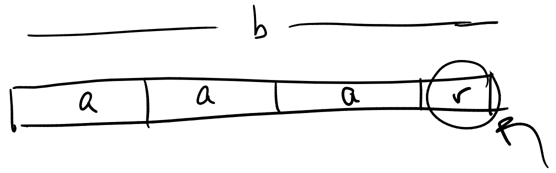
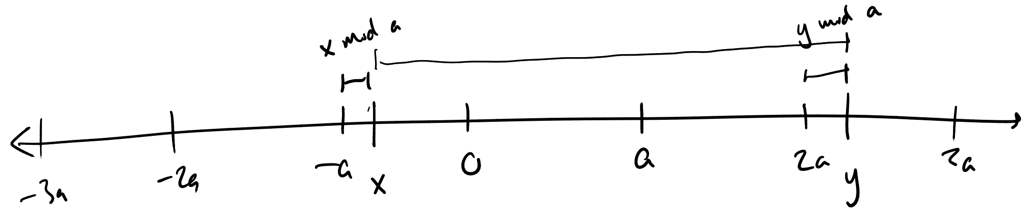
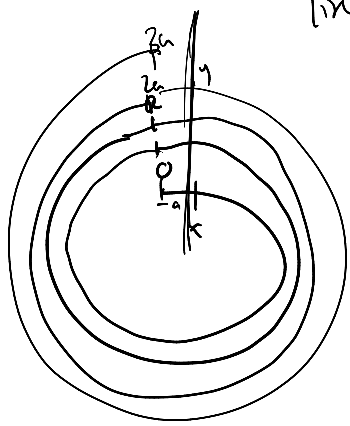
Modular equivalence



Sometimes we only care about remainder



only caring about remainder mod a = wrapping number line into a circle.



Defn If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a is congruent to b modulo m, written

$$a \equiv_m b$$

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

eg. $2 \equiv_3 8$ since $3 \mid (2-8)$. (or since $8 \bmod 3 = 2$.)

(Note: Standard notation is $a \equiv b \pmod m$.)

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

$$(a \equiv_m b) \longleftrightarrow (\exists k \in \mathbb{Z} \,.\, a = b + km).$$

Proof.

$$a \equiv_m b$$

$\longleftrightarrow$ $\{$definition of $\equiv_m\}$

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

$\longleftrightarrow$ $\{$definition of divides relation$\}$

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

$\longleftrightarrow$ $\{$algebra$\}$

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

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

$$(a \equiv_m b) \longleftrightarrow (a \bmod m = b \bmod m)$$

Proof — omitted (see lecture notes).

What properties does the $\equiv_m$ relation have?

- Symmetric? ie. $(a \equiv_m b) \rightarrow (b \equiv_m a)$. ✓
  (Proof: if $m \mid (a-b)$ then $km = a-b$, so $(-k)m = b-a$
  ie. $m \mid (b-a)$.)
- Transitive? ie. $(a \equiv_m b) \wedge (b \equiv_m c) \longrightarrow (a \equiv_m c)$. ✓
- Reflexive? ie. is $a \equiv_m a$? ✓
  ie. does $m \mid (a-a)$? Yes, anything divides 0.

Therefore $\equiv_m$ is an equivalence relation.

Theorem For any $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

if $a \equiv_m b$ and $c \equiv_m d$, then

(i) $a + c \equiv_m b + d$ → Note, subtraction is just adding a negative, that works too.

(ii) $ac \equiv_m bd$.

That is, $\equiv_m$ is a congruence with respect to addition + multiplication.

Proof of (i).

Let a, b, c, d be arbitrary integers and m a positive integer, and suppose $\boxed{a \equiv_m b}$ and $\boxed{c \equiv_m d}$. We will show $\boxed{a + c \equiv_m b + d}$.

By definition, $\boxed{m \mid (a-b)}$ and $\boxed{m \mid (c-d)}$, which means there are integers j and k such that $\boxed{mj = a - b}$ and $\boxed{mk = c - d}$. Adding these equations yields

$$mj + mk = a - b + c - d.$$

$$\rightarrow m(j+k) = (a+c) - (b+d)$$

So by definition $m \mid (a+c) - (b+d)$

which means $a + c \equiv_m b + d$.

Proof of (ii) is similar.

Question: is $\equiv_m$ a congruence w.r.t division?

i.e. if $(a \equiv_m b)$ and $(c \equiv_m d)$, is $(a/c \equiv_m b/d)$?

No! eg. $(2 \equiv_6 8)$ and $(2 \equiv_6 2)$

but $(2/2 \not\equiv_6 8/2)$.