

Little Results for Integers Modulo n

Below is our list of “little results” for integers, except I’ve pruned out the ones dealing with \leq (which makes no sense in \mathbb{Z}_n). Which are true for \mathbb{Z}_n ? Why?

Lemma: The additive identity is unique.

Lemma: For any $a \in \mathbb{Z}$, the additive inverse of a is unique.

Lemma: For any $a \in \mathbb{Z}$, $a \times 0 = 0$.

Lemma: For all $a \in \mathbb{Z}$, $-1 \times a = -a$.

Lemma: If $a \times b = 0$, then either $a = 0$ or $b = 0$.

Lemma: If $a \times b = a \times c$ and $a \neq 0$, then $b = c$.

Lemma: The multiplicative identity is unique.

So sometimes the product of two non-zero elements is zero in \mathbb{Z}_n . Another thing about \mathbb{Z}_n which is different from integers is the existence (sometimes) of *multiplicative inverses*.

Example: $[3]_{10} \times [7]_{10} = [1]_{10}$.

Previous results about congruences tell us much about such things.

What does it mean (written in terms of congruences) to say $[a]_n \times [b]_n = [1]_n$? What does it mean to say $[a]_n \times [b]_n = [0]_n$?