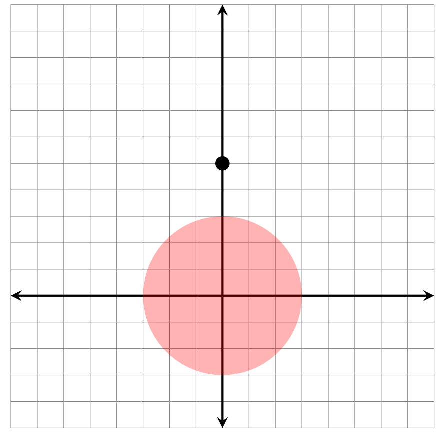
In lecture, we defined the following 2d "robot" transition system.

$$
\begin{aligned}
S &= \mathbb{Z} \times \mathbb{Z} \\
S_0 &= \{(0, 5)\} \\
\rightarrow &= \{((x, y), (x, y + 1)) \mid x, y \in \mathbb{Z}\} \cup \\
&\quad \{((x, y), (x + 1, y - 1)) \mid x, y \in \mathbb{Z}\}
\end{aligned}
$$

We analyzed this system with the safety property

$$P = \{(x, y) \mid x, y \in \mathbb{Z} \land \sqrt{x^2 + y^2} > 3\}$$



Problem 1. Warmup/lecture review

(a) Draw the set of reachable states as a region on the picture above.

(b) Just visually, why does the safety property hold? Use your drawing.

(c) Justify the safety property a bit more formally by giving an inductive invariant. Argue (informally) that no transition "crosses the boundary" from inside your inductive invariant to outside of it.

Problem 2. If we change the initial state to $(0, -5)$, does the safety property still hold? If yes, give a new inductive invariant. If no, give a counterexample to safety.

Problem 3. Consider the original system with initial state $(0, 5)$, but now suppose the transitions are to either take a step west or to take a step southeast. Does the safety property still hold? If yes, give a new inductive invariant. If no, give a counterexample to safety.

Problem 4. Consider the modified west-and-southeast system but now with the initial state $(0, -5)$. Does the safety property still hold? If yes, give a new inductive invariant. If no, give a counterexample to safety.

Problem 5. In the original system, consider changing the initial state to *any* point. For which points is the system safe?

Problem 6. Now consider changing the set of bad states (the red circle). Suppose we add one new bad state at the point $(8, 8)$. The system is now unsafe. What is the shortest execution that leads to a bad state?

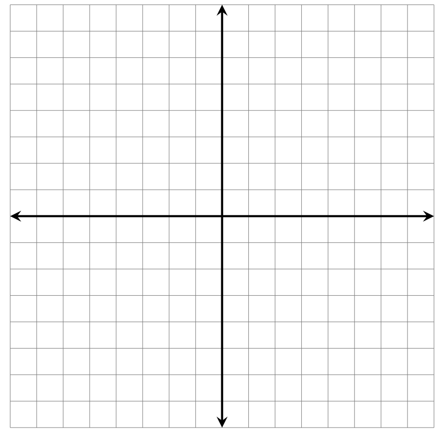
Problem 7. (Optional) Consider this pseudo-liveness claim:

> From any reachable state, there is at least one execution that reaches a point *on* the x-axis.

Is this claim true for this transition system? Why or why not?

Consider the following program

```
n = read_input();
x = 0;
y = n;
while (y != 0) {
  x = x + 1;
  y = y - 1;
}
assert x == n;
```



Given an input n, we can model this program's execution as a transition system:

$$S = \mathbb{Z} \times \mathbb{Z}$$
$$S_0 = \{(0, n)\}$$
$$\rightarrow = \{((x, y), (x + 1, y - 1)) \mid x, y \in \mathbb{Z} \wedge y \neq 0\}$$

The bad states are the ones that cause the assertion to be false. In other words, states where we have exited the loop (i.e., $y = 0$) but $x \neq n$.

Problem 8. Suppose $n = 5$. Draw the bad states as a region on the grid above.

Problem 9. Suppose $n = 5$. Draw the (only) execution of the program on the grid above.

Problem 10. Is the program safe in this execution? Why or why not?

Problem 11. The safety property is not inductive. Give a counterexample to induction (i.e., a state that satisfies the safety property but steps in one step to a state that violates the safety property).

Problem 12. Strengthen the safety property so that it is an inductive invariant. Explain why it is an inductive invariant.

Problem 13. Suppose we change the program to increment both x and y in the loop. Model the new program as a transition system. Is the safety property true?

Problem 14. (Optional) In the original transition system, consider this pseudo-liveness property:

> For any non-negative integer input n, there is an execution of the transition system that reaches a state on the x-axis.

Is this property true? Why or why not?