

## Week 4 Workshop Solutions

### Conceptual Review

- (a) How do we prove a "for all" implication in a formal proof?

E.g.,  $\forall x(Even(x) \rightarrow Odd(x + 1))$ , Domain: integers

#### Solution:

Let  $a$  be an arbitrary integer

1.1.1  $Even(a)$  Assumption

...

1.1.n  $Odd(a + 1)$

1.1  $Even(a) \rightarrow Odd(a + 1)$  Direct proof

1.  $\forall x(Even(x) \rightarrow Odd(x + 1))$  Intro  $\forall$

- (b) How do we prove a "for all" implication in an English proof?

E.g., The sum of any even integer and 1 is odd.

#### Solution:

Let  $a$  be an arbitrary integer.

Suppose  $a$  is even.

...

So [by definition],  $a + 1$  is odd.

Since  $a$  was arbitrary, we have shown that the sum of every even integer and 1 is odd.

- (c) What's a good strategy for writing English proofs?

#### Solution:

- (1) Introduce an arbitrary variable for each  $\forall$  quantifier (if there are any).
- (2) If there is an implication, assume the left-hand side of the statement (assume the premise).
- (3) Unroll any definitions.
- (4) Manipulate towards the goal (using creativity, algebra, etc.).
- (5) Re-roll your definitions to derive the desired outcome.
- (6) Conclude by summarizing your claim.

- (d) What is the definition of "a divides b"?

#### Solution:

For  $a, b \in \mathbb{Z}$  with  $a \neq 0$ :

$a \mid b := \exists k \in \mathbb{Z} (b = ka)$

- (e) What is the Division Theorem?

### Solution:

For  $a, b \in \mathbb{Z}$  with  $b > 0$ , there exist **unique**  $q, r \in \mathbb{Z}$  with  $0 \leq r < b$ , such that  $a = qb + r$ .

(f) What's the definition of "a is congruent to b mod m" ( $a \equiv_m b$ )?

### Solution:

For  $a, b \in \mathbb{Z}$  with  $m > 0$

$$a \equiv_m b := m \mid (a - b)$$

## 1 Formal Proofs: More Quantifiers (from end of last week)

(a) Given  $\forall x(T(x) \rightarrow M(x))$  and  $\exists xT(x)$ , prove that  $\exists xM(x)$ .

### Solution:

1.  $\forall x(T(x) \rightarrow M(x))$  (Given)
2.  $\exists xT(x)$  (Given)
3.  $T(r)^*$  (Elim  $\exists$ ; 2)
4.  $T(r) \rightarrow M(r)^{**}$  (Elim  $\forall$ ; 1)
5.  $M(r)$  (Modus Ponens; 3, 4)
6.  $\exists xM(x)$  (Intro  $\exists$ ; 5)

\*  $r$  is the value that satisfies  $T(x)$

\*\* We can pick any value we want. We intentionally pick the  $r$  from step 3.

(b) Given  $\forall x(P(x) \rightarrow Q(x))$ , prove that  $(\exists xP(x)) \rightarrow (\exists yQ(y))$ .

### Solution:

1.  $\forall x(P(x) \rightarrow Q(x))$  (Given)
  - 2.1.  $\exists xP(x)$  (Assumption)
  - 2.2.  $P(r)^*$  (Elim  $\exists$ ; 2.1)
  - 2.3.  $P(r) \rightarrow Q(r)^{**}$  (Elim  $\forall$ ; 1)
  - 2.4.  $Q(r)$  (Modus Ponens; 2.2, 2.3)
  - 2.5.  $\exists yQ(y)$  (Intro  $\exists$ ; 2.4)
2.  $(\exists xP(x)) \rightarrow (\exists yQ(y))$  (Direct Proof Rule)

\*  $r$  is the value that satisfies  $P(x)$

\*\* We can pick any value we want. We intentionally pick the  $r$  from step 2.2

## 2. English Proof

Let the predicates  $\text{Odd}(x)$  and  $\text{Even}(x)$  be defined as follows where the domain is the integers:

$$\text{Odd}(x) := \exists k (x = 2k + 1)$$

$$\text{Even}(x) := \exists k (x = 2k)$$

Write and **English proof** of the following claim:

$$\forall x \forall y [(\text{Even}(x) \wedge \text{Odd}(y)) \rightarrow \text{Odd}(x + y)]$$

- (a) Translate the claim to English.

**Solution:**

The sum of an even integer and an odd integer is odd.

- (b) Declare any arbitrary variables you may need.

**Solution:**

Let  $x$  and  $y$  be arbitrary integers.

- (c) Assume the left side of the implication.

**Solution:**

Suppose  $x$  is even and  $y$  is odd.

- (d) Unroll the definitions from your assumptions.

**Solution:**

Then by definition of even, there exists some integer  $k$  such that  $x = 2k$ , and by definition of odd, there exists some integer  $j$  such that  $y = 2j + 1$ .

**Note:** A common mistake here is to declare  $k$  and  $j$  as arbitrary. They're not arbitrary – they're the specific integers that satisfy the equations  $x = 2k$  and  $y = 2j + 1$ .

- (e) Manipulate what you have towards your goal.

**Solution:**

Adding  $x$  and  $y$ , we see that:  $x + y = (2k) + (2j + 1) = 2k + 2j + 1 = 2(k + j) + 1$ .

- (f) Reroll definitions into the right side of the implication.

**Solution:**

By definition of odd,  $x + y$  is odd.

- (g) Conclude that you have proved the claim.

**Solution:**

Since  $x$  and  $y$  were arbitrary, we conclude that for all integers  $x$  and  $y$ , if  $x$  is even and  $y$  is odd then  $x + y$  is odd.

- (h) Now take these proof parts and assemble them into one cohesive English proof.

### Solution:

Let  $x$  and  $y$  be arbitrary integers. Suppose  $x$  is even and  $y$  is odd. Then by definition of even, there exists some integer  $k$  such that  $x = 2k$ , and by definition of odd, there exists some integer  $j$  such that  $y = 2j + 1$ . Adding  $x$  and  $y$  we see that:  $x + y = (2k) + (2j + 1) = 2k + 2j + 1 = 2(k + j) + 1$ . By definition of odd,  $x + y$  is odd. Since  $x$  and  $y$  were both arbitrary, we conclude that for all integers  $x$  and  $y$ , if  $x$  is even and  $y$  is odd, then  $x + y$  is odd.

## 3. Divisibility Proof

Consider the following claim where the domain is the integers:

$$\forall n \forall d ((d \mid n) \rightarrow (-d \mid n))$$

- (a) Write a **formal proof** to show that the claim holds.

### Solution:

Let  $a$  and  $b$  be arbitrary integers.

|       |                                                            |                                |
|-------|------------------------------------------------------------|--------------------------------|
| 1.1.1 | $b \mid a$                                                 | (Assumption)                   |
| 1.1.2 | $\exists k (a = kb)$                                       | (Definition of divides: 1.1.1) |
| 1.1.3 | $a = jb$                                                   | (Elim $\exists$ : 1.1.2)       |
| 1.1.4 | $a = (-j)(-b)$                                             | (Algebra: 1.1.3)               |
| 1.1.5 | $\exists k (a = k(-b))$                                    | (Intro $\exists$ : 1.1.4)      |
| 1.1.6 | $-b \mid a$                                                | (Definition of divides: 1.1.5) |
| 1.1   | $(b \mid a) \rightarrow (-b \mid a)$                       | (Direct proof)                 |
| 1.    | $\forall n \forall d ((d \mid n) \rightarrow (-d \mid n))$ | (Intro $\forall$ )             |

- (b) Translate the claim into English.

### Solution:

For integers  $n, d$ , if  $d \mid n$ , then  $-d \mid n$ .

- (c) Write an **English proof** to show that the claim holds.

### Solution:

Let  $d, n$  be arbitrary integers, and suppose  $d \mid n$ . By definition of divides, there exists some integer  $k$  such that  $n = kd = 1 \cdot kd$ . Note that  $-1 \cdot -1 = 1$ . Substituting, we see  $n = (-1)(-1)kd$ . Rearranging, we have  $n = (-k)(-d)$ . Therefore, by definition of divides,  $-d \mid n$ . Since  $d$  and  $n$  were arbitrary, we have shown that for all integers  $d$  and  $n$ , if  $d \mid n$ , then  $-d \mid n$ .

## 4. Modular Computation

- (a) Circle the statements below that are true.

Recall for  $a, b \in \mathbb{Z}$ :  $a \mid b := \exists k \in \mathbb{Z} (b = ka)$ .

- (a)  $1 \mid 3$
- (b)  $3 \mid 1$
- (c)  $2 \mid 2018$
- (d)  $-2 \mid 12$
- (e)  $1 \cdot 2 \cdot 3 \cdot 4 \mid 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

### Solution:

- (a)  $1|3$  True:  $3 = 1 \cdot 3$
- (b)  $3|1$  False
- (c)  $2|2018$  True:  $2018 = 2 \cdot 1009$
- (d)  $-2|12$  True:  $12 = -2 \cdot -6$
- (e)  $1 \cdot 2 \cdot 3 \cdot 4|1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$  True:  $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5 \cdot (1 \cdot 2 \cdot 3 \cdot 4)$

(b) Circle the statements below that are true.

Recall for  $a, b, m \in \mathbb{Z}$  and  $m > 0$ :  $a \equiv_m b := m|(a - b)$ .

- (a)  $-3 \equiv_3 3$
- (b)  $0 \equiv_9 9000$
- (c)  $44 \equiv_7 13$
- (d)  $-58 \equiv_5 707$
- (e)  $58 \equiv_5 707$

### Solution:

- (a)  $-3 \equiv_3 3$  True:  $-3 - 3 = -6$ ,  $3|-6$
- (b)  $0 \equiv_9 9000$  True:  $0 - 9000 = -9000$ ,  $9|-9000$
- (c)  $44 \equiv_7 13$  False:  $44 - 13 = 31$   $31 = 7 \cdot 4 + 3 \therefore 7 \nmid 31$
- (d)  $-58 \equiv_5 707$  True:  $-58 - 707 = -765$   $5|-765$
- (e)  $58 \equiv_5 707$  False:  $58 - 707 = -649$   $5 \nmid -649$

## 5. Modular Multiplication

Write an **English proof** of the following claim: For all integers  $a, b, c, d, m$  with  $m > 0$ , if  $a \equiv_m b$  and  $c \equiv_m d$ , then  $ac \equiv_m bd$ .

### Solution:

Let  $m > 0$ ,  $a, b, c, d$  be arbitrary integers. Suppose that  $a \equiv_m b$  and  $c \equiv_m d$ . Then by definition of congruence,  $m|(a - b)$  and  $m|(c - d)$ . Then by definition of divides, there exists some integer  $k$  such that  $a - b = km$ , and there exists some integer  $j$  such that  $c - d = jm$ . Then  $a = b + km$  and  $c = d + jm$ . Multiplying gives us:

$$ac = (b + km)(d + jm) = bd + kmd + bjm + kjm^2 = bd + m(kd + bj + kjm)$$

Subtracting  $bd$  from both sides we get,  $ac - bd = m(kd + bj + kjm)$ . By definition of divides,  $m|ac - bd$ . Then by definition of congruence,  $ac \equiv_m bd$ . Since  $m > 0$ ,  $a, b, c, d$  were arbitrary integers, the claim holds for all integers  $a, b, c, d$  and positive integers  $m$ .

## 6. Mod Practice

Write an **English proof** of the following claim: For all integers  $n$ , if  $n$  is not divisible by 3, then  $n^2 \equiv_3 1$ . You may use, without proof, that for any integers  $a, m$  with  $m > 0$ ,  $m|a$  iff  $a \equiv_m 0$ .

### Solution:

Let  $n$  be an arbitrary integer.

Suppose that  $n$  is not divisible by 3.

Since  $3 \mid n$  iff  $n \equiv_3 0$  and  $3 \nmid n$ , we know that  $n \not\equiv_3 0$ . The only options remaining are  $n \equiv_3 1$  or  $n \equiv_3 2$ . We continue by cases.

**Case 1:** Suppose  $n \equiv_3 1$

By definition of congruence and divides,  $3 \mid (n - 1)$  so  $n - 1 = 3k$  for some integer  $k$ . Rearranging, we get  $n = 3k + 1$ . So,  $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$ . Subtracting 1 from both sides we get,  $n^2 - 1 = 3(3k^2 + 2k)$ . By definition of divides,  $3 \mid (n^2 - 1)$ . By definition of congruence,  $n^2 \equiv_3 1$

**Case 2:** Suppose that  $n \equiv_3 2$

By definition of congruence and divides,  $3 \mid (n - 2)$  so  $n - 2 = 3j$  for some integer  $j$ . Rearranging, we get  $n = 3j + 2$ . So,  $n^2 = (3j + 2)^2 = 9j^2 + 12j + 4 = 9j^2 + 12j + 3 + 1 = 3(3j^2 + 4j + 1) + 1$ . Subtracting 1 from both sides we get,  $n^2 - 1 = 3(3j^2 + 4j + 1)$ . By definition of divides,  $3 \mid (n^2 - 1)$ . By definition of congruence,  $n^2 \equiv_3 1$ .

Since these cases are exhaustive, we have shown that,  $n^2 \equiv_3 1$  holds in general. Since  $n$  was arbitrary, we have shown that for all integers  $n$ , if  $n$  is not divisible by 3, then  $n^2 \equiv_3 1$ .

## 7. An Odd Proof

Write and **English proof** of the following claim: If  $n, m$  are odd integers, then  $2n + m$  is odd.

**Solution:**

Let  $n, m$  be arbitrary odd integers. By definition of odd,  $n = 2k + 1$  for some integer  $k$  and  $m = 2j + 1$  for some integer  $j$ . Then

$$2n + m = 2(2k + 1) + 2j + 1 = 4k + 2 + 2j + 1 = 2(2k + j + 1) + 1$$

By definition,  $2n + m$  is odd. Since  $n$  and  $m$  were arbitrary, we have shown that for all integers  $n, m$ , if  $n$  and  $m$  are odd then  $2n + 1$  is odd.

## 8. A Rational Contradiction

Recall that a real number  $x$  is **rational** iff there exist integers  $p$  and  $q$ , with  $q \neq 0$ , such that  $x = \frac{p}{q}$ . Formally, for  $x \in \mathbb{R}$ ,  $\text{Rational}(x) := \exists p \exists q \in \mathbb{Z} (q \neq 0 \wedge x = \frac{p}{q})$ .

Write an **English proof** of the following statement:

For all real numbers  $a, b$ , if  $a$  is rational and  $ab$  is irrational, then  $b$  is irrational.

(a) Introduce any arbitrary variables you may need.

**Solution:**

Let  $a$  and  $b$  be arbitrary real numbers.

(b) Assume the premise of the implication.

**Solution:**

Suppose  $a$  is rational and  $ab$  is irrational.

(c) Unroll the definitions from your assumptions if necessary (use your judgment).

**Solution:**

By definition of rational,  $a = s/t$  for some integers  $s, t$ , where  $t \neq 0$ .

- (d) We're going to use Reductio Ad Absurdum to prove that  $b$  is irrational (not rational). Write down the assumption we must make in order to do that.

**Solution:**

Suppose that  $b$  is rational.

- (e) Finish the rest of the proof.

**Solution:**

By definition of rational,  $b = c/d$  for integers  $c, d$  with  $d \neq 0$ . Multiplying  $a$  and  $b$ , we get  $ab = (sc)/(td)$ . Since  $s, c, t, d$  are all integers,  $sc$  and  $td$  are both integers. Since  $t, d \neq 0$ ,  $td \neq 0$ . By definition, then,  $ab$  is rational, contradicting our earlier statement that  $ab$  is irrational (Note: In a formal proof, we would cite Principium Contradictionis here). Therefore,  $b$  must be irrational (Note: In a formal proof, we would cite Reductio Ad Absurdum here). Since  $a, b$  were arbitrary, we have proven the claim.