What is Abstract Algebra?

- Ex: There are many things we can "multiply":

  integers, real numbers, matrices, polynomials, ...

  What do these have in common?

  E.g. associative: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

  What don't they have in common?

  E.g. not all commutative: $x \cdot y = y \cdot x$

Worksheet 1: Modular Arithmetic

Math 335

---

1. Make sure every member of your group knows what the following statements mean:

$$5 \equiv 1 \mod 2 \longleftarrow \quad 5 \to 3 \to 1$$

$$2 \equiv 17 \mod 5 \longleftarrow \quad 2 \to 7 \to 12 \to 17$$

$$-1 \equiv 11 \mod 12$$

   If you haven't seen this notation before or don't remember what it means, ask questions of a groupmate. If you have seen it before, try to explain to your group what it means, in your own words; the more different perspectives your group has, the better.

   $a \equiv b \mod n$ means

   "you can get from a to b by adding & subtracting n's"

2. Consider the statement

$$26 \equiv \underline{\hspace{2cm}} \mod 12.$$

   (a) In how many ways could we fill in the blank? Are any of these ways "better" than any others?

   Infinitely many! E.g.

   $14, \boxed{2}, -10, -22, \ldots.$

   or $38, 50, 62, 74, \ldots.$

   (b) What's the smallest positive number that we could fill in the blank with?

$$26 \equiv \boxed{2} \mod 12$$

$$\uparrow$$

   this is the "best" answer for our purposes (between $0, 1, 2, \ldots, 11$)