Group Theory

4th - Class

I The group $\mathbb{Z}_n$

We defined an equivalence relation on the set of integers, $\mathbb{Z}$, as follows;

- Fix a positive integer n
- For $a, b \in \mathbb{Z}$, define $\boxed{a \equiv b \pmod{n}}$ a congruent to b modulo n
  if $b-a$ is divisible by n, i.e.
  $b-a = q \cdot n$ for some $q \in \mathbb{Z}$
- We checked that this indeed is an equiv. rel.
  i.e.: (1) $a \equiv a$
  (2) $a \equiv b \Leftrightarrow b \equiv a$
  (3) $a \equiv b$ & $b \equiv c \Rightarrow a \equiv c$
- $\mathbb{Z}_n := \{$ congruence classe of integers modulo $n\}$
  $= \{ [a]_n : a \in \mathbb{Z} \}$

where $[a]_n = \{ b \in \mathbb{Z} \mid n \mid a-b \}$

This set has a natural group structure, written additively $(* = +)$, with identity $e = [0]_n$:

$$\boxed{[a]_n + [b]_n := [a+b]_n}$$

check:
- $([a]+[b]) + [c] = [a] + ([b]+[c])$
- $[a] + [0] = [0] + [a] = [a]$
- $[a] + [n-a] = [n-a] + [a] = [0]$

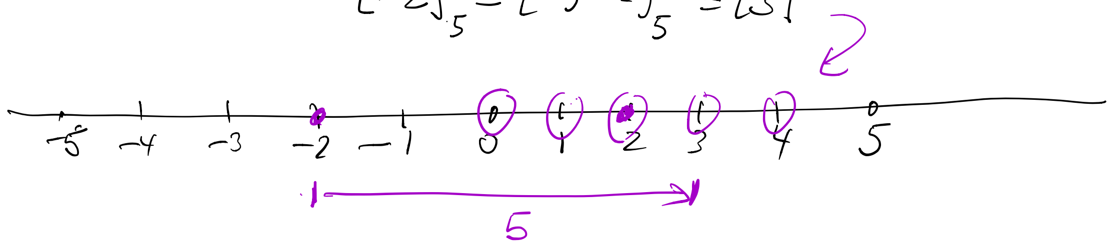
note . $\mathbb{Z}_n = \{ [0]_n, [1]_n, \ldots, [n-1]_n \}$

- recall $[a]_n = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$
  so we may write $[a]_n = [b]_n$ where
  $0 \le b \le n-1$

eg: $[17]_5 = [2]$ $\qquad 17 = 5 \cdot 3 + 2$

$\overset{\uparrow}{a} \quad \overset{\uparrow}{n} \quad \overset{|}{q} \quad \overset{\uparrow}{b}$

- $n=5$; $a=2$ has (additive) inverse
  $[-2]_5 = [5-2]_5 = [3]$



<u>Note</u> $\mathbb{Z}_n$ is a commutative group:

$$[a] + [b] = [b] + [a]$$

<u>Multiplication table for $\mathbb{Z}_n$</u> (or, <u>Cayley table</u>)

<u>$n=2$</u>

	0	1
0	0	1
1	1	0

$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$
$= \{0, 1\}$

<u>$n=3$</u>

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

<u>$n=4$</u>

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

- Important observation: Both rows and columns are permutations of $\{0, 1, \ldots, n-1\}$ (n of them)
  Moreover, there are no repetions on either rows or columns.
- Hence, the multiplication tables above are
  <u>Latin squares!</u>

- This is true for any (finite) group G: its multiplication is a Latin square of size $|G|$.

e	a	b	$c \cdots$	x
a	$a*a$	$a*b$	$a*c$	$a*x$
b	$b*a$	$b*b$	$b*c$	
c	$c*a$	$c*b$	$c*c$	
$\vdots$				

Suppose $a*b = a*x$. Then, by the Cancellation Law for groups: $b = x$.

<u>Rem</u> Magmas $(S,*)$ that have the cancellation property $(a*b = a*c \Rightarrow b=c)$ are called <u>quasi-groups</u>. Their Cayley tables are Latin squares. Conversely, any Latin square defines a quasi-group.

Back to $\mathbb{Z}_n$

$\mathbb{Z}_n$ also has a multiplication operation:

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$([a]_n, [b]_n) \longmapsto [a]_n \cdot [b]_n := [ab]_n$$

<u>check</u>: $\begin{matrix} a \equiv a' \\ b \equiv b' \end{matrix} \Rightarrow \begin{matrix} a'-a = qn \\ b'-b = pn \end{matrix} \Rightarrow a'b' = (a+qn)(b+pn)$
$= ab + bqn + apn + pqn^2$
$= ab + n(bq + ap + pqn)$

$\therefore\ a'b' \equiv ab \pmod n$

$\therefore\ [ab]_n = [a'b']_n$ and the $\cdot$ operation on $\mathbb{Z}_n$ is well-defined

Easily checked: this multiplication operation on $\mathbb{Z}_n$ is associative, and has identity $[1]_n$.

$[1]_n \cdot [a]_n = [a]_n \cdot [1]_n = [a]_n$ (since $a \cdot 1 = 1 \cdot a = a$ in $\mathbb{Z}$)

$\therefore (\mathbb{Z}_n, \cdot)$ is a monoid. But it is ~~not~~ not a group, since $[0]$ does not have an inverse.

Note: . Multiplication is distributive w.r.t. addition:

$$\boxed{[a]_n \cdot ([b]_n + [c]_n) = [a]_n [b]_n + [a]_n [c]_n}$$

. Also, $\cdot$ is commutative.

Hence, $(\mathbb{Z}_n, +, \cdot)$ is a ring (in fact, a commutative ring)

Def $\mathbb{Z}_n^{\times} = \{[a] \in \mathbb{Z}_n \mid [a]$ has a (multiplicative) inverse$\}$

i.e., $\exists [b]_n$ s.t. $[a]_n \cdot [b]_n = 1$,

i.e. $ab = 1 + qn$, for some $q \in \mathbb{Z}$

Prop $[a]_n$ in $\mathbb{Z}_n$ is invertible $\iff \gcd(a,n) = 1$

eg: * $[3]$ is invertible in $\mathbb{Z}_{10}$, since $\gcd(3,10) = 1$
or $\cdot [3] \cdot [7] = [21] = [1]$

* $[4]$ is not invertible in $\mathbb{Z}_{10}$, since $\gcd(4,10) = 2 \neq 1$

Proof ($\Rightarrow$) Suppose $[a]_n \cdot [b]_n = [1]_n$. Then:

$ab = 1 + nq$ for some $q \in \mathbb{Z}$

$ab + (-q)n = 1 \underset{\text{by Thm from last time}}{\Longrightarrow} \gcd(b,n) = 1$

($\Leftarrow$) $\gcd(a,n) = 1 \Rightarrow 1 = ak + qn$ for some $k, q \in \mathbb{Z}$

$\Rightarrow ak = 1 - qn$

$\Rightarrow [a]_n \cdot [k]_n = [1]_n$ (and so $[k]_n = [a]_n^{-1}$) ∎

Write $\mathbb{Z}_n^{\times} = \{[a]_n \in \mathbb{Z}_n : [a]_n$ is invertible$\}$

has a multiplicative inverse

$= \{ [a]_n \in \mathbb{Z}_n : \gcd(a,n)=1 \}$

Clearly, $(\mathbb{Z}_n^\times, \cdot, [1]_n)$ is a <u>group</u>!

<u>Question</u>: What is the size of this group?
i.e., what is $|\mathbb{Z}_n^\times|$?

<u>Examples</u>

n	$\mathbb{Z}_n$	$\mathbb{Z}_n^\times$	$\lvert\mathbb{Z}_n^\times\rvert$
2	$\{0,1\}$	$\{1\}$	1
3	$\{0,1,2\}$	$\{1,2\}$	2
4	$\{0,1,2,3\}$	$\{1,3\}$	2
5	$\{0,1,2,3,4\}$	$\{1,2,3,4\}$	4
6	$\{0,1,2,3,4,5\}$	$\{1,5\}$	2
7	$\{0\,1\,1\,3\,4\,5\,6\}$	$\{1\,2\,3\,4\,5\,6\}$	6
8	$0\,1\,2\,3\,4\,5\,6\,7$	$\{1,3,5,7\}$	4

<u>Define</u> The <u>Euler (totient) function</u> (or Euler's φ-function) is defined as:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$
$$\varphi(n) = |\mathbb{Z}_n^\times|$$

<u>Thm</u> (Euler) If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $(\alpha_k \geq 1)$ is the prime factorization of n, then:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

eg:
$$\varphi(2) = 2\left(1-\frac{1}{2}\right) = 2\cdot\frac{1}{2} = 1$$
$$\varphi(4) = 4\left(1-\frac{1}{2}\right) = 4/2 = 2$$
$$\varphi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 6\cdot\frac{1}{2}\cdot\frac{2}{3} = 2$$

p prime $\Rightarrow$ $\varphi(p) = |\{0 \leq a \leq p-1 \mid \gcd(a,p)=1\}| = p-1$

or $\varphi(p) = p \cdot \left(1 - \frac{1}{p}\right) = p \cdot \frac{p-1}{p} = p-1$ ✓