The integers modulo n

The integers modulo n

Formal definition of integers mod n

Definition: Let n be a natural number greater than 1. The set of integers modulo n, written $\mathbb{Z}_n$, is the set of equivalence classes $[a]$ for the equivalence relation defined by congruence modulo n.

Remark: The book gives a careful walkthrough of an example in the case where $n = 5$.

$$\mathbb{Z}_n = \{ [a] \mid a \in \mathbb{Z} \}$$

where $\underline{[a] = \{ x \in \mathbb{Z} \mid x \equiv a \mod n \}}.$

$n = 5 \qquad a = 2$

$[a] = \{ -8, -3, 2, 7, 12, 17, 22, \ldots \}$

Properties of $\mathbb{Z}_n$

Proposition: $\mathbb{Z}_n$ has n elements $\{[0], [1], \ldots, [n-1]\}$.

n = 5				
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
[0]	[1]	[2]	[3]	[4]

$\mathbb{Z}_n$ has n elements.

Proof: Every integer a in $\mathbb{Z}$ can be written in only way as $a = qn + r$ where $0 \le r < n$.

Therefore every integer a is congruent mod n to exactly one r between 0 (inclusive) and $n-1$ (inclusive). $a \equiv r \mod n$, $0 \le r < n$.

On the other hand if $a \equiv j \mod n$, $0 \le j < n$, then $a = kn + j$ so $j = r$ $k = q$.

Arithmetic in $\mathbb{Z}_n$

$[0], [1], \ldots, [4]$

Proposition: Define $[a] + [b] = [a + b]$ and $[a][b] = [ab]$. Then these are *well-defined* operations, meaning that if $[a] = [a']$ and $[b] = [b']$ then $[a] + [b] = [a'] + [b']$, and similarly for multiplication.

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

$[a][b] = [ab]$

mod 5

$[3][2] = [6] = [1]$

$n = 5$

$[2] + [1] = [3]$

$[2] + [3] = [5] = [0]$

$[4] + [3] = [7] = [2]$

$n = 7$

$[0], \ldots, [6]$

$[3] + [2] = [5]$

$[3] = [10]$

$[2] = [-12]$

$[10] + [-12] = [-2]$

$\{\ldots, -9, -2, 5, 12, \ldots\}$

Fix $\overline{n}$. Suppose $[a] = [a']$ $\quad a \equiv a' \bmod n$ so $a = a' + kn$ $\quad k, s \in \mathbb{Z}$.

$[b] = [b']$ $\quad b \equiv b' \bmod n$ so $b = k' + sn$

$[a+b] = [a'+b']$ $\quad a+b = a' + \cancel{b}' + (k+s)n$

so $a+b \equiv a' + b' \bmod n$