Modular Arithmetic

Assume we know about $\mathbb{Z}$. For integers $a, b, n$
Say $n$ divides $m$, and write $n \mid m$, when $\exists k \in \mathbb{Z}$ s.t. $m = n \cdot k$.

Fix $n \in \mathbb{N}$. Define a relation $\sim_n$ on $\mathbb{Z}$ s.t.

$$a \sim_n b \iff n \mid a - b$$

\[\begin{align*}
5 \sim_n 3 & \quad \text{because } 5 - 3 = 2 \text{ and } 2 \mid 2 \\
7 & \sim_n 337 \quad \text{because } 7 - 337 = -330 \\
10 & \mid 7 - 337 = -330 \\
& \quad \text{and } 10 \mid -330
\end{align*}\]

Claim $\sim_n$ is an equivalence relation.

Reflexive: Is $a \sim_n a$? $a - a = 0$ and $n \mid 0 \mid 0$ b/c $0 = n \cdot 0$ so $a \sim_n a$.

Symmetric: Suppose $a \sim_n b$ in which case $a - b = n \cdot k$ for some $k \in \mathbb{Z}$. Then $b - a = - (a - b) = - n \cdot k = n \cdot (-k)$ and $-k \in \mathbb{Z}$ so $n \mid b - a$ and thus $b \sim_n a$. 


Transitive Suppose \( a \sim b \), \( b \sim c \) with \( k, l \in \mathbb{Z} \) s.t. \( a - b = n \cdot k \), \( b - c = n \cdot l \). Adding these,
\[
(a - b) + (b - c) = nk + nl
\]
\[
a - c = n \cdot (k + l).
\]
Since \( k + l \in \mathbb{Z} \), get \( n \mid a - c \) so \( a \sim c \). \( \square \)

On partitions \( \mathbb{Z} \) into equivalence classes.

What are the equivalence classes?

Write \([a] = [a]_n\) for the equiv class (under \( \sim \)) of \( a \), i.e.,
\[
[a] = \{ b \in \mathbb{Z} \mid b \sim a \}
\]
\[
= \{ b \in \mathbb{Z} \mid n \mid b - a \}
\]
\[
= \{ b \in \mathbb{Z} \mid b - a = n \cdot k \text{ for some } k \in \mathbb{Z} \}
\]
\[
= \{ b \in \mathbb{Z} \mid b = a + nk \text{ for some } k \in \mathbb{Z} \}
\]
\[
= \{ a + nk \mid k \in \mathbb{Z} \}
\]
\[
\equiv x_i
\]
\[
\Xi = \Xi = X;
\]
Thus \( a = \frac{\Xi}{\Xi} \)
\[ n=3 \]

\[ [0]_3 = \{ 0+3k \mid k \in \mathbb{Z} \} = \{ 3k \mid k \in \mathbb{Z} \} \]

\[ [1]_3 = \{ 1+3k \mid k \in \mathbb{Z} \} \]

\[ [2]_3 = \{ 2+3k \mid k \in \mathbb{Z} \} \]

**Observation** \[ \mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3 \]

and \[ [i] \cap [j] = \emptyset \]

if \( i \neq j \) for \( i, j \in \{0, 1, 2\} \).

In fact, \[ [i]_n \cap [j]_n = \begin{cases} \emptyset & i \neq j \\ [i]_n = [j]_n & i = j \end{cases} \]

Write \( \mathbb{Z}_n \) for \( \mathbb{Z}/n\mathbb{Z} \), i.e., the set of mod \( n \) equivalence classes.

Preferred names for these: \( \{ [0]_n, [1]_n, \ldots, [n-1]_n \} \)

(If we go further, get \( [0]_n = [k]_n \) \( \forall c \) \( 0 \equiv n \)

\( \forall c \) \( \text{n} - 0 \equiv n = n \cdot 1 \).
Notation  The relation \( a \equiv b \pmod{n} \) is usually written as \( a \equiv b \pmod{n} \) or \( a \equiv b \pmod{n} \).

Read this as "\( a \) is congruent to \( b \pmod{n} \)."

Arithmetic  If \( a \equiv a', b \equiv b' \), then

\[
a + b \equiv a' + b' \quad \text{and} \quad a \cdot b \equiv a' \cdot b'.
\]

This allows us to define

\[
[a]_n + [b]_n = [a+b]_n
\]

\[
[a]_n \cdot [b]_n = [a \cdot b]_n
\]

\[\text{e.g.} \quad \text{In } \mathbb{Z}/3\mathbb{Z}, \quad [1] + [1] = [1+1] = [2]
\]

\[
[1] + [2] = [1+2] = [3] = [0]
\]

\[
\]

\[
(6/3 \times 4-1 = 3 \text{ is divisible by } 3)
\]

Then \(+, \cdot\) are comm & assoc on \( \mathbb{Z}/n\mathbb{Z} \).

They have additive identity \([0]\), multiplicative identity \([1]\).

\( \mathbb{Z}/n\mathbb{Z} \) has additive inverses: \(-[a] = [-a] = [n-a].\)
\[ [a] + [n-a] = [a+n-a] = [n] = [0], \text{ the add id.} \]
Thus \[ [n-a] = [a] \text{ & } [a] = -[n-a]. \]

Subtraction in \( \mathbb{Z} \)

Thm c't'd. Distribute over + in \( \mathbb{Z}/n\mathbb{Z} \).
\[
([a]+[b]).[c] = ([a][c]) + ([b][c])
\]

Note. \((R, +, \cdot)\) satisfying these properties is called a commutative ring.

Field = commutative ring in which \( 1 \neq 0 \) and multiplicative inverses of nonzero elts exist.

Is \( \mathbb{Z}/5\mathbb{Z} \) a field? \([0] \neq [1]\) so only have to check multi inverses of nonzero elts, i.e.
For \([a] \in \mathbb{Z}/5\mathbb{Z}\) need \([b] \in \mathbb{Z}/5\mathbb{Z}\) s.t. \([a][b] = [1] \).

<table>
<thead>
<tr>
<th>( \cdot )</th>
<th>([1])</th>
<th>([2])</th>
<th>([3])</th>
<th>([4])</th>
</tr>
</thead>
</table>
\([1]\) & \([1]\) & \([2]\) & \([3]\) & \([4]\) |
\([2]\) & \([2]\) & \([4]\) & \([1]\) & \([3]\) |
\([3]\) & \([3]\) & \([1]\) & \([4]\) & \([2]\) |
\([4]\) & \([4]\) & \([3]\) & \([2]\) & \([1]\) |

\[ 8 \equiv 3 \pmod{5}? \]
\[ 8 \cdot 3 = 5 \text{ a mult. of 5} \checkmark \]
\[ \Rightarrow \mathbb{Z}/5\mathbb{Z} \text{ is a field!} \]
Experiment: Fix a prime $p$.

Take any $[a] \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.

Take powers of $[a]$.

When is $[a]^r = [1]$?

\[ \rightarrow \text{ Fermat's little theorem. FLT } \]