Zero Knowledge Proofs: Homework 1

Meek Msaki (Meek#6464)

February 9, 2023

Question 1

$S = \mathbb{Z}_7$

a) $4 + 4 \equiv 1 \mod 7$

b) $3 \cdot 5 \equiv 1 \mod 7$

c) $3^{-1} \equiv 3^{7-2} \mod 7 \equiv 243 \mod 7 \equiv 5 \mod 7$. Verify $3 \cdot 5 \mod 7 \equiv 1 \mod 7$. Using Fermat's little theorem, answer is 5.

Question 2

Answer is Yes. $(\mathbb{Z}_7, +)$ is a group, it has a set of elements $0, 1, 2, 3, 4, 5, 6$ plus an operator $+$.

1. It is closed. For all $a, b \in \mathbb{Z}_7$, the results of the operation is also in $\mathbb{Z}_7$.
2. Associativity, for all $a, b, c \in \mathbb{Z}_7$ it's operation can be performed in any order $(a + b) + c = a + (b + c)$.
3. There exists an identity element e, where for each element $a \in \mathbb{Z}_7$, $a + e = e + a = a$, where the identity element $e = 0$.
4. There exists an inverse $-a$, for $a \in \mathbb{Z}_7$, such that $a + (-a) = (-a) + a = e$, where e is our identity element $e = 0$.

Question 3

$-13 \mod 5 \equiv 2 \mod 5$. Answer is 2.

Question 4

We can simplify our function $f(x) = x^3 - x^2 + 4x - 12$ to factors $f(x) = (x-2) \cdot (x^2 + x + 6)$

Using Polynomial Remainder Theorem $\frac{P(x)}{x-a} \rightarrow r = P(a)$ where $P(x) = x^3 - x^2 + 4x - 12$. If we divided $P(x)$ with a first degree polynomial $(x-a)$, and we don't get a remainder $r = 0$, this verifies $(x-a)$ is a valid factor of our polynomial $P(x)$. We can solve this with our factor $(x-2)$ for $P(a)$. When $x = 2$, $P(2) = 2^3 - 2^2 + 4 \cdot 2 - 12 = 0$. Solving for x using $(x-2) = 0$ or $(x^2 + x + 6) = 0$. Answer is 2. The degree of this polynomial is 3.

See: Remainder theorem: checking factors