Modular Arithmetic (Congruences)
Class activity, Week 5

Recall: For $n > 0$ in $\mathbf{N}$, we say a is **congruent** to b modulo n and write $a \equiv b \pmod{n}$, if $n|(a-b)$. The power of the $\equiv$ notation comes from the fact that it behaves like the equal sign. We now justify this.

Theorem 1: Let n be a positive integer. Then the following properties hold:

i. (Reflexivity) $a \equiv a \pmod{n}$ for any a.
ii. (Symmetry) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
iii. (Transitivity) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

proof: You proved (i) in problem pre-class, where we had $n = 7$.

To prove (ii), which is an 'if' statement, we assume the hypothesis and prove the conclusion. Assume $a \equiv b \pmod{n}$. By definition this means $n|(a-b)$, i.e. $a-b=kn$ for $k \in \mathbb{Z}$. In that case, $b - a =$ $(-k)n$, therefore $b \equiv a \pmod{n}$.

To prove (iii), assume $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. We want to show $a \equiv c \pmod{n}$. From the assumption, $a-b=kn$, $b-c=in$. Adding these two expressions, we find that $a - c =$ $(k+i)n$, therefore $a \equiv c \pmod{n}$. □

An *equivalence relation* is a relation satisfying the reflexivity, symmetry and transitivity properties. From Theorem 1, we conclude that the congruence relation on $\mathbf{Z}$ (the set of integers) is an equivalence relation. In other words, $\equiv$ behaves like an equal sign.

You also saw how different numbers congruent to each other behave under addition, subtract and multiplication. We summarize those results here:

Proposition 1: If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a + b \equiv a' + b' \pmod{n} \ , \ a - b \equiv a' - b' \pmod{n} \text{ and } ab \equiv a'b' \pmod{n}$$

Proposition 2: If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any integer $k \geq 0$.

These propositions basically say that, as far as addition, subtraction, and multiplication are concerned, congruences may be treated like equalities. This helps in simplifying congruence expressions.

For example, in order to simplify $17 \cdot 19 \pmod{5}$, we can use $17 \equiv 2 \pmod{5}$ and $19 \equiv 4 \pmod{5}$. Therefore, using Proposition 1, $17 \cdot 19 \equiv 2 \cdot 4 \pmod{5}$. Using transitivity and $8 \equiv 3 \pmod{5}$, we find that $17 \cdot 19 \equiv 3 \pmod{5}$, which can be double checked by evaluating $17 \cdot 19 \pmod{5}$ directly.

We can also use the first proposition to simplify congruence equations. Suppose $2x+4 \equiv 7 \pmod{9}$. Subtracting 4 from both sides gives $2x \equiv 3 \pmod{9}$. Since $3 \equiv 12 \pmod{9}$, this last equation is equivalent to $2x \equiv 12 \pmod{9}$. So, we see that $x = 6$ is a solution for the given congruence equation.

The two propositions can also be used in calculating powers, in an iterative fashion. Suppose we need to find $3^{105} \pmod{7}$. Notice $3^3 \equiv -1 \pmod{7}$. Since $3^{105} = (3^3)^{35}$, then $3^{105} \equiv (-1)^{35} \pmod{7}$. Hence $3^{105} \equiv -1 \pmod{7}$.

1. Find a solution for the congruence equation $4x+5 \equiv 6 \pmod{11}$ using the simplification process. (Note: Guess for an x when you have simplified the equation enough.)

$4x+5 \equiv 6 \pmod{11}$
$4x \equiv 1 \pmod{11}$
$4x \equiv 12 \pmod{11}$

$x = 3$ is a solution

Over →

2. Find a solution for the congruence equation $4x+9 \equiv 3 \pmod{11}$ using the simplification process.

$4x+9 \equiv 17$
$4x \equiv 5$
$4x \equiv 16$

$x = 4$ is a solution

3. Find a solution for the congruence equation $8x + 9 \equiv 3 \pmod{18}$. (Hint: Try other right hand sides after the first simplification.)

$8x+9 \equiv 21$
$8x \equiv 12$
$8x \equiv 48$

$x = 6$ is a solution

For now, we are only looking for one solution to these congruence equations. We will come back to the question of existence and uniqueness soon.

Residue Classes

As we saw in the pre-class, modulo n each number a is congruent to the remainder r for when a is divided by n. Therefore, we can think of the congruence relation as separating numbers into different groups based on their remainders. These groups are called the *residue classes* modulo n. Such a grouping is also valid for a general equivalence relation. For the congruence relation modulo n, we define $[a]$ (the residue class of a) to be the collection of all integers b such that $a \equiv b \pmod{n}$.

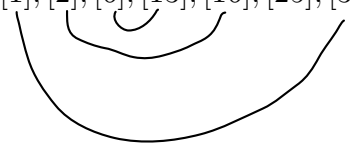
4 a. Modulo 7, determine which integers b are in $[3]$. List a few of these integers.

3
10
17
-4
-11

b. Modulo 7, determine which integers b are in $[10]$. List a few of these integers.

3
10
17
-4
-11

c. Modulo 7, determine which of the following residue classes are the same:
$[1], [2], [6], [13], [16], [25], [36]$.



We have the following results on how the residue classes relate.

Proposition 3: Let n be a positive integer and let $[a]$ represent the residue class of a modulo n.

i. If $a \equiv b \pmod{n}$, then $[a] = [b]$.
ii. If there exists a common element in $[a]$ and $[b]$, then $[a] = [b]$.
iii. Every element $z \in \mathbf{Z}$ belongs to a residue class.
iv. None of the residue classes is empty.

The last three properties can be said in a different way: The residue classes form a partition of non-empty subsets of **Z**. Because of the partition property, we can talk about each integer belonging to a unique residue class. All the integers that belong to a residue class are said to be *representatives* of that residue class. For example, 3 is a representative of [3] modulo 7, but 10 is also a representative of [3] modulo 7. A collection of integers is called a *complete residue system* modulo n if this collection contains exactly one integer for each residue class.

5 a. Show that $\{0, 1, \ldots, 6\}$ is a complete residue system modulo 7. This system is called the **least residue system**. by the division algorithm, every integer has a unique remainder r where $0 \leq r \leq 6$ after division by 7. (& all 7 are used) → Since each integer is congruent to its remainder, these all possible remainders cover all residue classes.

b. Find another complete residue system modulo 7.

$\{-6, -5, \ldots, -1, 0\}$