Prove: $\forall n : \mathbb{Z}.\ \neg \text{Even}(n) \leftrightarrow \text{Odd}(n)$.

We will prove $(\rightarrow)$ direction.

Proof: Let n be an arbitrary integer, and suppose $\neg \text{Even}(n)$, that is, there does not exist integer k such that $n = 2k$. We must show n is odd.

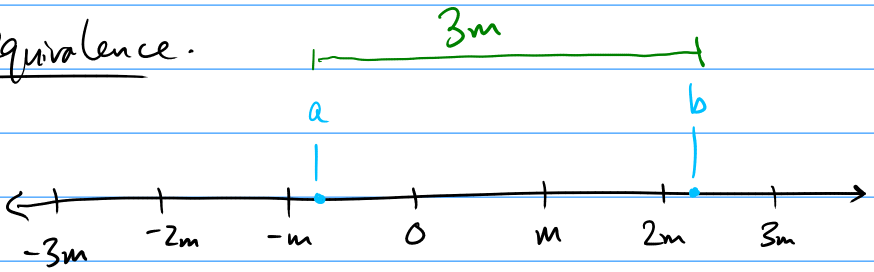
(Idea: n must be odd because even + odd are the only 2 possibilities.)

By the division algorithm, there must exist integers q and r such that $n = 2q + r$ where $0 \leq r < 2$. So $0, 1$ are the only possibilities for r.

- If $r = 0$, then $n = 2q$ so by definition it is even. But we assumed n is not even, so this can't actually happen.
- If $r = 1$, then $n = 2q + 1$, so by definition it is odd, which is what we wanted to show. $\blacksquare$

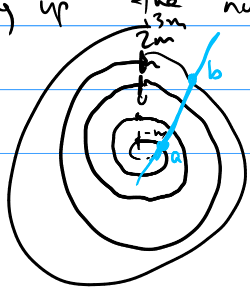
Modular equivalence.

line w/ multiples of m:



Sometimes we want to consider a + b "the same", ie. wrap around at multiples of m.

Think of "wrapping up" the number line: so all multiples of m line up.



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

$$a \equiv_m b$$

if and only if $m \mid (a-b)$. (or $m \mid (b-a)$, doesn't matter)

[Alternatively, it is common to write $a \equiv b \pmod{m}$.]

Does $\equiv_m$ behave like equality $=$?

What properties does $=$ have? What things are we allowed to do with $=$?

- Substitute results of operations, eg. $2+2=x \to 4=x$.
- Do the same operation on both sides, eg. if $x=y$, then $2x+1 = 2y+1$. (congruence)
- Flip the order, eg. if $x=y$ then $y=x$. (symmetric)
- If $a=b$ and $b=c$, then $a=c$. (transitive)
- $a=a$. (reflexive)

Q: which properties does $\equiv_m$ also have?

Thm $\equiv_m$ is reflexive, ie. if $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then

$$a \equiv_m a.$$

Proof. By definition, $a \equiv_m a$ means $m \mid (a-a)$, ie. $m \mid 0$, which is true (everything divides 0).

Thm. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv_m b$ if and only if there exists an integer k such that $a = b + km$.

Proof. $a \equiv_m b$

$\leftrightarrow$ {definition}

$m \mid (a-b)$

$\leftrightarrow$ {definition of divides}

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

$\leftrightarrow$ {algebra}.

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

Thm $\equiv_m$ is transitive, ie. for all $a,b,c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

Proof. Let $a,b,c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Suppose $a \equiv_m b$ and $b \equiv_m c$, that is, by the previous theorem, there exist integers j and k such that $a = b + jm$ and $\underline{b = c + km}$. Then:

a

$=$ {subst}

$b + jm$

$=$ {subst for b}

$(c+km) + jm$

$=$

$c + (k+j)m$

So $a = c + (k+j)m$, so by the same theorem, since a is c plus a multiple of m, $a \equiv_m c$.

Thm. $\equiv_m$ is a congruence with respect to addition, that is if $a \equiv_m b$ and $c \equiv_m d$, then $\underline{a+c \equiv_m b+d}$.

Proof. Let a,b,c,d be arbitrary integers, and m a positive integer. Suppose $a \equiv_m b$ and $c \equiv_m d$, which means $a = b+km$ and $c = d+jm$ for some integers k, j.
Then $a+c = (b+km) + (d+jm) = b+d + (k+j)m$.
Since $a+c$ is $b+d$ plus a multiple of m, $a+c \equiv_m b+d$.

Ex. Solve for x: $x + 7 \equiv_3 12$.

We can subtract 7 (that is, add -7) to both sides

$$x + 7 \equiv_3 12$$

$\leftrightarrow$ { subtract 7 from both sides }

$$x \equiv_3 5$$

So anything equivalent to 5 modulo 3 is a solution:

$$x \in \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}.$$

More simply, $\boxed{x \equiv_3 2}$.

Ex. $27x + 17 \equiv_5 x - 10$. $(x \in \mathbb{Z})$.

$\leftrightarrow$ { sub. 17 }

$27x \equiv_5 x - 27$.

$\leftrightarrow$ { sub. x }

$26x \equiv_5 -27$

$\leftrightarrow$ { $-27 \equiv_5 -2$, $\equiv_5$ is transitive }

$26x \equiv_5 -2$

$\leftrightarrow$ { $26 \equiv_5 1$, therefore $26x \equiv_5 1x$. }

$\boxed{x \equiv_5 -2}$

Ex. $2x + 7 \equiv_7 16$

$\leftrightarrow$ { $7 \equiv_7 0$ }.

$2x \equiv_7 16$

$\leftrightarrow$ { $16 \equiv_7 2$ }.

$2x \equiv_7 2$??? Stuck. Can't divide by 2?