Lecture 8

Def: Let $[a] \in \mathbb{Z}/n$.

(1) An additive inverse of $[a]$ is an element $[b] \in \mathbb{Z}/n$ such that

$$[a] \oplus [b] = [b] \oplus [a] = [0]$$

(2) If $[a] \neq 0$, a multiplicative inverse of $[a]$ is an element $[b] \in \mathbb{Z}/n$ such that $[a] \odot [b] = [b] \odot [a] = [1]$.

Ex: In $\mathbb{Z}/6$.

$[2]$ is an additive inverse of $[4]$: $[4] \oplus [2] = [0]$

$[3]$ is a multiplicative inverse of $[2]$: $[2] \odot [3] = [1]$

Proposition 15: For all $[a] \in \mathbb{Z}/n$, there exists an additive inverse. Moreover, it is unique.

Proof: Observe that $[-a] \in \mathbb{Z}/n$ is s.t. $[a] \oplus [-a] = [-a] \oplus [a] = [0]$.

Suppose there are $[b], [c] \in \mathbb{Z}/n$ additive inverses of $[a]$. Then,

$$[b] = [b] \oplus [0] = [b] \oplus ([a] \oplus [c]) = [b] \oplus [a+c]$$

$$= [b+(a+c)] = [(b+a)+c]$$

$$= [b+a] \oplus [c] = ([b] \oplus [a]) \oplus [c] = [0] \oplus [c] = [c].$$

⚠ Unlike additive inverses, multiplicative inverses do not always exist.

However, if they exist, they are unique.

Proposition 16: If $[a] \neq [0]$ in $\mathbb{Z}/n$ has a multiplicative inverse, then it is unique.

Proof: Similar to the one in Prop 15.

Def: Let $[a] \in \mathbb{Z}/n$.

The additive inverse of $[a]$ will be denoted by $-[a]$. (i.e. $-[a] = [-a]$)

The multiplicative inverse of $[a]$ will be denoted by $[a]^{-1}$ (when it exists).

Ex: In $\mathbb{Z}/9$.

$[6] \oplus [3] = [0]$, then $-[6] = [3]$ and $-[3] = [6]$.

additive inverse of $[6]$ is $[3]$

additive inverse of $[3]$ is $[6]$

$[5] \odot [2] = [1]$, then $[5]^{-1} = [2]$ and $[2]^{-1} = [5]$

multiplicative inverse of $[5]$ is $[2]$

multiplicative inverse of $[2]$ is $[5]$

Def: Let $k \in \mathbb{N} \setminus \{0\}$ and $[a] \in \mathbb{Z}/n$.

$$-k[a] := \underbrace{(-[a]) \oplus \cdots \oplus (-[a])}_{k\text{-times}}$$

Ex: In $\mathbb{Z}/9$. $\quad -2[6] = (-[6]) \oplus (-[6]) = [3] \oplus [3] = [6]$

Remark: $-k[a] = [-ka]$. As you would expect!

Properties of Addition

In $\mathbb{Z}$

1. Closure
2. Associativity
3. Identity (additive)
   $\exists\, 0 \in \mathbb{Z},\ \forall a \in \mathbb{Z},\ a + 0 = 0 + a = a.$
4. Inverse
   $\forall a \in \mathbb{Z},\ \exists -a \in \mathbb{Z},\ a + (-a) = (-a) + a = 0.$
5. Commutativity

In $\mathbb{Z}/n$

1. Closure
2. Associativity
3. Identity (additive)
   $\exists [0] \in \mathbb{Z}/n,\ \forall [a] \in \mathbb{Z}/n,\ [a] \oplus [0] = [0] \oplus [a] = [a].$
4. Inverse
   $\forall [a] \in \mathbb{Z}/n,\ \exists [-a] \in \mathbb{Z}/n,\ [a] \oplus [-a] = [-a] \oplus [a] = [0].$
5. Commutativity

Properties of Multiplication

In $\mathbb{Z}$

1) Closure

2) Associativity

3) Identity (multiplicative)

$\exists\, 1 \in \mathbb{Z},\ \forall a \in \mathbb{Z},\quad a \cdot 1 = 1 \cdot a = a$

4) Commutativity

~~5) Inverse~~

$\cancel{\forall a \in \mathbb{Z},\ \exists\, a^{-1} \in \mathbb{Z},\quad a \cdot a^{-1} = a^{-1} \cdot a = 1}$

$\cancel{a \neq 0}$

6) If $ab = 0$, then $a = 0$ or $b = 0$.

In $\mathbb{Z}/n$

1) Closure

2) Associativity

3) Identity (multiplicative)

$\exists\, [1] \in \mathbb{Z}/n,\ \forall [a] \in \mathbb{Z}/n,\quad [a] \odot [1] = [1] \odot [a] = [a]$

4) Commutativity

5) Inverse

Not true in general

$\forall [a] \in \mathbb{Z}/n,\ \exists\, [a]^{-1} \in \mathbb{Z}/n,\quad [a] \odot [a]^{-1} = [a]^{-1} \odot [a] = [1]$

$[a] \neq [0]$

~~6) If $[a] \odot [b] = 0$, then $[a] = 0$ or $[b] = 0$.~~

Addition and Multiplication Tables

Since $\mathbb{Z}/n$ is a finite set we can use a table to describe operations on it.

Ex: In $\mathbb{Z}/5$

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

We can identify properties that an operation satisfies by examining its table:

1. Identity:

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]				
[2]	[2]				
[3]	[3]				
[4]	[4]				

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]		[0]			
[1]	[0]	[1]	[2]	[3]	[4]
[2]		[2]			
[3]		[3]			
[4]		[4]			

② Inverse:

⊕	[0]	[1]	[2]	[3]	[4]
[0]	[0]				
[1]					[0]
[2]				[0]	
[3]			[0]		
[4]		[0]			

⊙	[0]	[1]	[2]	[3]	[4]
[0]					
[1]		[1]			
[2]				[1]	
[3]			[1]		
[4]					[1]

$-[1] = [4]$ $\quad -[3] = [2]$

$-[2] = [3]$ $\quad -[4] = [1]$

$[1]^{-1} = [1]$ $\quad [3]^{-1} = [2]$

$[2]^{-1} = [3]$ $\quad [4]^{-1} = [4]$

③ Commutativity:

⊕	[0]	[1]	[2]	[3]	[4]
[0]		[1]	[2]	[3]	[4]
[1]	[1]		[3]	[4]	[0]
[2]	[2]	[3]		[0]	[1]
[3]	[3]	[4]	[0]		[2]
[4]	[4]	[0]	[1]	[2]	

⊙	[0]	[1]	[2]	[3]	[4]
[0]		[0]	[0]	[0]	[0]
[1]	[0]		[2]	[3]	[4]
[2]	[0]	[2]		[1]	[3]
[3]	[0]	[3]	[1]		[2]
[4]	[0]	[4]	[3]	[2]	

Symmetry with respect to the diagonal.

Equations in $\mathbb{Z}/n$

Equations in $\mathbb{Z}/n$ can be solved by substituting each class in the equation to see which ones are solutions.

Ex: Solve $x^2 \oplus ([5] \odot x) = [0]$ in $\mathbb{Z}/6$

Solutions
$[0], [1], [3], [4]$

$x = [0]$ clearly works ✓

$x = [1] \implies [1]^2 \oplus ([5] \odot [1]) = [1] \oplus [5] = [0]$ ✓

$x = [2] \implies [2]^2 \oplus ([5] \odot [2]) = [4] \oplus [4] = [2] \neq [0]$

$x = [3] \implies [3]^2 \oplus ([5] \odot [3]) = [3] \oplus [3] = [0]$ ✓

$x = [4] \implies [4]^2 \oplus ([5] \odot [4]) = [4] \oplus [2] = [0]$ ✓

$x = [5] \implies [5]^2 \oplus ([5] \odot [5]) = [1] \oplus [1] = [2] \neq [0]$

Def: Let $[a] \neq [0]$ in $\mathbb{Z}/n$.

(1) $[a]$ is called a unit if the equation $[a] \odot x = [1]$ has a solution in $\mathbb{Z}/n$.

Explicitly $\rightsquigarrow$ $\exists\, [b] \in \mathbb{Z}/n$ s.t. $[a] \odot [b] = [1]$. (i.e. $[a]$ has an inverse).

(2) $[a]$ is called a zero divisor if the equation $[a] \odot x = [0]$ has a nonzero solution in $\mathbb{Z}/n$.

Explicitly $\rightsquigarrow$ $\exists\, [b] \in \mathbb{Z}/n$ s.t. $[b] \neq 0$ and $[a] \odot [b] = [0]$.

Ex: Find the units and zero divisors in the following sets of congruence classes.

- $\mathbb{Z}/2 = \{ [0], [1] \}$

  Units: $[1]$ with $[1]^{-1} = [1]$

  Zero divisors: none

- $\mathbb{Z}/3 = \{[0], [1], [2]\}$

  Units: $[1]$ with $[1]^{-1} = [1]$
  $[2]$ with $[2]^{-1} = [2]$

  Zero divisors: none

- $\mathbb{Z}/4 = \{[0], [1], [2], [3]\}$

  Units: $[1]$ with $[1]^{-1} = [1]$
  $[3]$ with $[3]^{-1} = [3]$

  Zero divisors: $[2]$ bc $[2] \odot [2] = [0]$

- $\mathbb{Z}/5 = \{[0], [1], [2], [3], [4]\}$

  Units: $[1]$ with $[1]^{-1} = [1]$
  $[2]$, $[3]$ with $[2]^{-1} = [3]$
  $[4]$ with $[4]^{-1} = [4]$

  Zero divisors: none

- $\mathbb{Z}/6 = \{[0], [1], [2], [3], [4], [5]\}$

  Units: $[1]$ with $[1]^{-1} = [1]$
  $[5]$ with $[5]^{-1} = [5]$

  Zero divisors: $[2]$, $[3]$ bc $[2] \odot [3] = [0]$
  $[4]$ bc $[4] \odot [3] = [0]$

Theorem 17: Let $n \in \mathbb{N} \setminus \{0,1\}$ and $[a] \in \mathbb{Z}/n$.

$$[a] \text{ is a unit in } \mathbb{Z}/n \text{ iff } \gcd(a,n) = 1.$$

Proof: See Question 5, PS4.

Theorem 18: Let $p \in \mathbb{N} \setminus \{0,1\}$, then the following conditions are equivalent:

(1) p is prime.

(2) $\forall [a] \neq 0$ in $\mathbb{Z}/p$, the equation $[a] \odot x = [1]$ has a solution in $\mathbb{Z}/p$.

(3) Whenever $[b] \odot [c] = [0]$ in $\mathbb{Z}/p$, then $[b] = [0]$ or $[c] = [0]$.

Proof:

$$\begin{tikzcd} & (1) \arrow[dr, Rightarrow] & \\ (3) \arrow[ur, Rightarrow] & & (2) \arrow[ll, Rightarrow] \end{tikzcd}$$