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.

$$Z_n = \left\{ \begin{bmatrix} a \end{bmatrix} \mid a \in \mathbb{Z} \right\}$$

where $\begin{bmatrix} a \end{bmatrix} = \left\{ x \in \mathbb{Z} \mid x \equiv a \mod n \right\}$.

$$n = 5 \quad a = 2$$

$$[a] = \{-8, -3, 2, 57, (2, 1), 22, -1\}$$

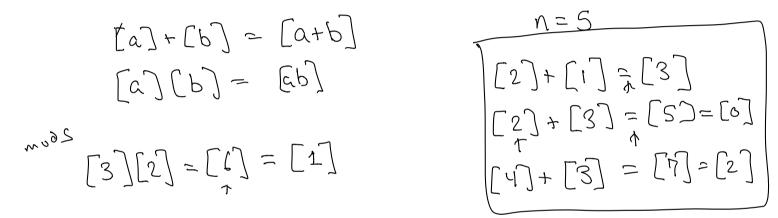
Properties of \mathbb{Z}_n

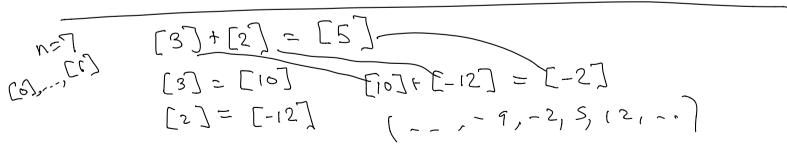
In has n elements. [~] (~] (~] (~) (~) I can be written in only way Proof: Every integerain as a=qn+r where osv<n. Therefore every integer a is congruent mod n to exactly one n between O (inclusive) and N-1 (metusive). a=r modr, o≤r<n. On the other hand of a = j moden, O = j < n, then a = kn + j so $j = r k = q_{f}$.

Arithmetic in \mathbb{Z}_n

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.

[6] [1] ...[4]





Fix suppose
$$[a] = [a']$$
 $a \equiv a' \mod so$ $a \equiv a' + kn$ kise Z.
The suppose $[b] = [b']$ $b \equiv b' \mod so$ $b = k' + sn$
 $[b] = [c'+b']$ $a+b \equiv a'+b' + (k+s)n$
 $[a+b] = [c'+b']$ $a+b \equiv a'+b' \mod n$