CSE 390Z: Mathematics for Computation Workshop

Week 4 Workshop

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: $\quad a \equiv b \pmod{m} \quad \leftrightarrow \quad m \mid (a - b)$

(b) What's the Division Theorem?

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

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

1. 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.

2. 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.

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

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 that the claim holds.

6. Another Divisibility Proof

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

7. 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 $3 \nmid b$.

8. Proof by...how many cases?

Prove that for all integers n, $2n^2 + n + 1$ is not divisible by 3.

Hint: *You will probably want to use proof by cases for this problem. To decide which cases to use, consider the possible outcomes when dividing n by 3.*