was designed to get you to explore and to formulate a hypothesis that you could then prove, as well as to get you playing around with proof by cases.

Finally, part (vi) of this problem was designed to get you to use your earlier results as stepping stones toward a larger (and less obvious) result. If you were hoping to divide everyone in the US into two groups and have them stand in perfectly square grids, unfortunately, you will need to find a different task to focus your efforts on.

Problem Three: Balls in Bins

Suppose that you have twenty-five balls to place into five different bins. Eleven of the balls are red, and the other fourteen are blue. Prove that no matter how the balls are placed into the bins, there must be at least one bin containing at least three red balls.

Proof: Suppose for the sake of contradiction that the balls are placed in the bins and every bin has at most two red balls. That means that there are at most ten balls, since there are five bins with at most two red balls each, which is impossible. We've reached a contradiction, so our assumption must have been wrong. Thus there must be at least one bin with at least three red balls. ■

Why we asked this question: This question was designed as a proof by contradiction without any guidance. It's related to a result called the *generalized pigeonhole principle* that we'll explore in a few weeks.

Problem Four: Pythagorean Triples

A *Pythagorean triple* is a triple of positive natural numbers (a, b, c) such that $a^2 + b^2 = c^2$. For example, (3, 4, 5) is a Pythagorean triple because $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

i. Prove that if (a, b, c) is a Pythagorean triple, then at least one of a, b, and c is even.

There are several ways you could prove this. Here are two options, one done by contrapositive and one done by contradiction:

Proof: We will instead prove the contrapositive, that if each of a, b, and c is odd, then (a, b, c) is not a Pythagorean triple. Since a and b are odd, we know that a^2 and b^2 are odd as well. Therefore, $a^2 + b^2$ is even. Similarly, since c is odd, we know that c^2 is odd as well. Therefore, $a^2 + b^2 \neq c^2$, since no even number is equal to an odd number. Consequently, (a, b, c) is not a Pythagorean triple, as required. ■

Proof: Assume for the sake of contradiction that there is a Pythagorean triple (a, b, c) such that each of a, b, and c are odd.

Since a and b are odd, we know that a^2 and b^2 are odd as well. Therefore, $a^2 + b^2$ is even. Similarly, since c is odd, we know that c^2 is odd as well. Now, since we assumed (a, b, c) is a Pythagorean triple, we know that $a^2 + b^2 = c^2$. But this is impossible, since the left-hand side of this equation is even and the right-hand side of this equation is odd.

We have reached a contradiction, so our assumption must have been wrong. Therefore, in any Pythagorean triple (a, b, c), at least one of a, b, and c must be even. ■

Notice how the cores of these proofs are the same – we ultimately get to the conclusion that $a^2 + b^2$ is even but that c^2 is odd, so we see that $a^2 + b^2 \neq c^2$. The difference between the proofs is how that argument is structured. In the proof by contrapositive, we start with the assumption that a, b, and c are odd, then are done once we conclude that $a^2 + b^2 \neq c^2$ because this proves the implication "if a, b, and c are odd, then (a, b, c) is not a Pythagorean triple." In the proof by contradiction, we also assume that a, b, and c are odd, conclude that $a^2 + b^2 \neq c^2$, but then conclude the proof by saying that we've reached a contradiction, since we also assumed that $a^2 + b^2 = c^2$. I personally prefer the proof by contrapositive here because I think the argument is a bit cleaner (there's no need to say "but that's impossible, so we're done,") but either proof approach would be totally fine.

ii. Prove that if (a, b, c) is a Pythagorean triple, then (a+1, b+1, c+1) is *not* a Pythagorean triple.

There are many ways that we could do this proof, either directly, by contradiction, or by contrapositive. I personally think that this proof is easiest to do by contradiction, so that's the proof I've included here.

Proof: Assume for the sake of contradiction that there are positive integers a, b, and c such that (a, b, c) is a Pythagorean triple and (a+1, b+1, c+1) is also a Pythagorean triple. Expanding out the definitions, we see that

$$a^2 + b^2 = c^2 \tag{1}$$

and that

$$(a+1)^2 + (b+1)^2 = (c+1)^2. \tag{2}$$

We can rewrite equation (1) to see that

$$a^2 + b^2 - c^2 = 0 \tag{3}$$

Let's now expand and simplify equation (2) as follows:

$$(a+1)^2 + (b+1)^2 = (c+1)^2$$
$$(a^2 + 2a + 1) + (b^2 + 2b + 1) = (c^2 + 2c + 1)$$
$$(a^2 + b^2 - c^2) + 2a + 2b + 2 = 2c + 1$$
$$2(a + b + 1) = 2c + 1 \tag{4}$$

(That last step follows from statement (3)). However, statement (4) is impossible – the left-hand side is an even number, and the right-hand side is odd.

We have reached a contradiction, so our assumption must have been wrong. Therefore, if we know that (a, b, c) is a Pythagorean triple, we know that (a+1, b+1, c+1) must not be. ■

Why we asked this question: We included this problem for a number of reasons. First, we included this problem because, unlike the previous problems, there aren't any hints about how to proceed. We wanted you to get the experience of working through a problem where it really isn't immediately clear what approach you should take. Second, this problem can be solved using a number of different techniques, and therefore is a great testbed for trying out different proof approaches. Finally, while there are many ways to solve this problem, many of them ultimately boil down to showing that two numbers can't be equal because one is odd and one is even, a technique that (hypothetically speaking) might be useful later on.

Problem Five: Proofs on Set Theory

In the middle of class, we'll take a break to prove the following result: if A and B are arbitrary sets, then $\wp(A) \cap \wp(B) \subseteq \wp(A \cap B)$. Once we've done that and you've seen that proof, prove the following statement: if A and B are any sets, then

$$\wp(A) \cap \wp(B) = \wp(A \cap B).$$

Proof: Let A and B be arbitrary sets. We will prove that $\wp(A) \cap \wp(B) = \wp(A \cap B)$. To do so, we will show that $\wp(A) \cap \wp(B) \subseteq \wp(A \cap B)$ and that $\wp(A \cap B) \subseteq \wp(A) \cap \wp(B)$. Since we proved the first of these statements as a group, we only need to prove the second.

Consider any $S \in \wp(A \cap B)$. This means that $S \subseteq A \cap B$. We need to prove that $S \in \wp(A) \cap \wp(B)$, meaning that we need to show that $S \in \wp(A)$ and $S \in \wp(B)$. Equivalently, we need to show that $S \subseteq A$ and that $S \subseteq B$.

Consider any $x \in S$. Since $S \subseteq A \cap B$ and $x \in S$, we see that $x \in A \cap B$. This means that $x \in A$ and $x \in B$. Since our choice of x was arbitrary, we've shown that any arbitrary $x \in S$ satisfies $x \in A$ and also satisfies $x \in B$, so we see that $S \subseteq A$ and $S \subseteq B$, as required. ■

Why we asked this question: This question was designed to get you working with set equality and hopefully the theorem that if $S \subseteq T$ and $T \subseteq S$, then $S = T$. We also hoped that this question would get you thinking about how to "unpack" set theory definitions and ultimately reason about the sets in question by expanding out the definitions of $\wp$, $\subseteq$, and $\cap$ into simpler statements about the $\in$ relation.

Problem Six: A Review of Propositional Logic

List the seven propositional connectives and give their truth tables. Check your answers by using the online truth table tool.

The seven connectives are shown here:

$$\wedge \quad \vee \quad \neg \quad \rightarrow \quad \leftrightarrow \quad \top \quad \bot$$

Since you can use the Truth Table Tool to look up their truth tables, we won't list them here. But do head over to the CS103 website to learn more!

Problem Seven: Knight's Tours

Prove that there is no knight's tour that starts in the bottom-left corner of the board and ends in the upper-right corner of the board.

Proof: Notice that whenever a knight moves, the color of the square it's sitting on changes from white to black or from black to white. Therefore, if a knight moves an even number of times, it will end up on a square of the same color that it started on (the color flips cancel out), and if a knight moves an odd number of times, it will end up on a square of the opposite color.

In a knight's tour, the knight visits 64 squares, so it must move 63 times. Therefore, it must start and end on squares of different colors. Since diagonally opposite corners of a chessboard have the same color, this means that a knight's tour cannot start and end on diagonally opposite corners of the chessboard. ■

Why we asked this question: This question was designed as a wrap-up question that's more challenging than the other ones from this particular packet of problems. It's more insight-driven than the other problems, which we figured would be an interesting contrast from before. We also thought that this would be a good example of a clean writeup of a proof that's more conversational and less mathematical but is still perfectly rigorous.