LECTURE 4
(Friday Oct. 4, 2019)
**Goal:** Define addition & multiplication on the set 
\[ \mathbb{Z}_N = \{[0], [1], \ldots, [N-1]\} \sim \text{"integers mod } N\sim \]
(collection of all residue classes modulo \( N \)).

**Idea:** How to add two boxes of numbers?

1) Pick a number from each box
2) Add the two numbers
3) Put the sum back in a box.

**Problem:** The resulting box in 3) may depend on the numbers drawn in 1), i.e., not well-defined.

**EX:** Divide \( \mathbb{Z} \) into two boxes:

- \( A = \{x \in \mathbb{Z}: x > 0\} \)
- \( B = \{x \in \mathbb{Z}: x \leq 0\} \)

○ First say we pick \( 1 \in A \) and \( -2 \in B \). Then \( 1 + (-2) = -1 \notin B \).

○ On the other hand, picking \( 2 \in A \) and \( -1 \in B \) yields \( 2 + (-1) = 1 \in A \). —different boxes!
This issue does not arise for residue classes:

**Theorem.** Suppose \( a \equiv a' \) and \( b \equiv b' \pmod{N} \).

Then:

(i) \( ab \equiv a'b' \) and

(ii) \( a+b \equiv a'+b' \pmod{N} \).

**Proof (ii):**

\[
(a+b)-(a'+b') = (a-a')+(b-b') \quad \text{is divisible by } N.
\]

**Trick:**

\[
ab-a'b' = ab-a'b + a'b - a'b' \quad \text{cancel.}
\]

\[
= (a-a')b + a'(b-b') \quad \text{is divisible by } N.
\]

This result justifies:

**Definition.** Two residue classes in \( \mathbb{Z}_N \) are added/multiplied by the rules:

\[
[a] + [b] := [a+b] \quad \text{(on RHS usual + and \hspace{1cm} \bullet \hspace{1cm} \text{for } \mathbb{Z})}
\]

\[
[a] \cdot [b] := [ab]
\]
Well-defined: \[ [a] = [a'] \text{ and } [b] = [b'] \implies [a+b] = [a'+b'] \text{ and } [ab] = [a'b'] \checkmark \]

Observe: \( \mathbb{Z}_N \) with + is a (abelian) group. Indeed, the associative law is "inherited" from \( \mathbb{Z} \):

- \( ([a] + [b]) + [c] = [a+b] + [c] = [a+b+c] = [a] + [b+c] = e \downarrow [a] + ([b] + [c]) \)

- \( [a] + [0] = [a+0] = [a] \)

- \( [a] + [-a] = [a+(-a)] = [0] \).

\( e \) is the (additive) inverse of \([a]\).

However, \( \mathbb{Z}_N \) with \( \cdot \) is not a group:

- Associative law holds, \([1]\) is neutral, but \([0]\) has no (multiplicative) inverse — unless \( N = 1 \).
Taking out \([0]\) may still not yield a group:

**Theorem.** \([a]\) has a multiplicative inverse in \(\mathbb{Z}_N\) exactly when \(\text{GCD}(a, N) = 1\).

**Why?** ↑: 1st suppose \(a, N\) are **coprime**. Find \(x, y \in \mathbb{Z}\) such that \(1 = ax + Ny\). Shows

\(1 \equiv ax \pmod{N}\). I.e., \([x]\) is an inverse of \([a]\).

↓: Conversely, if \([a] \cdot [x] = [1]\) we conclude \(ax \equiv 1 \pmod{N}\). In other words \(1 - ax = Ny\) for some \(y \in \mathbb{Z}\).

If \(d > 0\) divides \(a, N\) this shows \(d \mid 1\)

— and therefore \(d = 1\). □

**Exc.:** If \(a, b \in \mathbb{Z}\) are both **coprime** to \(N\), then so is their product \(ab\).

**Hint:** \(p \mid ab \Rightarrow p \mid a\) or \(p \mid b\)
Deduce from exercise that \( \ast \) is a composition law on the set
\[ \mathbb{Z}_N^\times = \{ [a] : \text{GCD}(a, N) = 1 \} \]

family of all invertible residue classes. (multiplicative) group of units.
\[ |\mathbb{Z}_N^\times| = \# \{ a : 0 \leq a < N, \text{GCD}(a, N) = 1 \} = \phi(N) \]

"Euler's totient function."

Special case: \( N = p \) prime.
Here every positive \( a < p \) is coprime to \( p \), so
\[ |\mathbb{Z}_p^\times| = \phi(p) = p - 1. \]

In other words, in the prime case, \( \mathbb{Z}_p^\times \) consists of all nonzero residue classes.

Example \((N = 6)\):
\[ \mathbb{Z}_6^\times = \{ [1], [5] \} ? \]
\[ [2] \cdot [3] = [0]. \] "zero-divisors"