Units and zero divisors in $\mathbf{Z}_n$

MTH 350 -- Module 5B

Three important observations from last class:

In $\mathbf{Z}_n$ (for any n),

- An additive identity exists, and it's [0].
- A multiplicative identity exists, and it's [1].
- Every class [a] has an additive inverse, and it's [n-a].

Two important questions:

1. Does every element in $\mathbf{Z}_n$ have a *multiplicative* inverse? Given [a], is there a solution to [a][x] = 1?
2. If [a][b] = [0], does one of the two classes have to be zero?

Answers:

1. Not always (example: [3] in $\mathbf{Z}_6$) → Which element of $\mathbf{Z}_n$ have multiplicative inverses?
2. No (example: [3] in $\mathbf{Z}_6$) → Which elements of $\mathbf{Z}_n$ cause this to happen?

Activity 1: What are the zero divisors in $\mathbf{Z}_n$?

Go to the spreadsheet from last class.

- Group 1: n = 7 and 8
- Group 2: n = 4 and 11
- Group 3: n = 5 and 10
- Group 4: n = 9

List all the zero divisors in your $\mathbf{Z}_n$'s. $\mathbf{Z}_6$ was done for you in the Daily Prep video.

Any patterns or shortcuts here?

Zero divisors

Z_2	None
Z_3	None
Z_4	
Z_5	
Z_6	[2], [3], [4]
Z_7	
Z_8	
Z_9	
Z_{10}	
Z_{11}	

Let n be a natural number. Then $[a] \neq [0]$ is a zero divisor in $\mathbf{Z}_n$ if and only if...

Activity 2: What are the units in $\mathbf{Z}_n$?

Go to the spreadsheet from last class.

- Group 1: n = 7 and 8
- Group 2: n = 4 and 11
- Group 3: n = 5 and 10
- Group 4: n = 9

List all the units in your $\mathbf{Z}_n$'s. $\mathbf{Z}_6$ was done for you in the Daily Prep video.

Any patterns or shortcuts here?

Units and multiplicative inverses

	Units	Multiplicative inverses of the units
Z_2	[1]	[1]
Z_3	[1], [2]	[1], [2]
Z_4		
Z_5		
Z_6	[1], [5]	[1], [5]
Z_7		
Z_8		
Z_9		
Z_{10}		
Z_{11}		

Let n be a natural number. Then [a] is a unit in $\mathbf{Z}_n$ if and only if...

Finding multiplicative inverses without tables

If [a] is a unit,

- Corollary 3.11 says there are integer solutions to $ax + ny = 1$
- Since the two sides are equal integers, their congruence classes mod n are equal: $[ax + ny]_n = [1]_n$
- The left side is [a][x] + [n][y] (Why?)
- This simplifies to [a][x] (Why?)
- Therefore [a][x] = [1] and so [x] is the multiplicative inverse; can be computed using the Extended Euclidean Algorithm