Math 105, "Modular Arithmetic" – a brief introduction

<u>Definition</u>: "mod n" arithmetic
We say that two numbers, say a and b, are "equivalent mod n" if we can add n to (or subtract n from) a one or more times to get a result of b. In other words, a and b are "equivalent mod n" if the difference between a and b – that is, $a - b$ – is divisible by n.

Notation: If a and b are equivalent mod n, we write "$a \equiv b \ (mod\ n)$."

For example: 17 is equivalent to 1 mod 8. This is because 17-8=9, and 9-8=1. (It's also true that 17 is equivalent to 9 mod 8; in fact, all three of these numbers – 17, 9, and 1- are considered "equivalent" under mod 8 arithmetic rules.)

Typically, when we do arithmetic mod n, we only consider the numbers 0, 1, 2, etc., up to n-1. This is to keep things as simple as possible – under "mod n" rules, we only need n different numbers. So, if a number is greater than n-1 (that is, n or greater), we subtract n from it; conversely, if a number is less than 0, we add n to it.

Example: The above paragraph exactly describes the way we combine transpositions (based on the twelve-tone scale) – specifically, transpositions are combined according to "mod 12" arithmetic rules.

Note: Instead of saying "0, 1, 2, etc. up to n-1," we'll typically say "between 0 and n-1." Our usage of the word "between" will be in the inclusive sense; that is, 0 and n-1 are included, not excluded. For example, the phrase "between 0 and 5" means "0, 1, 2, 3, 4, or 5."

Examples:
* Find a number between 0 and 9 which is equivalent to 33 (mod 10).
Answer: To find numbers equivalent to 33, we can add 10 to it, or subtract 10 from it. Since 33 is greater than 9, we'll subtract: 33-10 = 23; 23-10=13; 13-10 = 3. Thus, 33 is equivalent to 3 (mod 10). This can also be written as $33 \equiv 3 \ (mod\ 10)$.

* Find a number between 0 and 8 which is equivalent to -22 (mod 9).
Answer: Since -22 is less than 0, we'll add 9: -22 + 9 = -13; -13 + 9 = -4; -4 + 9 = 5.
Therefore, -22 is equivalent to 5 (mod 9). In other "words," $-22 \equiv 5 \ (mod\ 9)$.

* Find a number between 0 and 7 which is equivalent to 100 (mod 8).
Answer: We could subtract 7 from 100 multiple times until we reached a result less than 8. Obviously we'd have to do that several times, which seems like a lot of work. A short cut for this problem would be to use division to see how many times we can take 7 away from 100: dividing 100 by 7 gives us $100 \div 7 = 14R2$. That is, $100 = 14 \times 7 + 2$; this tells us, in one step, that we would have to take 7 away from 100 14 times, and the end result would be the remainder of 2. So, our answer is 2.

This last example leads to a more general observation: two numbers are equivalent modulo n if, and only if, they have the same remainder when divided by n. This observation can be particularly useful when we are dealing with larger numbers.