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. Modular Multiplication

Write an English proof to prove that for an integer $m > 0$ and any integers a, b, c, d, 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. Assume that $a \equiv_m b$ and $c \equiv_m d$. 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, $ac \equiv_m bd$.

2. Proofs by Contrapositive

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

(a) If $a^2 \not\equiv_n b^2$, then $a \not\equiv_n b$.

Solution:

We argue by contrapositive. Suppose $a \equiv_n b$. 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 $a^2 \equiv_n b^2$ by definition of equivalence mod n. Thus, the original statement also holds by contrapositive.

(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.

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 $n^2 \equiv_3 1$.

Solution:

Let n be an arbitrary integer and suppose that n is not divisible by 3. Then, there are two cases:
Case 1: $n \equiv_3 1$
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, $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. 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, $n^2 \equiv_3 1$

Case 2: $n \equiv_3 2$
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, $n^2 \equiv_3 1$.
So, in all cases, $n^2 \equiv_3 1$. 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 $ab \equiv_8 2$.
Hint: You need to reason about the gcd(a,8) and use Bezout's theorem.

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, $a(2x) \equiv_8 2$. So, there is an integer $b = 2x$ that satisfies $ab \equiv_8 2$. Since a was an arbitrary odd integer, there is an integer b that satisfies $ab \equiv_8 2$ for any odd integer a.

6. Extended Euclidean Algorithm

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

$$311x \equiv_{2021} 3$$

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. $311 * 13 \equiv_{2021} 1$. We can then multiply both sides of the original modular equation by 13 to get $13 * 311x \equiv_{2021} 13 * 3$. Simplifying gives us $x \equiv_{2021} 39$. By the definition of congruence and division we have $x = 39 + 2021k$ for $k \in \mathbb{N}$, but since we're only asked for solutions in the range of $0 \leq x < 2021$, $x = 39$.

7. Weak Induction Warmup

Prove by induction on n that for all integers $n \geq 4$, the inequality $n! > 2^n$ is true.

Complete the induction proof below.

Solution:

Let $P(n)$ be "$n! > 2^n$". We will prove $P(n)$ is true for all $n \in \mathbb{N}$, $n \geq 4$, by induction.

Base Case: (n = 4)**:** $4! = 24$ and $2^4 = 16$, since $24 > 16$, $P(4)$ is true.

Inductive Hypothesis: Suppose that $P(k)$ is true for some arbitrary integer $k \in \mathbb{N}$, $k \geq 4$.

Inductive Step:

Goal: Show $P(k+1)$, i.e. show $(k+1)! > 2^{k+1}$

$$\begin{aligned}
(k+1)! &= k! \cdot (k+1) \\
&> 2^k \cdot (k+1) && \text{(By I.H., } k! > 2^k\text{)} \\
&> 2^k \cdot 2 && \text{(Since } k \geq 4\text{, so } k+1 \geq 5 > 2\text{)} \\
&= 2^{k+1}
\end{aligned}$$

Conclusion: So by induction, $P(n)$ is true for all $n \in \mathbb{N}$, $n \geq 4$.

8. Induction with Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all $n > 1$ by induction.

Solution:

Let $P(n)$ be "$9 \mid n^3 + (n+1)^3 + (n+2)^3$". We will prove $P(n)$ for all integers $n > 1$ by induction.

Base Case $(n = 2)$**:** $2^3 + (2+1)^3 + (2+2)^3 = 8 + 27 + 64 = 99 = 9 \cdot 11$, so $9 \mid 2^3 + (2+1)^3 + (2+2)^3$, so $P(2)$ holds.

Inductive Hypothesis: Assume that $9 \mid k^3 + (k+1)^3 + (k+2)^3$ for an arbitrary integer $k > 1$. Note that this is equivalent to assuming that $k^3 + (k+1)^3 + (k+2)^3 = 9j$ for some integer j by the definition of divides.

Inductive Step: Goal: Show $9 \mid (k+1)^3 + (k+2)^3 + (k+3)^3$

$$\begin{aligned}
(k+1)^3 + (k+2)^3 + (k+3)^3 &= (k^2+6k+9)(k+3) + (k+1)^3 + (k+2)^3 && \text{[expanding trinomial]} \\
&= (k^3+6k^2+9k+3k^2+18k+27) + (k+1)^3 + (k+2)^3 && \text{[expanding binomial]} \\
&= 9k^2+27k+27+k^3+(k+1)^3+(k+2)^3 && \text{[adding like terms]} \\
&= 9k^2+27k+27+9j && \text{[by I.H.]} \\
&= 9(k^2+3k+3+j) && \text{[factoring out 9]}
\end{aligned}$$

Since k and j are integers, $k^2+3k+3+j$ is also an integer. Therefore, by the definition of divides, $9 \mid (k+1)^3 + (k+2)^3 + (k+3)^3$, so $P(k) \to P(k+1)$ for an arbitrary integer $k > 1$.

Conclusion: $P(n)$ holds for all integers $n > 1$ by induction.