CSE 390z: Mathematics for Computation Workshop

Week 5 Workshop

0. 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: $\quad a \equiv_m b \quad \leftrightarrow \quad m \mid (a - b)$

(b) How do you know if a multiplicative inverse does not exist?
A multiplicative inverse does not exist when $gcd(a, b) \neq 1$.

(c) Bezout's theorem: If a and b are positive integers, then there exist integers s and t such that gcd(a, b) is equal to what?

$$\text{gcd}(a, b) = sa + tb$$

(d) What is Euclid's algorithm? What does it help us calculate?
Euclid's algorithm helps us find gcd(a, b).The algorithm is as follows:

- Repeatedly use gcd$(a, b) =$ gcd$(b, a\%b)$
- When you reach gcd$(g, 0)$, return g.

1. Modular Multiplication

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 $ac \equiv_m bd$.

2. Proofs by Contrapositive

For each part, write a proof by contrapositive of the statement.

(a) If $a^2 \not\equiv_n b^2$, then $a \not\equiv_n b$.

(b) For all integers a, b, if $3 \nmid ab$, then $3 \nmid a$ and $3 \nmid b$.

3. 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.

4. 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 $n^2 \equiv_3 1$.

5. Modular Arithmetic

Prove that for any odd integer a there is an integer b that satisfies $ab \equiv_8 2$.
Hint: You need to reason about the gcd(a,8) and use Bezout's theorem.

6. Extended Euclidean Algorithm

Find all solutions in the range of $0 \leq x < 2021$ to the modular equation:

$$311x \equiv_{2021} 3$$

7. Weak Induction Warmup

Prove by induction on n that for all integers $n \geq 4$, the inequality $n! > 2^n$ is true.
Complete the induction proof below.

8. Induction with Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all $n > 1$ by induction.