CSE 390z: Mathematics for Computation Workshop

Week 5 Workshop Solutions

0. Conceptual Review

(a) What are the different proof strategies we've learned?

Solution:

- Direct proof
- Proof by contrapositive
- Proof of biconditional
- Proof by counterexample
- Proof by cases
- Proof by contradiction

(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.

(e) What are the five steps that must be included in an induction proof?

(a) "Let P(n) be... . We show that P(n) is true for $n \geq 0$ by induction"
(b) Base Case: Prove P(0).
(c) Inductive Hypothesis: Suppose P(k) is true for an arbitrary integer $k \geq 0$.
(d) Inductive Step: Show P(k+1).
(e) Conclusion: We have shown P(k+1), so the result follows by induction.

This template is very important to follow for induction proofs! It is also important to pay attention to the bounds for your variables, as you may not always be asked to prove something starting with P(0).

(f) **In what step of an induction proof do you apply your inductive hypothesis? Do you always need to use the inductive hypothesis?** You apply your inductive hypothesis during the inductive step. You must always use your inductive hypothesis at some point in your inductive step and clearly label it as "I. H.".

Number Theory

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:

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, Thus, if $3 \mid a$ or $3 \mid b$, then $3 \mid ab$.

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 $\exists a \exists b(\text{Integer}(a) \land \text{Integer}(b) \land b \neq 0 \land x = \frac{a}{b})$.

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. $\square$

4. 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.

5. Extended Euclidean Algorithm

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

$$311x \equiv 3 \text{ (mod 2021)}$$

Solution:

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

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 $0 \leq x < 2021$, $x = 39$.

6. Inductively Divisible

Prove that for all $n \in \mathbb{N}$, $8^n - 3^n$ is divisible by 5 (i.e. $5|8^n - 3^n$) by induction on n.

Solution:

1. Let P(n) be $5|8^n - 3^n$. We will show that P(n) is true for $n \in \mathbb{N}$ by induction.
2. **Base Case:** $(n = 0)$
   $8^0 - 3^0 = 1 - 1 = 0 = 0 * 5$, so $5|8^0 - 3^0$ and $\therefore$ P(0) is true.
3. **Inductive Hypothesis:** Suppose P(k) is true for an arbitrary $k \in \mathbb{N}$.
4. **Inductive Step:**

   $$\boxed{\textbf{Goal: } \text{Show } P(k+1), \text{ i.e. show } 5|8^{k+1} - 3^{k+1}}$$

   $$\begin{aligned} 8^{k+1} - 3^{k+1} &= 8 \cdot 8^k - 3 \cdot 3^k && \text{(Factor exponentials)} \\ &= 5 \cdot 8^k + 3 \cdot 8^k - 3 \cdot 3^k && \text{(split 8 into 5 + 3)} \\ &= 5 \cdot 8^k + 3 \cdot (8^k - 3^k) && \text{(factor out 3)} \end{aligned}$$

   By the I.H., $5|8^k - 3^k$, which means there is an integer q such that $5q = 8^k - 3^k$, so:

   $$\begin{aligned} 8^{k+1} - 3^{k+1} &= 5 \cdot 8^k + 3 \cdot 5q && \text{(by I.H.)} \\ &= 5 \cdot (8^k + 3q) && \text{(factor out 5)} \end{aligned}$$

   Since $5|5 \cdot (8^k + 3q)$, $5|8^{k+1} - 3^{k+1}$, so P$(k+1)$ is true.
5. Thus, we have shown P(n) is true for all $n \in \mathbb{N}$ by induction.

7. Prove the inequality

Prove by induction on n that for all $n \in \mathbb{N}$ the inequality $(3 + \pi)^n \geq 3^n + n\pi 3^{n-1}$ is true.

Solution:

1. Let $P(n)$ be "$(3 + \pi)^n \geq 3^n + n\pi 3^{n-1}$". We will prove $P(n)$ is true for all $n \in \mathbb{N}$, by induction.
2. **Base case (n = 0):** $(3 + \pi)^0 = 1$ and $3^0 + 0 \cdot \pi \cdot 3^{-1} = 1$, since $1 \geq 1$, $P(0)$ is true.
3. **Inductive Hypothesis:** Suppose that $P(k)$ is true for some arbitrary integer $k \in \mathbb{N}$.
4. **Inductive Step:**

   $$\boxed{\text{Goal: Show } P(k+1), \text{ i.e. show } (3+\pi)^{k+1} \geq 3^{k+1} + (k+1)\pi 3^{(k+1)-1} = 3^{k+1} + (k+1)\pi 3^k}$$

   $$\begin{aligned} (3 + \pi)^{k+1} &= (3 + \pi)^k \cdot (3 + \pi) && \text{(Factor out } (3+\pi)\text{)} \\ &\geq (3^k + k3^{k-1}\pi) \cdot (3 + \pi) && \text{(By I.H., } (3+\pi) \geq 0\text{)} \\ &= 3 \cdot 3^k + 3^k\pi + 3k3^{k-1}\pi + k3^{k-1}\pi^2 && \text{(Distributive property)} \\ &= 3^{k+1} + 3^k\pi + k3^k\pi + k3^{k-1}\pi^2 && \text{(Simplify)} \\ &= 3^{k+1} + (k+1)3^k\pi + k3^{k-1}\pi^2 && \text{(Factor out } (k+1)\text{)} \\ &\geq 3^{k+1} + (k+1)\pi 3^k && (k3^{k-1}\pi^2 \geq 0) \end{aligned}$$
5. So by induction, $P(n)$ is true for all $n \in \mathbb{N}$.

8. Inductively Odd

An 123 student learning recursion wrote a recursive Java method to determine if a number is odd or not, and needs your help proving that it is correct.

```
public static boolean oddr(int n) {
   if (n == 0)
      return False;
   else
      return !oddr(n−1);
}
```

Help the student by writing an inductive proof to prove that for all integers $n \geq 0$, the method `oddr` returns `True` if n is an odd number, and `False` if n is not an odd number (i.e. n is even). You may recall the definitions Odd$(n) := \exists x \in \mathbb{Z}(n = 2x + 1)$ and Even$(n) := \exists x \in \mathbb{Z}(n = 2x)$; `!True = False` and `!False = True`.

Solution:

Proof. Let P(n) be "`oddr(n)` returns True if n is odd, or False if n is even". We will show that P(n) is true for all integers $n \geq 0$ by induction on n.

Base Case: (n $= 0$)
0 is even, so P(0) is true if `oddr(0)` returns False, which is exactly the base case of `oddr`, so P(0) is true.
Inductive Hypothesis: Suppose P(k) is true for an arbitrary integer $k \geq 0$.
Inductive Step:

- **Case 1:** $k + 1$ is even.

  If $k+1$ is even, then there is an integer x s.t. $k+1 = 2x$, so then $k = 2x - 1 = 2(x-1)+1$, so therefore k is odd. We know that since $k+1 > 0$, `oddr(k+1)` should return `!oddr(k)`. By the Inductive Hypothesis, we know that since k is odd, `oddr(k)` returns True, so `oddr(k+1)` returns `!oddr(k)= False`, and $k + 1$ is even, therefore P(k+1) is true.

- **Case 2:** $k + 1$ is odd.

  If $k + 1$ is odd, then there is an integer x s.t. $k + 1 = 2x + 1$, so then $k = 2x$ and therefore k is even. We know that since $k + 1 > 0$, `oddr(k+1)` should return `!oddr(k)`. By the Inductive Hypothesis, we know that since k is even, `oddr(k)` returns False, so `oddr(k+1)` returns `!oddr(k)= True`, and $k + 1$ is odd, therefore P(k+1) is true.

Then P$(k + 1)$ is true for all cases. Thus, we have shown P(n) is true for all integers $n \geq 0$ by induction. □