CS 131 - Spring 2020, Assignment 7 Answers

Andy Vo

April 3, 2020

Tools: $\emptyset, \in, \notin, \subseteq, \subset, \cup, \cap, \exists, \forall, \neg, \vee, \wedge, \iff, \rightarrow, \leftarrow, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \neq, \therefore, \leq, \geq, \{\}$

Problem 1.

1.

a) This proof does not use variables to introduce why m and n are odd. Rather, it uses a specific instance where m = 7 and n = 9. Thus, we cannot assume that the proof applies to all odd numbers for m and n.

b) This proof lacks the assumptions of what are k and j. We do not introduce them as integers; we are only given "since they are integers", implying the fact before introducing it.

c) This proof skips essential steps and does not show how the product of two odd numbers is odd. It simply assumes that without showing proof through mathematical equations.

d) This proof does not make sense because does not apply any fact with variables k and j. Rather, it skips the steps needed to prove that $n^2 + m^2$ is equivalent to two times an another integer that has to have been introduced. We are only given this $(2k+1)^2 + (2j+1)^2$, which does not conclude anything.

e) This proof lacks the step of explaining why $4j^2 + 4j + 1$ is also an integer. It must introduce the variable name that indicates that it represents a variable.

2.

a) True.

Proof. Assume x and y are even integers, such that $x = 2k$ where k is any integer, and $y = 2j$ for j of any integer. So $x + y = 2k + 2j = 2(k + j)$. Since k and j are both integers, $k + j = m$, where m is an integer. Since $x + y$ is two times larger than $k + j$ and that $x + y = 2(m)$ where m is an integer, then $x + y$ is even. Therefore, if x and y are even, then $x + y$ is even. ∎

b) False. Any choice in which x and/or y are odd numbers is a counterexample. For example, $x = 3$ and $y = 3$. $x + y = 6$ which is even; however, x and y are both odd integers.

i) False. Any choice in which x and/or y are not perfect squares is a counterexample. For example, $x = 3$ and $y = 12$. $xy = 36$, which is a perfect square because $\sqrt{36} = 6 \cdot 6$; however, $x(3)$ and $y(12)$ are not perfect squares themselves.

k) True.

Proof. Assume x, y, and z are all integers and that $xy|z$, or rather, xy divides z. We will show that x divides z and y divides z. Since x and y are integers and xy divides z, x and y are nonzero and there is an integer k such that $k(xy) = z$. Therefore, we know x divides z because $x|z = ky = m$ where ky is an integer m because we know that an integer multiplied by another integer is an integer. Furthermore, we can apply it the other way and prove that $y|z = kx = n$ where kx is an integer n because we know that an integer multiplied by an integer is an integer. Thus, if x, y, and z are integers such that xy divides z, then x divides z and y divides z. ■

l) False. Any choice in which x does not divide y and x does not divide z is a counterexample. For example, if $x = 6$, $y = 2$, and $z = 9$. $x|yz$ is true since 6 divides 18. However, there does not exist an integer where 6 divides 2 or 6 divides 9.

3.

a)

Proof. Assume n is an integer such that n^3 is even. We will prove that n is even by contradiction. Suppose that there is an integer n such that n^3 is even and n is odd. If n is odd, then n can be expressed such that $n = 2k+1$ where k is any integer. So, by substituting n in for n^3, $n^3 = (2k+1)^3 = (2k+1)(2k+1)(2k+1) = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$. Since k is an integer, $4k^3 + 6k^2 + 3k$ can be expressed as an integer j by mathematical definition of multiplication. Thus, $n^3 = 2j + 1$, which is a contradiction to our assumption that n^3 is even. Therefore, n is not an odd integer; rather, it is an even integer. ■

b)

Proof. We will prove that $\sqrt[3]{2}$ is irrational, we will prove by contradiction. We assume that $\sqrt[3]{2}$ is rational, and therefore can be expressed as the ratio of two integers n/d, where $d \neq 0$ and n and d do not have any common factors. Therefore, we can assume that there is no integer greater than 1 that divides both n and d. Cubing both sides of the equation $\sqrt[3]{2} = n/d$ gives $2 = n^3/d^3$. Multiplying both sides by d^3 gives $2d^3 = n^3$. Since n^3 is an integer multiple of 2, we know that n^3 is even. If the cube of an integer is even, then the integer itself must be even. Therefore, n is even which means that n can be expressed as $2k$ for some integer k. By plugging $2k$ for n into n^3, $n^3 = (2k)^3 = 8k^3$. By combining the two equations, it yields $2d^3 = 8k^3$. Dividing both sides by 2 results in the equation $d^3 = 4k^3 = 2(2k^3)$. Therefore, d^3 is even, and we can use the fact about cubed integers from before that if the cube of an integer is even, then that integer is also even. Thus, d is even. Since both n and d are even, both are divisible by 2. This contradicts the assumption made at the beginning that the greatest integer that divides both numbers (a common factor) is 1. This contradiction concludes that $\sqrt[3]{2}$ is a rational number is a false assumption. ■

4.

c)

Proof. If x is a real number such that $x^2 + 2x - 3 < 0$, then $-3 < x < 1$.
Case 1: $x \leq -3$. We want to prove that $x^2 + 2x - 3 \geq 0$. When $x = -3$, $(-3)^2 + 2(-3) - 3 = 9 - 6 - 3 = 0$. If x equal to -3, then the left-side term of the inequality above will be non-negative, equalling 0. For all real numbers where $x < 3$, the resulting number will be a non-negative number. We know this because x^2 grows exponentially larger compared to the linear growth of $2x$ when x is a negative number. By proving the contrapositive, we have proven that $x^2 + 2x - 3 < 0$ for $x > -3$.
Case 2: $x \geq 1$. We want to prove that $x^2 + 2x - 3 \geq 0$. When $x = 1$, $1^2 + 2(1) - 3 = 1 + 2 - 3 = 0$, which is non-negative. For all real numbers where $x \geq 1$, we get a non-negative number. Proving the contrapositive, we can conclude that if x is a real number such that $x^2 + 2x - 3 < 0$, then $-3 < x < 1$.

■

d) If x is a real number such that $x^2 - 3x - 10 < 0$, then $-2 < x < 5$.
Case 1: $x \leq -2$. We want to prove that $x^2 - 3x - 10 \geq 0$. Firstly, when $x = -2$, $(-2)^2 - 3(-2) - 10 = 4 + 6 - 10 = 0$, which is non-negative and is true. Now let's say we have a real number $k = x$ where $k \leq -2$ such that $k^2 - 3k - 10 \geq 0$. Let's prove that the statement is true for $x = k - 1$, such that $(k-1)^2 - 3(k-1) - 10 \geq 0$. $(k-1)^2 - 3(k-1) - 10 = k^2 - 2k + 1 - 3k + 3 - 10 = (k^2 - 3k - 10) - (2k - 4) \geq 0$. We proved that $(k-1)^2 - 3(k-1) - 10 \geq 0$ since $-(2k-4) \geq 0$ for $k \leq -2$. Therefore, the statement is true for $k - 1$. By the principle of mathematical induction, we proved the basis steps and the inductive steps along with proof by contrapositive to show that $x^2 - 3x - 10 < 0$ is true for $x > -2$ because we will always get a non-negative number.
Case 2: $x \geq 5$. We want to prove that $x^2 - 3x - 10 \geq 0$. Firstly, when $x = 5$, $(5)^2 - 3(5) - 10 = 25 - 15 - 10 = 0$, which is non-negative and is true. Now let's say we have a real number $k = x$ where $k \geq 5$ such that $k^2 - 3k - 10 \geq 0$. Let's prove that the statement is true for $x = k + 1$, such that $(k+1)^2 - 3(k+1) - 10 \geq 0$. $(k+1)^2 - 3(k+1) - 10 = k^2 + 2k + 1 - 3k - 3 - 10 = (k^2 - 3k - 10) + (2k - 2) \geq 0$. We proved that $(k+1)^2 - 3(k+1) - 10 \geq 0$ since $(2k-2) \geq 0$ for $k \geq 5$. Therefore, the statement is true for $k + 1$. By the principle of mathematical induction, we proved the basis steps and the inductive steps along with proof by contrapositive to show that $x^2 - 3x - 10 < 0$ is true for $x < 5$ because we will always get a non-negative number.

Problem 2.

Proof. Assume there are integers numbers b_1, b_2, and non-zero integer number a such that there is a remainder r_1 when b_1 is divided by a, and there is a remainder r_2 when b_2 is divided by a. By definition of the division theorem, because a divides b_1 with remainder r_1, then $b_1 = ak + r_1$, where k is some integer and we know that r_1 is an integer such that $r_1 \geq 0$, and $r_1 < a$. Likewise, because a divides b_2 with remainder r_2, then $b_2 = aj + r_2$ by the division theorem, where j is some integer and we now that r_2 is an integer such that $r_2 \geq 0$, and $r_2 < a$.
We will prove that $b_1 + b_2$ has a remainder $r_1 + r_2$ or $r_1 + r_2 - a$ when divided by a. By the division theorem, there exists an integer q such that $b_1 + b_2 = aq + (r_1 + r_2)$. Furthermore, because $r_1 \geq 0$ and $r_2 \geq 0$, then $r_1 + r_2 \geq 0$. We know that $r_1 + r_2$ is the remainder when $r_1 + r_2 < a$. However, there is also the case where $r_1 + r_2 - a$ is the remainder. This is when $r_1 + r_2 > a$. For example, if $b_1 = 7$, $b_2 = 6$, and $a = 4$. $r_1 = 3$, $r_2 = 2$, and thus, $r_1 + r_2 = 5 > 4 = a$, and the remainder to $(b_1 + b_2)/a = 13/4$ is 1 which is obtained when $r_1 + r_2 - a = 3 + 2 - 4 = 1$. Thus, we will prove that $b_1 + b_2$ has a remainder $r_1 + r_2$ or $r_1 + r_2 - a$ when divided by a using two cases.
Case 1: $r_1 + r_2 < a$. In the case where the sum of the remainders is less than the divisor, let's have an example where $b_1 = 14$, $b_2 = 8$, and $a = 6$. The remainders will be $r_1 = 2$ and $r_2 = 2$. So, $r_1 + r_2 = 2 + 2 = 4 < 6 = a$. As mentioned before, there exists an integer q such that $b_1 + b_2 = aq + (r_1 + r_2)$. We know that $r_1 + r_2 >= 0$ because $r_1 \geq 0$ and $r_2 \geq 0$, and thus, the addition of two non-negative integers is a non-negative integer. We prove that $r_1 + r_2 < a$ when either b_1 modulo a and b_2 modulo a is less than half of a. Thus, we have proven that $r_1 + r_2$ is a remainder of $b_1 + b_2$.
Case 2: $r_1 + r_2 > a$. In the case where the sum of the remainders is more than the divisor, b_1 modulo a and b_2 modulo a is more than half of a. For example, $b_1 = 7$, $b_2 = 6$, and $a = 4$, so that $r_1 = 3$, $r_2 = 2$, and $r_1 + r_2 = 3 + 2 = 5 > 4 = a$. We can prove that $r_1 + r_2 - a$ is a remainder because firstly, $r_1 + r_2 \geq 0$ because since $r_1 + r_2 \geq a$ and a is a positive integer, then $r_1 + r_2 \geq 0$. Secondly, $r_1 + r_2 - a < a$ because by adding a to both sides, we get $r_1 + r_2 < 2a$, and can be rewritten as $((r_1 + r_2)/2) < a$, which is true because the remainders can never be equal to b_1 or b_2, which means that the combination of remainders can be at most less than half of the divisor. Furthermore, there exists an integer q such that $b_1 + b_2 = aq + (r_1 + r_2 - a)$. ■

Problem 3.

a)

Proof. Assume there are integers a such that $a > 0$ and b, such that there exists a unique remainder r after the division of b by a such that $r \geq 0$ and $r < a$. Furthermore, by the division theorem, let's assume there exists an integer q for which $b = aq + r$. We will prove uniqueness of remainders by contradiction by cases. As such, if r_1 and r_2 are both remainders after the division of b by a, then $r_1 = r_2$.
Suppose we have two remainders r_1 and r_2 such that

$$b = aq_1 + r_1$$

$$b = aq_2 + r_2$$

Combining the equations, $aq_1 + r_1 = aq_2 + r_2$. Rearranging the equation, we can get $aq_1 - aq_2 = r_2 - r_1$, which is also equal to $a(q_1 - q_2) = r_2 - r_1$. Suppose we have the following cases:
Case 1: $r_2 > r_1$. Since we have $a(q_1 - q_2) = r_2 - r_1$ where $a > r_2 \geq r_1 \geq 0$, then we know $a > r_2 \geq r_2 - r_1 \geq 0$. This means that because $r_2 < a$ and $r_1 \geq 0$, then $a(q_1 - q_2) = r_2 - r_1$. Thus, $a > a(q_1 - q_2) \geq 0$, which is $1 > q_1 - q_2 \geq 0$ when we cancel out the a. Since q_1 and q_2 are integers, the subtraction of integers is an integer. Therefore, $q_1 - q_2 = 0$, or $q_1 = q_2$. The implies that $r_2 - r_1 = 0$, or $r_2 = r_1$, which contradicts that notion that $r_2 > r_1$, proving that there is a unique quotient and unique remainder.
Case 2: $r_1 > r_2$.
However, these two cases are similar if we simply swap the position of the variables such that $a(q_1 - q_2) = r_2 - r_1$ for $r_2 > r_1$ becomes $a(q_2 - q_1) = r_1 - r_2$ for $r_1 > r_2$. Thus, without loss of generality, we can simply assume one remainder is larger than the other to prove by contradiction that they must be the same number and therefore, unique. ■

b)

Proof. Assume $S = \{\text{integer } s \geq 0 : \exists \text{ integer } q \text{ such that } b = aq + s\}$. We will prove that set S contains a remainder after the division of real numbers b by a (that there exists at least one remainder). If $s \geq 0$ (a non-negative number $\mathbb{N}$), then we know that $(0)a + s \in \mathbb{N}$. We now know there exists at least one element in set S, such that $S \neq \emptyset$. We can now prove that there is at least one element s where $s \geq 0$ in set S for every a and b.
Case 1: $b \geq 0$. If integer $q = 0$, then by algebraic manipulation $b = s$ which is true because $a \cot 0 = 0$ and $s \geq 0$. This satisfies the conditions if $b \geq 0$. Essentially, for any integer $b \geq 0$, there is an integer $s \geq 0$. In another way to put it, if we have $b - aq = s$ where we set $q = 0$, then we have $b - 0 = s$, which is true because both b and s are integers that are greater than 0, implying that we have an element in our set for $b \geq 0$. Thus, we have proven that there exists such an s based on a function of a and b when $b \geq 0$.
Case 2: $b < 0$. If we manipulate the expression such that $b - aq \geq 0$, we can set $q = b$, which will result in $b - ba = b(1 - a) = s$ and we are trying to show that this is an element in our set. We know that $a > 0$ because a divides b and thus cannot be zero (definition of a divisor). Thus, a has to be at least 1, so if we let $1 - a = k$ where k is an integer, k will either be zero or negative. Thus, $b(1 - a)$ or bk will always either be zero or positive since a negative times a negative is positive. Thus, we have proven that there exists an element in our set S, so that it is non-empty. ■

c)

Proof. Assume that m is an element in set S such that it is the smallest number in S. Essentially, there is an element m such that $0 \leq m < a$ where $b = aq + m$ for some integer q where a and b, as mentioned throughout this proof, are integers where a is non-zero by definition of a divisor. We know that m is the smallest element in S and that there exists this element integer q such that $b = aq + m$. By definition, every non-empty subset of non-negative integers contains an element that is smaller than all other values in the subset. So let's assume that $m \geq a$. Then we can claim that $b - (aq) \geq a$. Subtracting a on both sides, we get $b - (aq) - a \geq 0$, which is equivalent to $b - ((q + 1)a) \geq 0$. We know that $b - ((q + 1)a)$ is an element in S. Since $m = b - aq$, then $b - ((q + 1)a) = m - a$ since we subtracted a on both sides. That means that $b - ((q + 1)a) < m$ because a is a positive integer, which means that m is not the smallest element. This contradiction proves that m is smaller than the divisor a and thus, the smallest integer and remainder in this set S for $b = aq + m$. ■

d)

In conclusion, we have proven the following: When non-zero integer a divides integer b, there exists a unique quotient q which is an integer such that $b = aq$ and there exists at least one and only one unique remainder r that is always smaller than the divisor a such that $b = aq + r$. Thus, there is a unique remainder r after the division of b by a.

Problem 4.

a)

Proof. Assume that for any real number c, there exists $\lceil c \rceil$ for every real c as an integer d such that $\exists z$ with $0 \leq z < 1$ and $c = d - z$. We will prove that there exists a unique $\lceil c \rceil$ for any c by contradiction.
Say there are integers d_1 and d_2, and there exist numbers z_1 and z_2 where $0 \leq z_1 < 1$ and $0 \leq z_2 < 1$ such that $d_1 - z_1 = c = d_2 - z_2$. To show uniqueness by contradiction, we will prove that $d_1 \neq d_2$. Changing the equation, we show that $d_1 - d_2 = z_1 - z_2$. Thus, we can have two cases:
Case 1: $z_1 = z_2$. If $z_1 = z_2$, then $z_1 - z_2 = 0$, and substituting that into the equation, $d_1 - d_2 = 0$. As a result, $d_1 = d_2$, which is a contradiction against the fact that $d_1 \neq d_2$.
Case 2: $z_1 \neq z_2$. Without loss of generality, $z_1 > z_2$ will produce a very similar result as $z_2 > z_1$. We know $z_1 - z_2$ must be an integer because d_1 and d_2 are integers and integer subtraction yields an integer. The range of $z_1 - z_2$, then, is $-1 < z_1 - z_2 < 1$ because $0 \leq z < 1$. Given that the bounds of $z_1 - z_2$ are -1 and 1 non-inclusively, 0 is the only integer that satisfies $z_1 - z_2$. If $z_1 - z_2 = 0$, then $z_1 = z_2$, which means $d_1 = d_2$, which contradicts the assumption made before that $d_1 \neq d_2$.
As a result, in both cases, we have proven by contradiction and cases that there is a unique $\lceil c \rceil$ for every c. ■

b)

Proof. To prove that $\forall a, b : \lceil a + b \rceil$ is equal to $\lceil a \rceil + \lceil b \rceil$ or $\lceil a \rceil + \lceil b \rceil - 1$, let there be integers a and b such that $a = \lceil a \rceil - z_1$ and $b = \lceil b \rceil - z_2$, where z_1 and z_2 are also integers. Therefore, $a + b = \lceil a \rceil - z_1 + \lceil b \rceil - z_2 = \lceil a \rceil + \lceil b \rceil - (z_1 + z_2)$. We will prove by cases where this.
Case 1: $0 \leq z_1 + z_2 < 1$. Since z_1 and z_2 are integers, the addition of integers will result in an integer, and let's call that z_3 such that $z_1 + z_2 = z_3$. Since z_3 must be an integer, and given the condition of $0 \leq z_1 + z_2 < 1$, then the most and only integer z_3 can be is 0. When evaluating the ceiling of the summation of a and b, we must turn to the definition of a ceiling function to properly alter our equation. By definition of a ceiling of a term, $\lceil a + b \rceil = d - z$ where d and z are integers as proved in the previous proof. Since the ceiling function of a term is an integer d, then we can substitute the ceiling of a and ceiling of b as both are integers for integer d_0. Furthermore, the z term is an integer and we have proven that z_3 can only be 0. Combining all of the components together, $\lceil a + b \rceil = \lceil a \rceil + \lceil b \rceil - 0 = \lceil a \rceil + \lceil b \rceil$. **Case 2:** $1 \leq z_1 + z_2 < 2$. Similar to Case 1, the summation of z_1 and z_2 can be at most 1 given the condition. Substituting that into the equation for the ceiling of $a + b$, we get $\lceil a + b \rceil = \lceil a \rceil + \lceil b \rceil - 1$. Thus, the ceiling of $a + b$ can be expressed as $\lceil a \rceil + \lceil b \rceil$ or $\lceil a \rceil + \lceil b \rceil - 1$ for all a and b. ■

Problem 5.

Prove that $\forall n \in \mathbb{N}, \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

Proof. Is this true for $n = 0$? $2^0 = 1$ and $2^{0+1} - 1 = 2 - 1 = 1$ which is true. Is this true for $n = 1$? $2^0 + 2^1 = 1 + 2 = 3$ and $2^{1+1} - 1 = 4 - 1 = 3$ so yes.
Base Case: The statement is true for $n = 0$.
Inductive Case: Let's assume that the statement is true for $n = k$. Then, we assume that $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$ is true such that $1 + 2 + 4 + 8 + ... + 2^k = 2^{k+1} - 1$. If this is true, then we must prove if it holds true for $n = k + 1$ such that $1 + 2 + 4 + 8 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1$. We know that we can substitute everything up to the 2^{k+1} term as $2^{k+1} - 1$ because we assumed it to be true. Thus, we can rewrite our equation as $2^{k+1} - 1 + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{k+2} - 1$ This is equivalent to the right-hand side expression $2^{k+2} - 1$. Therefore, we have proven the basis step and the inductive step that $n = k + 1$ is true to prove that $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$ for all n where $n \in \mathbb{N}$. ■