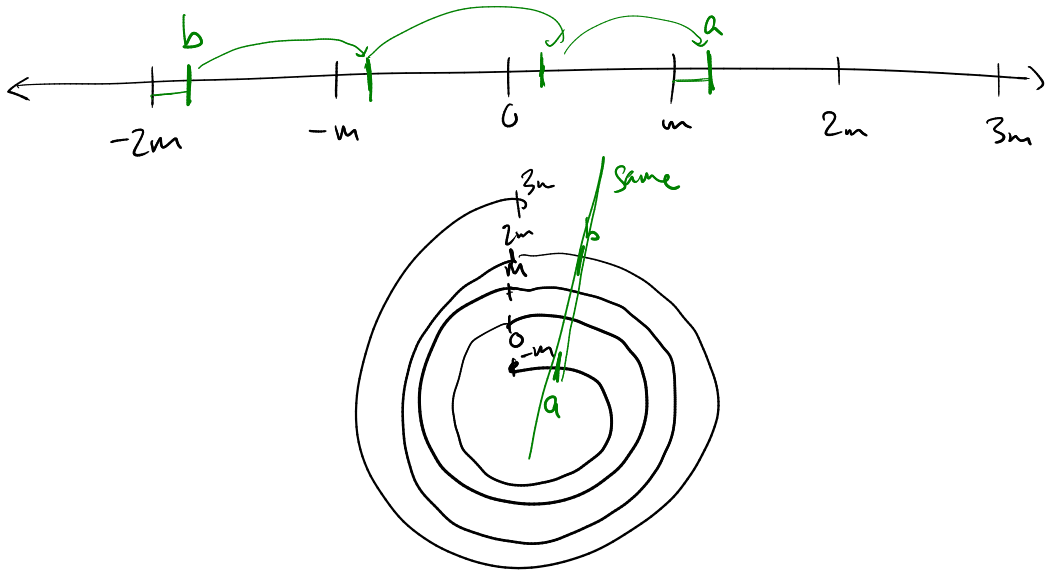
Modular Equivalence

Many situations where we only care about remainder when dividing by something, eg things that go in cycles.



Defn Let $m \in \mathbb{Z}^+$ be a positive integer. Then for integers a and b, we say "a is equivalent to b modulo m", written

$$a \equiv_m b$$

iff $m \mid (a - b)$.

Equivalent definitions:

1. $a \bmod m = b \bmod m$
2. $\exists k.\ a = b + km$

(Note: common notation is $a \equiv b \pmod{m}$.)

Thm. For all $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$$a \equiv_m b \quad \text{iff} \quad \exists k : \mathbb{Z}.\ a = b + km. \leftarrow$$

Prof.

$a \equiv_m b$

$\leftrightarrow$ {defn of $\equiv_m$}

$m \mid (a-b)$

$\leftrightarrow$ {defn of $\mid$}

$\exists k : \mathbb{Z}.\ km = a - b$

$\leftrightarrow$ {algebra}

$\exists k : \mathbb{Z}.\ a = b + km$.

(Note $\leftrightarrow$ is transitive.) ∎

Thm For all $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$$(a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m).$$

Proof

Let a, b, m be arbitrary. We will prove both directions of the $\leftrightarrow$.

($\leftarrow$) Suppose $a \bmod m = b \bmod m$. By the Division Algorithm $a = q_1 m + r_1$ and $b = q_2 m + r_2$; $a \bmod m = b \bmod m$ means $r_1 = r_2$.

$$\begin{aligned} a - b &= (q_1 m + r_1) - (q_2 m + r_2) \\ &= q_1 m - q_2 m \\ &= m(q_1 - q_2) \end{aligned}$$

So by definition, $m \mid (a-b)$, which means $a \equiv_m b$.

($\rightarrow$) Suppose $a \equiv_m b$. Then, by our previous theorem, there exists $k \in \mathbb{Z}$ such that $a = b + km$. By the Div. Alg., $a = q_1 m + r_1$ and $b = q_2 m + r_2$, where $0 \leq r_1, r_2 < m$. We must show $r_1 = r_2$.

$a = b + km$

$\rightarrow$ {subst. for a, b}

$(q_1 m + r_1) = (q_2 m + r_2) + km$

$\rightarrow$ {algebra}

$r_1 - r_2 = q_2 m - q_1 m + km$

$\rightarrow$ {algebra}

$r_1 - r_2 = m(q_2 - q_1 + k)$

$\rightarrow$ {defn of $|$}.

$\rightarrow$ $m \mid (r_1 - r_2)$

Since $0 \leq r_1, r_2 < m$, we can conclude that

$-m < r_1 - r_2 < m$.

The only multiple of m in this range is 0.

Therefore, it must be that $r_1 - r_2 = 0$, i.e. $r_1 = r_2$.

Theorem. $\equiv_m$ is an equivalence relation.

Proof

Reflexive? Yes, $a \bmod m = a \bmod m$

$\longrightarrow a \equiv_m a$.

Symmetric? $a \equiv_m b \leftrightarrow (a \bmod m = b \bmod m)$

$\leftrightarrow (b \bmod m = a \bmod m)$

$\leftrightarrow (b \equiv_m a)$.

Transitive? Yes, inherits transitivity from equality.

Motivation: solving modular equivalences.

$$x + 2 \equiv_7 3.$$

Can we solve this? Turns out yes, subtract 2 from both sides.

BUT!

$$2 \equiv_4 6$$

divide both sides by 2?? $1 \equiv_4 3$ ✗

So, Q: what ops are we allowed to do?