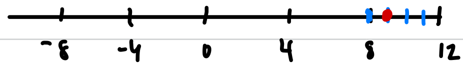
Modular arithmetic : based on division algorithm.

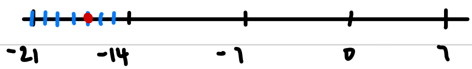
Ex. $9 = 2 \cdot 4 + 1$

so $9 \bmod 4 = 1$



$-17 = -3 \cdot 7 + 4$

So $-17 \bmod 7 = 4$



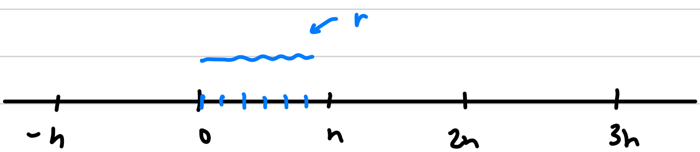
Defn If n is a positive integer and

from division algorithm

$a = qn + r$ where $0 \le r < n$ *

then $a \bmod n = r$.

defn of $a \bmod n$.



Idea: "translate" to segment 0 to $n-1$.

The idea:

If $a \bmod n = b \bmod n$, then a and b are the same from the point of view of divisibility by n.

Important properties:

"if and only if"

1. $a \bmod n = b \bmod n \Leftrightarrow n \mid a-b$.

2. $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$.

Ex $(35+29) \bmod 4 = 64 \bmod 4 = 0$.

"on the other hand" → OTOH $35 \bmod 4 = 3$ $29 \bmod 4 = 1$ $(3+1) \bmod 4 = 0$.

3. $(ab) \bmod n = [(a \bmod n)(b \bmod n)] \bmod n$

Ex $(47 \cdot 19) \bmod 5 = 893 \bmod 5 = 3$.

OTOH $47 \bmod 5 = 2$ $19 \bmod 5 = 4$ $(2 \cdot 4) \bmod 5 = 3$

proof of properties: exercise ← use official defn. to carry out proofs.