CSE 390z: Mathematics for Computation Workshop

Week 5 Workshop Solutions

0. 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: $\quad a \equiv_m b \quad \leftrightarrow \quad m \mid (a - b)$

(b) How do you know if a multiplicative inverse does not exist?
A multiplicative inverse does not exist when $gcd(a, b) \neq 1$.

(c) Bezout's theorem: If a and b are positive integers, then there exist integers s and t such that gcd(a, b) is equal to what?

$$\text{gcd}(a, b) = sa + tb$$

(d) What is Euclid's algorithm? What does it help us calculate?
Euclid's algorithm helps us find gcd(a, b).The algorithm is as follows:

- Repeatedly use gcd$(a, b) =$ gcd$(b, a\%b)$
- When you reach gcd$(g, 0)$, return g.

1. 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. 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.

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

Solution:

Let a, b be an arbitrary integers. We argue by contrapositive. 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, if $3 \mid a$ or $3 \mid b$, then $3 \mid ab$. Thus, the contrapositive is also true. Since a, b were arbitrary, this proves that the statement is true for all integers a, b.

2. Proofs by Contradiction

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

(a) If a is rational and ab is irrational, then b is irrational.

Solution:

Suppose for the sake of contradiction that this statement is false, meaning there exists an a, b where a is rational and ab is irrational, and b is not irrational. Then, b is rational. By definition of rational, $a = \frac{s}{t}$ and $b = \frac{x}{y}$ for some integers s, t, x, y where $t \neq 0$ and $y \neq 0$. Multiplying these together, we get $ab = \frac{sx}{ty}$. Since integers are closed under multiplication, sx, ty are integers. And since the product of two non zero integers cannot be zero, $ty \neq 0$. Thus, ab is rational. This is a contradiction since we stated that ab was irrational. Therefore, the original statement must be true.

(b) For all integers n, $4 \nmid n^2 - 3$.

Solution:

Suppose for the sake of contradiction there exists an integer n such that $4 \mid (n^2 - 3)$. Then, by definition of divides, there exists an integer k such that $n^2 - 3 = 4k$. We will consider two cases:

Case 1: n is even

By definition of even, there is some integer a where $n = 2a$. Substituting n into the equation above, we get $(2a)^2 - 3 = 4a^2 - 3 = 4k$. By algebra,

$$k = \frac{4a^2 - 3}{4} = a^2 - \frac{3}{4}$$

Since integers are closed under multiplication, a^2 must be an integer. Since $\frac{3}{4}$ is not an integer, k must not be an integer. This is a contradiction, since k was introduced as an integer.

Case 2: n is odd

By definition of odd, there is some integer b where $n = 2b + 1$, Substituting n into the equation above, we get $(2b + 1)^2 - 3 = 4b^2 + 4b + 1 - 3 = 4k$. By algebra,

$$k = \frac{4b^2 + 4b - 2}{4} = b^2 + b - \frac{1}{2}$$

Since integers are closed under multiplication and addition, $b^2 + b$ must be an integer. Since $\frac{1}{2}$ is not an integer, k is not an integer. This is a contradiction, since k was introduced as an integer.

As shown, all cases led to a contradiction, so the original statement must be true.

3. 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.

Proof. 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:

$$\begin{aligned} x - y &= \frac{n}{m} && \text{Given} \\ y &= x - \frac{n}{m} && \text{Algebra} \\ y &= \frac{a}{b} - \frac{n}{m} && \text{Substituting } x = \frac{a}{b} \end{aligned}$$

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. □

4. More Number Theory Practice

For each of the following parts, prove or disprove the claim.

(a) If $a \mid b$ and $c \mid (-a)$, then $(-c) \mid b$.

Solution:

Suppose $a \mid b$ and $c \mid (-a)$. By definition of divides, $b = ka$ and $-a = cj$ for some integers k, j. By algebra, $a = -cj$. Substituting a into the first equation, we get $b = k(-cj) = (-kj)(-c)$. Then, by definition of divides, $(-c) \mid b$ and the claim holds.

(b) For all $a, b, n, x \in \mathbb{Z}$, $a \equiv_n b$ implies $x^a \equiv_n x^b$.

Solution:

We can disprove this through counterexample. Let $a = 2, b = 5, n = 3, x = 2$. Since $2 \equiv_3 5$, $a \equiv_n b$. But $2^2 \not\equiv_3 2^5$ because $2^2 \pmod 3 = 4 \pmod 3 = 1$ and $2^5 \pmod 3 = 32 \pmod 3 = 2$, and $1 \neq 2$. Therefore, the implication is false.

(c) For all integers n, if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

Solution:

Let n be an arbitrary integer and suppose that n is not divisible by 3. Then, there are two cases:
Case 1: $n \equiv 1 \pmod 3$
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, $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Then, $n^2 - 1 = 3(3k^2 + 2k)$. Since $3k^2 + 2k$ is an integer, $3 \mid (n^2 - 1)$ by definition of divides. By definition of congruence, $n^2 \equiv 1 \pmod 3$

Case 2: $n \equiv 2 \pmod 3$
By definition of congruence and divides, $3|(n-2)$ so $n - 2 = 3j$ for some integer j. Rearranging, we get $n = 3j + 2$. So, $n^2 = 9j^2 + 12j + 4 = 3(3j^2 + 4j + 1) + 1$. Then, $n^2 - 1 = 3(3j^2 + 4j + 1)$. Since $3j^2+4j+1$ is an integer, $3 \mid (n^2-1)$ by definition of divides. By definition of congruence, $n^2 \equiv 1 \pmod 3$.
So, in all cases, $n^2 \equiv 1 \pmod 3$. Since n was arbitrary, the claim holds for all integers n.

5. Modular Arithmetic

Prove that for any odd integer a there is an integer b that satisfies $ab \equiv 2 \pmod 8$.

Solution:

Let a be an arbitrary odd integer. Since a is not even, a does not divide 8. Since 8 is only divisible by $1, 2, 4$, and 8, we have $\gcd(a, 8) = 1$. By Bezout's Theorem, we know $\gcd(a, 8) = 1 = ax + 8y$ for some integers x, y. By algebra, $8y = 1 - ax$. Multiplying both sides by 2, we get $8(2y) = 2 - a(2x)$. Since integers are closed under multiplication, $2y$ and $2x$ are integers. By definition of divides, $8|(2 - a(2x))$ and by definition of equivalence, $a(2x) \equiv 2 \pmod 8$. So, there is an integer $b = 2x$ that satisfies $ab \equiv 2 \pmod 8$. Since a was an arbitrary odd integer, there is an integer b that satisfies $ab \equiv 2 \pmod 8$ for any odd integer a.

6. Extended Euclidean Algorithm

Find all solutions in the range of $0 \leq x < 2021$ to the modular equation:

$$311x \equiv 3 \pmod{2021}$$

Solution:

$$\begin{aligned}\gcd(2021, 311) &= \gcd(311, 2021 \bmod 311) = \gcd(311, 155) \\ &= \gcd(155, 311 \bmod 155) = \gcd(155, 1) \\ &= 1\end{aligned}$$

Then we know that there is a multiplicative inverse:

$$\begin{aligned}2021 &= 311 * 6 + 155 \\ 311 &= 155 * 2 + 1 \\ 155 &= 1 * 155\end{aligned}$$

From here, we can rearrange the equations to get:

$$\begin{aligned}155 &= 2021 - 311 * 6 \\ 1 &= 311 - 155 * 2\end{aligned}$$

From here, we use back substitution and plug these back into our equations:

$$\begin{aligned}1 &= 311 - 155 * 2 \\ 1 &= 311 - 2 * (2021 - 311 * 6) \\ 1 &= 311 - 2 * 2021 + 12 * 311 \\ 1 &= 13 * 311 - 2 * 2021\end{aligned}$$

So the multiplicative inverse is 13, i.e. $311 * 13 \equiv_{2021} 1$, so $311 * 13 * 3 \equiv_{2021} 3$. Then $x = 13 * 3 + 2021k = 39 + 2021k$ for $k \in \mathbb{N}$, but since we're only asked for solutions in the range of $0 \leq x < 2021$, $x = 39$.

7. 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.

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

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.