CSE 390z: Mathematics for Computation Workshop

Week 4 Workshop

Conceptual Review

(a) How do we prove a "for all" implication in a formal proof?
E.g., $\forall x(Even(x) \rightarrow Odd(x+1))$, Domain: integers

(b) How do we prove a "for all" implication in an English proof?
E.g., The sum of any even integer and 1 is odd.

(c) What's a good strategy for writing English proofs?

(d) What is the definition of "a divides b"?

(e) What is the Division Theorem?

(f) What's the definition of "a is congruent to b mod m" ($a \equiv_m b$)?

1 Formal Proofs: More Quantifiers (from end of last week)

(a) Given $\forall x(T(x) \to M(x))$ and $\exists x T(x)$, prove that $\exists x M(x)$.

(b) Given $\forall x(P(x) \to Q(x))$, prove that $(\exists x P(x)) \to (\exists y Q(y))$.

2. English Proof

Let the predicates Odd(x) and Even(x) be defined as follows where the domain is the integers:

$$\text{Odd}(x) := \exists k\ (x = 2k + 1)$$

$$\text{Even}(x) := \exists k\ (x = 2k)$$

Write and **English proof** of the following claim:

$$\forall x \forall y[(Even(x) \wedge Odd(y)) \rightarrow Odd(x + y)]$$

(a) Translate the claim to English.

(b) Declare any arbitrary variables you may need.

(c) Assume the left side of the implication.

(d) Unroll the definitions from your assumptions.

(e) Manipulate what you have towards your goal.

(f) Reroll definitions into the right side of the implication.

(g) Conclude that you have proved the claim.

(h) Now take these proof parts and assemble them into one cohesive English proof.

3. 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.

4. Modular Computation

(a) Circle the statements below that are true.
Recall for $a, b \in \mathbb{Z}$: $a|b \ := \ \exists k \in \mathbb{Z}\ (b = ka)$.

(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 $m > 0$: $a \equiv_m b \ := \ m|(a - b)$.

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

5. Modular Multiplication

Write an **English proof** of the following claim: For all integers a, b, c, d, m with $m > 0$, if $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.

6. Mod Practice

Write an **English proof** of the following claim: For all integers n, if n is not divisible by 3, then $n^2 \equiv_3 1$. You may use, without proof, that for any integers a, m with $m > 0$, $m \mid a$ iff $a \equiv_m 0$.

7. An Odd Proof

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

8. A Rational Contradiction

Recall that a real number x is **rational** iff there exist integers p and q, with $q \neq 0$, such that $x = \frac{p}{q}$.
Formally, for $x \in \mathbb{R}$, Rational$(x) := \exists p \exists q \in \mathbb{Z}\ (q \neq 0\ \wedge\ x = \frac{p}{q})$.

Write an **English proof** of the following statement:

For all real numbers a, b, if a is rational and ab is irrational, then b is irrational.

(a) Introduce any arbitrary variables you may need.

(b) Assume the premise of the implication.

(c) Unroll the definitions from your assumptions if necessary (use your judgment).

(d) We're going to use Reductio Ad Absurdum to prove that b is irrational (not rational). Write down the assumption we must make in order to do that.

(e) Finish the rest of the proof.