CSE 390Z: Mathematics for Computation Workshop

Week 4 Workshop Solutions

Conceptual Review

(a) **Definitions**
a divides b: $\quad a \mid b \quad \leftrightarrow \quad \exists k \in \mathbb{Z}\ (b = ka)$
a is congruent to b modulo m: $\quad a \equiv b \pmod{m} \quad \leftrightarrow \quad m \mid (a - b)$

(b) What's the Division Theorem?

Solution:

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

(c) Circle the statements below that are true.
Recall for $a, b \in \mathbb{Z}$: $a|b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$.

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

Solution:

a, c, d, and e are true.

(d) Circle the statements below that are true.
Recall for $a, b, m \in \mathbb{Z}$ and $m > 0$: $a \equiv b \pmod{m}$ iff $m|(a - b)$.

(a) $-3 \equiv 3 \pmod{3}$
(b) $0 \equiv 9000 \pmod{9}$
(c) $44 \equiv 13 \pmod{7}$
(d) $-58 \equiv 707 \pmod{5}$
(e) $58 \equiv 707 \pmod{5}$

Solution:

a, b, and d are true.

1. A Rational Conclusion

Note: This problem will walk you through the steps of an English proof. If you feel comfortable writing the proof already, feel free to jump directly to part (h).

Let the predicate Rational(x) be defined as $\exists a \exists b(\text{Integer}(a) \wedge \text{Integer}(b) \wedge b \neq 0 \wedge x = \frac{a}{b})$. Prove the following claim:

$$\forall x \forall y(\text{Rational}(x) \wedge \text{Rational}(y) \wedge (y \neq 0) \rightarrow \text{Rational}(\frac{x}{y}))$$

(a) Translate the claim to English.

Solution:

If x is rational and $y \neq 0$ is rational, then $\frac{x}{y}$ is rational.

(b) Declare any arbitrary variables you need to use.

Solution:

Let x and y be arbitrary.

(c) State the assumptions you're making. **Hint:** assume everything on the left side of the implication.

Solution:

Suppose x and y are rational numbers and that $y \neq 0$.

(d) Unroll the predicate definitions from your assumptions.

Solution:

Since x and y are rational numbers, by definition there are integers a, b, n, m with $b, m \neq 0$ such that $x = \frac{a}{b}$ and $y = \frac{n}{m}$.

(e) Manipulate what you have towards your goal.

Solution:

Then $\frac{x}{y} = \frac{a/b}{n/m} = \frac{a \cdot m}{b \cdot n}$. Let $p = a \cdot m$ and $q = bn$. Note that since $y \neq 0$, n cannot be 0, and since $b \neq 0$ then $q \neq 0$. Because a, b, m, n are integers, $a \cdot m$ and $b \cdot n$ are integers.

(f) Reroll into your predicate definitions.

Solution:

Since $\frac{x}{y} = \frac{p}{q}$, p, q are integers, and $q \neq 0$, $\frac{x}{y}$ is rational.

(g) State your final claim.

Solution:

Because x and y were arbitrary, for any rational numbers x and y with $y \neq 0$, $\frac{x}{y}$ is rational.

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

Solution:

Let x and y be arbitrary rational numbers with $y \neq 0$. Since x and y are rational numbers, by definition there are integers a, b, n, m with $b, m \neq 0$ such that $x = \frac{a}{b}$ and $y = \frac{n}{m}$. Then $\frac{x}{y} = \frac{a/b}{n/m} = \frac{a \cdot m}{b \cdot n}$. Let $p = a \cdot m$ and $q = bn$. Note that since $y \neq 0$, n cannot be 0, and since $b \neq 0$ then $q \neq 0$. Because a, b, n, m are integers, $a \cdot m$ and $b \cdot n$ are integers. Since $\frac{x}{y} = \frac{p}{q}$, p, q are integers, and $q \neq 0$, $\frac{x}{y}$ is rational. Because x and y were arbitrary, for any rational numbers x and y with $y \neq 0$ $\frac{x}{y}$ is rational.

2. Don't be Irrational!

Recall that the predicate Rational(x) is defined as $\exists a \exists b(\text{Integer}(a) \wedge \text{Integer}(b) \wedge b \neq 0 \wedge x = \frac{a}{b})$.
One of the following statements is true, and one is false:

- If xy and x are both rational, then y is also rational.
- If $x - y$ and x are both rational, then y is also rational.

Decide which statement is true and which statement is false. Prove the true statement, and disprove the false statement. For the disproof, it will be helpful to use proof by counterexample.

Solution:

Claim: If xy and x are both rational, then y is also rational.
We wish to disprove this through counterexample. Let x be 0, which is rational. $x * y$ will be 0 regardless of y, so for an irrational y like $y = \pi$, x and xy are rational, while y is not.

Claim: If $x - y$ and x are both rational, then y is also rational.
Let x, y be arbitrary integers. Suppose x and $x - y$ are rational. By the definition of rational numbers, if x and $x - y$ are rational, then there are $a, b, n, m \in \mathbb{Z}$ with $b, m \neq 0$ such that $x = \frac{a}{b}$ and $x - y = \frac{n}{m}$. Then:

$x - y = \frac{n}{m}$	Given
$y = x - \frac{n}{m}$	Algebra
$y = \frac{a}{b} - \frac{n}{m}$	Substituting $x = \frac{a}{b}$

Now we can rearrange this expression for y:

$$\begin{aligned} y &= \frac{a}{b} - \frac{n}{m} \\ &= \frac{a}{b} * \frac{m}{m} - \frac{n}{m} * \frac{b}{b} \\ &= \frac{am}{bm} - \frac{nb}{bm} \\ &= \frac{am - bn}{bm} \end{aligned}$$

Since integers are closed on multiplication and subtraction, $am, bn, bm \in \mathbb{Z}$, and therefore $am - bn \in \mathbb{Z}$. Since $b, m \neq 0$, $bm \neq 0$ also, and therefore for $p = am - bn$ and $q = bm$, $y = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ with $q \neq 0$. By the definition of rational, y is rational.

3. Modular Addition

Let m be a positive integer. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Solution:

Let $m > 0$, a, b, c, d be arbitrary integers. Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by definition of mod, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integer k such that

$a - b = mk$, and there exists some integer j such that $c - d = mj$. Then $(a - b) + (c - d) = mk + mj$. Rearranging, $(a+c)-(b+d) = m(k+j)$. Then by definition of divides, $m \,|(a+c)-(b+d)$. Then by definition of congruence, $a + c \equiv b + d \pmod{m}$.

4. Modular Multiplication

Write an English proof to prove that for an integer $m > 0$ and any integers a, b, c, d, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Solution:

Let $m > 0$, a, b, c, d be arbitrary integers. Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by definition of mod, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integer k such that $a - b = mk$, and there exists some integer j such that $c - d = mj$. Then $a = b + mk$ and $c = d + mj$. So, multiplying, $ac = (b + mk)(d + mj) = bd + mkd + mjb + m^2jk = bd + m(kd + jb + mjk)$. Subtracting bd from both sides, $ac - bd = m(kd + jb + mjk)$. By definition of divides, $m \mid ac - bd$. Then by definition of congruence, $ac \equiv bd \pmod{m}$.

5. Divisibility Proof

Let the domain of discourse be integers. Consider the following claim:

$$\forall n \forall d \, ((d \mid n) \to (-d \mid n))$$

(a) Translate the claim into English.

Solution:

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

(b) Write an English proof that the claim holds.

Solution:

Let d, n be arbitrary integers, and suppose $d|n$. By definition of divides, there exists some integer k such that $n = dk = 1 \cdot dk$. Note that $-1 \cdot -1 = 1$. Substituting, we see $n = (-1)(-1)dk$. Rearranging, we have $n = (-d)(-1 \cdot k)$. Since k is an integer, $-1 \cdot k$ is an integer because the integers are closed under multiplication. So, by definition of divides, $-d|n$. Since d and n were arbitrary, it follows that for any integers d and n, if $d|n$, then $-d|n$.

6. Another Divisibility Proof

Write an English proof to prove that if k is an odd integer, then $4 \,|\, k^2 - 1$.

Solution:

Let k be an arbitrary odd integer. Then by definition of odd, $k = 2j + 1$ for some integer j. Then $k^2 - 1 = (2j + 1)^2 - 1 = 4j^2 + 4j + 1 - 1 = 4j^2 + 4j = 4(j^2 + j)$. Then by definition of divides, $4 \mid k^2 - 1$.

7. Proofs by Contrapositive

For each part, write a proof by contrapositive of the statement.

(a) If $a^2 \not\equiv b^2 \pmod{n}$, then $a \not\equiv b \pmod{n}$.

Solution:

We argue by contrapositive. Let a, b be arbitrary integers and let n be an arbitrary positive integer. Suppose $a \equiv b \pmod{n}$. Then, by definition of equivalence mod n, $n|(a-b)$ and by definition of divides, there exists some integer k such that $a - b = nk$. Multiplying both sides of the equation by $a+b$, we get $(a-b)(a+b) = a^2 - b^2 = nk(a+b)$. Since integers are closed under addition and multiplication, $k(a+b)$ must be an integer. Therefore, $n|a^2 - b^2$ by definition of divides and $a^2 \equiv b^2 \pmod{n}$ by definition of equivalence mod n. Since a, b, n were arbitrary, we have shown that the contrapositive holds for all integers a, b, n. Therefore, the original claim holds.

(b) For all integers a, b, if $3 \nmid ab$, then $3 \nmid a$ and $3 \nmid b$.

Solution:

We argue by contrapositive. Let a, b be arbitrary integers. Suppose $3 \mid a$ or $3 \mid b$. Thus, there are two cases to consider:

Case 1:

Suppose $3 \mid a$. Then, by definition of divides, there exists some integer k such that $a = 3k$. Multiplying both sides by b, we get $ab = 3kb$. Since integers are closed under multiplication, kb is an integer. Then, by definition of divides, $3 \mid ab$.

Case 2:

Suppose $3 \mid b$. Then, by definition of divides, there exists some integer j such that $b = 3j$. Multiplying both sides by a, we get $ab = 3ja$. Since integers are closed under multiplication, ja is an integer. Then, by definition of divides, $3 \mid ab$.

In both cases, $3 \mid ab$. So, if $3 \mid a$ or $3 \mid b$, then $3 \mid ab$. Since a and b were arbitrary, this proves the contrapositive holds for all a, b. Therefore, the original claim holds.

8. Proof by...how many cases?

Prove that for all integers n, $2n^2 + n + 1$ is not divisible by 3.

Hint: *You will probably want to use proof by cases for this problem. To decide which cases to use, consider the possible outcomes when dividing n by 3.*

Solution:

Let n be an arbitrary integer. When n is divided by 3, there are three possible remainders. These form the following cases.

Case 1: When n is divided by 3, the remainder is 0.

Then, $n = 3q + 0$ for some integer q.

$$\begin{aligned} 2n^2 + n + 1 &= 2(3q)^2 + (3q) + 1 \\ &= 2(9q^2) + 3q + 1 \\ &= 18q^2 + 3q + 1 \\ &= 3(6q^2 + q) + 1 \end{aligned}$$

Since q is an integer, $6q^2 + q$ is also an integer. This means when $2n^2 + n + 1$ is divided by 3, the remainder is 1, so it is not divisible by 3.

Case 2: When n is divided by 3, the remainder is 1.

Then, $n = 3q + 1$ for some integer q.

$$2n^2 + n + 1 = 2(3q + 1)^2 + (3q + 1) + 1$$

$$
\begin{aligned}
&= 2(9q^2 + 6q + 1) + (3q + 1) + 1 \\
&= 18q^2 + 12q + 2 + 3q + 1 + 1 \\
&= 18q^2 + 15q + 4 \\
&= 3(6q^2 + 5q + 1) + 1
\end{aligned}
$$

Since q is an integer, $6q^2+5q+1$ is also an integer. This means when $2n^2+n+1$ is divided by 3, the remainder is 1, so it is not divisible by 3.

Case 3: When n is divided by 3, the remainder is 2. Then, $n = 3q + 2$ for some integer q.

$$
\begin{aligned}
2n^2 + n + 1 &= 2(3q + 2)^2 + (3q + 2) + 1 \\
&= 2(9q^2 + 12q + 4) + (3q + 2) + 1 \\
&= 18q^2 + 24q + 8 + 3q + 2 + 1 \\
&= 18q^2 + 27q + 11 \\
&= 3(6q^2 + 9q + 3) + 2
\end{aligned}
$$

Since q is an integer, $6q^2+9q+3$ is also an integer. This means when $2n^2+n+1$ is divided by 3, the remainder is 2, so it is not divisible by 3.

So, in all cases, $2n^2 + n + 1$ is not divisible by 3. Since n was arbitrary, this proves the claim for all integers.