

# Homework 13

## Circom

Complete the circom exercises in the [repo](#), following the instructions in the README.md files.

You can use the repl tool [zkREPL](#),

---

# Stark Theory

1. Imagine you get the following trace

0,2,4,6,8,10,12

from your program (which simply adds 2 to the previous value.)

Write out the constraints for this trace, in terms of  $i, j$

2. Polynomial practice

for

$$p(x) = x^3 - 5x^2 - 4x + 20$$

a) find an integer root  $a$ , i.e.  $p(a) = 0$  (clue  $< 7$ )

b) write this in terms of a lower degree polynomial  $q(x)$

such as  $p(x) = (x - a)q(x)$

What are the degrees of  $p(x)$  and  $q(x)$  ?

Note we are doing this over the real numbers, for zkps we would use a finite field