ZK Bootcamp: Day 13 Problem Set

Brian Justin Stout*

August 14, 2023

Problem 1. *Complete the circom exercises in the repo.*

Completed.

Problem 2. *Stark Theory: Imagine you have the following trace:*

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

from your program (it adds 2 to the previous value). Write out he constraints for the trace in terms of i and j.

The initial value is zero, so $a_{0,2} = 0$ and the final value is 12 so we have $a_{6,2} = 12$. The amount added each time is 2 so we have $a_{i,1} = 2$ for $i = 1, ..., 6$. Lastly, the adding relationships between the rows for $i = 1, ..., 6$ we have $a_{i,2} - a_{i,1} - a_{i-1,2} = 0$.

Problem 3. *Let the polynomial $p(x) = x^3 - 5x^2 - 4x + 20$. (a) Find an integer root. (b) write p in terms of a lower degree polynomial $q(x)$ such that $p(x) = (x - a)q(x)$. What are the degrees of p and q?*

We have a root at $a = 2$ because $p(2) = 8 - 20 - 8 + 20 = 0$. Using polynomial long division we write $p(x) = (x - 2)(x^2 - 3x - 10)$ so $q(x) = x^2 - 3x - 10$. We see that that the degree of p is 3 and the degree of q is 2, which is one less for the factor of degree 1 which was removed.

*email: bjstout@proton.me