CSEC 519: Blockchain and Cryptocurrency Technologies
Homework 1
Deadline 27 April 2023 09:30
NO LATE SUBMISSIONS !!!!!!

1. (10 Points) Is $(\mathbb{Z}_8^*, \cdot)$ a group? If it is, show that it satisfies every group axiom. If it is not, provide a counter-example that contradicts one of the group axioms.

2. (10 Points) Provide a generator for $(\mathbb{Z}_{13}^*, \cdot)$, show that it generates every element in $\mathbb{Z}_{13}^*$.

3. (10 Points) Is $E : y^2 = x^3 + x + 3$ defined over $\mathbb{F}_{13}$ an elliptic curve? Justify your answer.

4. (30 Points) Find every point of the elliptic curve $E : y^2 = x^3 + x + 2$ defined over $\mathbb{F}_{13}$. How many points does it have? You can use any programming language to solve this problem but you are **NOT** allowed to include any library (e.g. libraries related to finite fields, elliptic curves etc.). DO NOT FORGET to submit your codes with your homework.

5. (40 Points) Find a generator for the elliptic curve $E : y^2 = x^3 + x + 2$ defined over $\mathbb{F}_{13}$. Show that repeatedly adding that point generates every point on the curve (and also the point at infinity). You can use any programming language to solve this problem but you are **NOT** allowed to include any library (e.g. libraries related to finite fields, elliptic curves etc.). DO NOT FORGET to submit your codes with your homework.