CSE 390z: Mathematics for Computation Workshop

Week 4 Workshop

Conceptual Review

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

(b) What's the definition of "a is congruent to b mod m" ($a \equiv b \pmod{m}$)?

(c) 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 $\exists k \in \mathbb{Z}\ (b = ak)$.

(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 $m|(b - a)$.

(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. Divisibility Proof

Consider the following claim where the domain is the integers:

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

(a) Write a **formal proof** to show that the claim holds.

(b) Translate the claim into English.

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

3. Proofs by Contrapositive Part 1

Prove the following statement.

For all integers a, b, n, with $n > 0$: If $a^2 \not\equiv b^2 \pmod{n}$, then $a \not\equiv b \pmod{n}$.

(a) Why is this statement hard to prove with a Direct Proof? Try it out. Where do you get stuck?

(b) What is the contrapositive of the statement?

(c) Prove the original statement by contrapositive (using an English proof).

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. An Odd Proof

Write and English proof of the following statement: If n, m are odd, then $2n + m$ is odd.

6. Proofs by Contrapositive Part 2

Prove the following statement.

For all integers a, b: If $3 \nmid ab$, then $3 \nmid a$ and $3 \nmid b$.

(a) Why is this statement hard to prove with a Direct Proof? Try it out. Where do you get stuck?

(b) What is the contrapositive of the statement?

(c) Prove the original statement by contrapositive (using an English proof).

7. Proofs by Contradiction

Prove each statement by contradiction (using an English proof).

(a) Recall that a real number x is **rational** iff there exists integers p and q, with $q \neq 0$, such that $x = \frac{p}{q}$.
Prove: For all real numbers a, b, if a is rational and ab is irrational, then b is irrational.

(b) For all integers n, $4 \nmid n^2 - 3$.
Hint: It may be helpful to use cases.

8. More Number Theory Practice

Prove or disprove each of the following claims. Remember, you can disprove a "for all" claim by providing a counter example.

(a) For all $a, b, c \in \mathbb{Z}$, If $a \mid b$ and $c \mid (-a)$, then $(-c) \mid b$.

(b) For all $a, b, n, x \in \mathbb{Z}$ with $n > 0$, $a \equiv b \pmod{n}$ implies $x^a \equiv x^b \pmod{n}$.

(c) For all integers n, if n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.