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 $n = 5$.

Properties of $\mathbb{Z}_n$

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

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.