

CSE 390Z: Mathematics for Computation Workshop

QuickCheck: Number Theory Proof Solutions (due Monday, February 10)

Please submit a response to the following questions on Gradescope. We do not grade on accuracy, so please submit your best attempt. You may either typeset your responses or hand-write them. Note that hand-written solutions must be legible to be graded.

We have created [this template](#) if you choose to typeset with Latex. [This guide](#) has specific information about scanning and uploading pdf files to Gradescope.

0. Mod Madness

Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$. Write an English proof of the statement.

Solution:

Let integers $n > 1, m > 1$ be arbitrary and integers a, b be arbitrary. Suppose $n \mid m$ and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some integer k . By definition of congruence, we have $m \mid a - b$. By definition of divides, this means that $a - b = mj$ for some integer j . Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of divides, we have $n \mid a - b$. By definition of congruence, we have $a \equiv_n b$. Since n, m, a, b were arbitrary, we have shown that if $n \mid m$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

1. Video Solution

Watch [this video](#) on the solution **after** making an initial attempt. Then, answer the following questions.

- (a) What is one thing you took away from the video solution?