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. Example Proofs

(a) Prove that if n, m are odd, then $n + m$ is even.

(b) Let m be a positive integer. Prove that if $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.

2. Computation

(a) Which of the following statements 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) Which of the following statements are true?
Recall for $a, b, m \in \mathbb{Z}$ and $m > 0$: $a \equiv_m b$ iff $m|(a - b)$.

- (a) $-3 \equiv_3 3$
- (b) $0 \equiv_9 9000$
- (c) $44 \equiv_7 13$
- (d) $-58 \equiv_5 707$
- (e) $58 \equiv_5 707$

3. 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) State the givens and declare any arbitrary variables you need to use.
Hint: there are no givens in this problem.

(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 (might be easier to do the next step first).

(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.

4. 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 a formal proof to show that the claim holds.

(c) Translate your proof to English.

5. Modular Arithmetic Proof

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 $ac \equiv_m bd$.

6. Another Divisibility Proof

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