ZK Bootcamp: Day 14 Problem Set

Brian Justin Stout*

August 15, 2023

Problem 1. *Samir Secret Sharing. Create a polynomial with the secret being the constant term a_0, the other values $(a_1, ..., a_4)$ can be chosen at random. Create polynomial of the form:*

$$y(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

I will selet a prime $p = 7297$ and values for $a_1 = 13, a_2 = 45, a_3 = 89, a_4 = 11$ My secret is $S = 1011$. My polynomial is:

$$y(x) = 11x^4 + 89x^3 + 45x^2 + 13x + 1011$$

Problem 2. *Calculate the y values for five x values by evaluating the polynomial. List the shares.*

The following points are on this curve:

$$(1, 1169), (2, 2105), (3, 4749), (4, 2998), (5, 5607)$$

Problem 3. *Reconstruct the polynomial using the shares and an online interpolation calculator and recover the secret.*

Interpolating gives the following polynomial:

$$L(x) = \frac{7429}{12}x^4 - 7209x^3 + \frac{343499}{12}x^2 - 43769x + 22902$$

Evaluating at $x = 0$ gives $L(0) = 22902 = 1011 \bmod(7297)$.

*email: bjstout@proton.me