# 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 modulo 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 $\exists k \in \mathbb{Z}\ (b = ka)$.

(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. 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 $3 \nmid b$.

## 4. 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 $n$, $4 \nmid n^2 - 3$.

## 5. 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.

## 6. More Number Theory Practice

For each of the following parts, prove or disprove the claim.

(a) If $a \mid b$ and $c \mid (-a)$, then $(-c) \mid b$.

(b) For all $a, b, n, x \in \mathbb{Z}$, $a \equiv_n b$ implies $x^a \equiv_n x^b$.

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

## 7. 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 $ac \equiv bd \pmod m$.