CSE 390z: Mathematics for Computation Workshop

Week 5 Workshop

0. Conceptual Review

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

(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 $a \not\equiv b \pmod{n}$.

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

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.

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

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.

4. Modular arithmetic

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

5. Extended Euclidean Algorithm

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

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

Induction

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.

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.

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`.