Tuesday 6/24: Modular Arithmetic

Congruence Class

Congruence mod k: if k is any positive integer, $a, b \in \mathbb{Z}$ are congruent mod k (written $a \equiv b \pmod{k}$) if and only if $k \mid (a - b)$. In other words, a and b differ by a factor of k.

e.g., $17 \equiv 5 \pmod{12}$, $5 \equiv 12 \pmod{12}$, $38 \equiv 3 \pmod{7}$, $-6 \equiv 1 \pmod{7}$

Note: mod is not an operation; we are saying a and b are congruent to each other under some special mathematical system; *i.e.,* when we divide by k and find the remainder.

When we gather up groups of congruent integers and treat them all as a unit, we create a **congruence class** or an **equivalence class**. Specifically, suppose that we fix a particular value for k. Then, if x is an integer, the equivalence class of x (written $[x]$) is the set of all integers congruent to x mod k. Or, equivalently, the set of integers that have remainder x when divided by k.

For example, if we fix $k = 7$, then [3] contains all integers that are congruent to 3 (mod 7):

$$[3] = \{3, 10, -4, -11...\}$$

Note that:

- $[3] = [10] = [-4] = [-11]$... All of these expressions refer to the same set containing integers congruent to 3 (mod 7). By convention, we often use the smallest natural number in this class (in this case, 3) as the representative.
- The content of [3] depends on the modifier "(mod 7)". If we choose a different mod k, the number of congruence classes will change, and the members of each congruence class will change too.

For each fixed value of k, there are exactly k congruence classes, [0], [1] ... $[k-1]$. Each congruence class is disjoint, meaning that no integer can belong in more that one class. Every integer belongs in exactly one congruence class.

You might see the notation like "$[5]_7$" sometimes, and this means "the congruence class of [5] mod 7".

Modular Arithmetic

You can apply basic arithmetic operations (addition, subtraction, multiplication) on congruence classes just like you would on normal integers:

$$[x] + [y] = [x + y]$$

$$[x] * [y] = [x * y]$$

For example, using mod 7, or as we call it "in $\mathbb{Z}_7$", we can do computations such as:

$$[4] + [10] = [4 + 10] = [14] = [0]$$

$$[-4] * [10] = [-4 * 10] = [-40] = [2]$$

These operations can be pronounced as "four mod seven plus ten mod seven equals zero mod seven" and "negative four mod seven times ten mod seven equals two mod seven".