Math 412. §2.1: Congruence in $\mathbb{Z}$.

DEFINITION: Fix a nonzero integer N. We say that $a, b \in \mathbb{Z}$ are **congruent modulo** N if $N|(a-b)$. We write $a \equiv b \mod N$ for "a is congruent to b modulo N." Parse this notation as $a \equiv b \mod N$: the a and b are the two inputs, and $\equiv \quad \mod N$ is one piece, like a complicated equals sign.

DEFINITION: Fix a nonzero integer N. For $a \in \mathbb{Z}$, the **congruence class of** a **modulo** N is the subset of $\mathbb{Z}$ consisting of all integers congruent to a modulo N; That is, the **congruence class of** a **modulo** N is

$$[a]_N := \{b \in \mathbb{Z} \,|\, b \equiv a \mod N\}.$$

Note here that $[a]_N$ is the **notation** for this congruence class— in particular, $[a]_N$ stands for a *subset of* $\mathbb{Z}$, not a number.

Part 1: Getting acquainted.

A. WARM-UP: True or False. Justify.

(1) T or F: $5 \equiv 19 \mod 7$,
(2) T or F: $-5 \equiv 20 \mod 10$,
(3) T or F: $-11 \equiv -26 \mod 5$,
(4) T or F: Any two odd integers are congruent modulo 2.
(5) T or F: Any two odd integers are congruent modulo 3.

Solution.

(1) True: $7|(5-19)$
(2) False: $10 \not| -25$.
(3) True: $5|15$.
(4) True: the difference of odd numbers is even, so divisible by 2.
(5) False: $5-3$ is not divisible by 3.

B. INTRODUCTORY PROOFS.

(1) Show that Congruence Modulo N is an *Equivalence Relation*. That is, prove that
  (a) $a \equiv a \mod N$ (congruence is reflexive);
  (b) If $a \equiv b \mod N$, then $b \equiv a \mod N$ (congruence is symmetric);
  (c) If $a \equiv b \mod N$ and $b \equiv c \mod N$, then $a \equiv c \mod N$ (congruence is transitive).

(2) For a fixed $N > 0$, prove that every $a \in \mathbb{Z}$ is congruent mod N to some $r \in \mathbb{Z}$ such that $0 \leq r < N$.[1]

Solution.

(1) Since $N|(a-a)$, congruence is reflexive. Since $N|(a-b)$ if and only if $N|(b-a)$, congruence is symmetric. For transitivity, say $N|(a-b)$ and $N|(b-c)$. Then N divides the sum $(a-b)+(b-c) = a-c$.

(2) By the division algorithm, $a = Nq + r$ where $0 \leq r < N$.So $a \equiv r \mod N$.

C. Congruence Class Basics.

(1) List out (with the help of some "…"s) all of the elements in $[11]_4$.

(2) Given two congruence classes, $[a]_N$ and $[b]_N$, show that[2]

$$\text{either } [a]_N = [b]_N \text{ or } [a]_N \cap [b]_N = \emptyset.$$

(3) Explain why there are exactly N equivalence classes modulo N.

(4) Discuss with your team the following important idea: *Congruence Classes Mod N partition the integers into exactly N nonoverlapping subsets of $\mathbb{Z}$.* Have we proven this? What are these sets when $N = 2$? Can you find a nice way to list out these N sets using the notation $[a]_N$ in general? How does it look in set-builder notation?

Solution.

(1) Suppose $[a]_N \cap [b]_N \neq \emptyset$. Let $x \in [a]_N \cap [b]_N$. Then $x \equiv a \mod N$ and $x \equiv b \mod N$, so $a \equiv b \mod N$ by transitivity. We need to show $[a]_N \subset [b]_N$. Take any $y \in [a]_N$. Then $y \equiv a \mod N$, so again by transitivity, $y \equiv b \mod N$. So $[a]_N \subset [b]_N$. A similar argument shows the reverse inclusion.

(2) This follows from (2) and (3): Every integer is congruent to one of $0, 1, \ldots, N-1$ modulo N. So there are at most N congruence classes. But also, $[a]_N \neq [b]_N$ for $0 \leq a, b < N$, since if $N(a-b)$ then $a - b = 0$.

D. True or False? Justify.

(1) $47 \in [17]_5$.

[1] Hint: Division algorithm!

[2] Hint: One form of the contrapositive statement is: if $[a]_N \cap [b]_N \neq \emptyset$, then $[a]_N = [b]_N$. There are standard techniques you know from 217 to show two sets are the same.

(2) $[17]_7 \cap [23]_7 = \emptyset$.
(3) $[17]_6 \cap [19]_7 = \emptyset$.
(4) For all integers a, $[a]_{60} \subset [a]_{10}$.

Solution.

(1) TRUE: $47 - 17$ is a multiple of 5.
(2) TRUE: We show last time that either $[a]_N = [b]_N$ or $[a]_N \cap [b]_N = \emptyset$ for all a, b, N. Since $3 \in [17]_7$ but $3 \notin [23]_7$, these sets are not the same, and therefore, their intersection is empty.
(3) FALSE. $5 \in [17]_6 \cap [19]_7$.
(4) TRUE. Let $a+60k$ be an arbitrary element of $[a]_{60}$. Then writing $a + 60k = a + 10(6k)$, we see that it is also in $[a]_{10}$. So $[a]_{60} \subset [a]_{10}$.

An introduction to abstraction.

E. FUNCTIONS / OPERATIONS ON CONGRUENCE CLASSES.

(1) Take a second to recall the definition of a function. What makes a rule for turning inputs into outputs a well-defined function?
(2) Consider the following rule to turn congruence classes modulo 7 into congruence classes modulo 7:

$$[a]_7 \mapsto [\text{“round down } a \text{ to the nearest multiple of 10”}]_7.$$

Explain carefully why this is *not* a function from congruence classes modulo 7 to congruence classes modulo 7.
(3) Consider the following different rule to turn congruence classes modulo 7 to congruence classes modulo 7:

$$[a]_7 \mapsto [-a]_7.$$

Explain why this *is* a function from congruence classes modulo 7 to congruence classes modulo 7. Explain why this justifies that “taking negatives” is a well-defined function from congruence classes modulo 7 to itself.

Solution.

(1) There are different ways to define a function, but the key point we have in mind here is that the output depends only on the input; whenever we give the same input, we get the same result.
(2) Consider $x = [0]_7 = [14]_7$. Writing out x as $[0]_7$ and applying the rule gives $[0]_7$ as a result, whereas writing $x = [14]_7$ and applying the rule gives $[10]_7$, and these are different! Thus, the

rule does not only depend on the input (congruence class), but rather depends nontrivially on *how we write the class*.

(3) The rule a priori depends on how we write the class, so we need to check that if we write it in two different ways, we get the same result. Write $x = [a]_7 = [b]_7$. We need to show that $[-a]_7 = [-b]_7$. We know that $7|(a-b)$, so there is an integer c such that $(a-b) = 7c$. Then, $((-a)-(-b)) = -(a-b) = -7c$, so $7|((-a)-(-b))$. This shows that $[-a]_7 = [-b]_7$, as required.

Part 2: Looking forward.

F. ADDING & MULTIPLYING CONGRUENCE CLASSES. Fix $N \neq 0$. Let $a, b, c, d \in \mathbb{Z}$.

(1) Show that if $a \equiv c \mod N$ and $b \equiv d \mod N$, then $(a+b) \equiv (c+d) \mod N$.
(2) Show that if $a \equiv c \mod N$ and $b \equiv d \mod N$, then $(ab) \equiv (cd) \mod N$.[3]
(3) Discuss with your workmates how to use (1) and (2) to define a natural addition and multiplication on the set of congruence classes modulo N. This is delicate: we want to add/multiply two *sets* (namely, congruence classes) together to produce a third set. If you make some choices, how do you know that your operations are *well-defined*?
(4) There are exactly two congruence classes mod 2: the set of even numbers and the set of odd numbers. Make addition and multiplication tables for the operations you came up in (3) on the set $\{even, odd\}$ of all congruence classes mod 2. Is there an additive identity? Is there a multiplicative identity?
(5) Compute $([7]_5 + [-9]_5)$. Compute $[11]_3 \times [-66]_3$.

Solution. (1) and (2) are proven in Theorem 2.2 the book.
(3) is just reinterpreting this fact as a statement about congruence classes, as explained in the book at the beginning of 2.2 (page 32) and in the statement and proof of Theorem 2.6 in the book. Reread these sections if (3) is unclear to you.
(4) Modulo 2, the even numbers are the additive identity and the odd numbers are the multiplicative identity.
(5) $([7]_5 + [-9]_5) = [3]_5$ and $[11]_3 \times [-66]_3 = [0]_3$.

[3] Try adding and subtracting a convenient quantity from $ab - cd$.