ZK Bootcamp: Day 1 Problem Set

Brian Justin Stout[*]

July 24, 2023

Problem 1. *Working with the following set of integers* $S = \{0, 1, 2, 3, 4, 5, 6\}$*, compute the following:* $4 + 4$*,* $3 * 5$*,* 3^{-1}

S is the finite field of seven elements, or $\mathbb{F}_7$. Therefore $4 + 4 = 8 = 1 \pmod 7$, $3 * 5 = 15 = 1 \pmod 7$ which also shows that $3^{-1} = 5 \pmod 7$.

Problem 2. *For* $S = \{0, 1, 2, 3, 4, 5, 6\}$ *can we consider* S *and the operationg* $+$ *to be a group?*

Yes, because $S = \mathbb{F}_7$ we know that S is a group under addition and the non-zero elements form a group under multiplication.

Problem 3. *What is* -13 *(mod 5)?*

Adding multiples of the modulus we obtain $-13 = -13 + 15 = 2 \pmod 5$.

Problem 4. *For the polynomial* $p(x) = x^3 - x^2 + 4x - 12$ *find the positive root* a*. What is the degree of this polynomial?*

The degree of the polynomial is 3, the largest power of x. A positive root for this polynomial is $x = 2$ because $2^3 - 2^2 + 4 * 2 - 12 = 8 - 4 + 8 - 12 = 0$. Therefore the polynomial factors as $(x - 2)(x^2 + x + 6)$.

[*] email: bstout.eth@ethermail.io