CSE 390Z: Mathematics for Computation Workshop

Week 4 Workshop

Name: ____________________ Collaborators: ____________________

Conceptual Review

(a) What's the definition of "a divides b"?

(b) What's the definition of "a is congruent to b modulo m"?

(c) What's the Division Theorem?

(d) What's a good strategy for writing English proofs?

1. Modular Computation

(a) 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) $1 \cdot 2 \cdot 3 \cdot 4 | 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

(b) 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) $58 \equiv 707 \pmod{5}$

2. An Odd Proof

Prove that if n, m are odd, then $2n + m$ is odd.

3. Modular Addition

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

4. 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.

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

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

(d) Unroll the predicate definitions from your assumptions.

(e) Manipulate what you have towards your goal.

(f) Reroll into your predicate definitions.

(g) State your final claim.

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

5. Divisibility Proof

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

$$\forall n \forall d \; ((d \mid n) \rightarrow (-d \mid n))$$

(a) Translate the claim into English.

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

6. 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 $ac \equiv bd \pmod{m}$.

7. Another Divisibility Proof

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

8. 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.