MA503: Homework 11

Exercise 11.1. [2pts] Consider an elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + x + 3$ over $\mathbb{Z}_{13}$. Is it singular?

Exercise 11.2. [10pts] Find all points on the elliptic curve $\mathcal{E}$ defined by $y^2 = x^3 + 2x + 3$ over $\mathbb{Z}_{13}$. You can proceed like in class: for each value $x \in \mathbb{Z}_{13}$ find solutions of $y^2 = x^3 + 2x + 3$. (The table of square roots modulo 13 on page 10 of lecture 6 can be useful).

Exercise 11.3. [10pts] For the curve $\mathcal{E}$ from the previous problem compute

(a) $(4, 7) + (9, 10)$,
(b) $(4, 7) + (4, 7)$.

Please, show computations (at least show the value of the slope λ).

Exercise 11.4. [10pts] Consider the curve $\mathcal{E}$ defined on page 10 of lecture 11. Use the addition table on page 11 to compute the order and the cyclic subgroup generated by each of the following points:

(a) $(1, 5)$,
(b) $(9, 6)$,
(c) $(12, 2)$.