Charles Harrison (csharris)
CS 157 — Spring 2013 **Homework Study Guide** March 16, 2013

Modular Arithmetic

Modular Arithmetic is a system for dealing with restricted ranges of Integers. $x \mod n$ is the remainder when x is divided by n. So if

$$x = qn + r$$

then

$$x \mod n = r$$

Two numbers are said to be *conguent modulo* n if they differ by a multiple of n, that is

$$x \equiv y \mod n \iff n \text{ divides } (x - y)$$