Upload to Canvas before Apr/20, 6:00pm

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?

Solution: Here $a = 1$ and $b = 3$. Hence, $4a^3 + 27b^2$ produces

$$4a^3 + 27b^2 = 4 + 27 \cdot 9 \equiv_{13} 4 + 9 = 13 \equiv_{13} 0.$$

Therefore, the curve is 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).

Solution:
$\mathcal{E} = \{\mathcal{O}, (0,4), (0,9), (3,6), (3,7), (4,6), (4,7), (6,6), (6,7), (7,3), (7,10), (9,3), (9,10), (11,2), (11,11), (12,0)\}$ □

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).

Solution: To compute $(4,7) + (9,10)$ we compute the following:

- $\lambda = \frac{10-7}{9-4} = \frac{3}{5} \equiv_{13} \frac{-10}{5} \equiv_{13} -2 \equiv_{13} 11.$
- $x_3 = \lambda^2 - x_1 - x_2 = 121 - 4 - 9 \equiv_{13} 4.$
- $y_3 = \lambda(x_1 - x_3) - y_1 = 11(4 - 4) - 7 \equiv_{13} 6.$
- Hence, $(4,7) + (9,10) = (4,6)$.

To compute $(4,7) + (4,7)$ we compute the following:

- $\lambda = \frac{3 \cdot 4^2 + 2}{2 \cdot 7} = \frac{50}{14} = \frac{25}{7} = \frac{4}{7} \equiv_{13} \frac{77}{7} = 11.$
- $x_3 = \lambda^2 - x_1 - x_2 = 121 - 4 - 4 \equiv_{13} 9.$
- $y_3 = \lambda(x_1 - x_3) - y_1 = 11(4 - 9) - 7 \equiv_{13} 3.$
- Hence, $(4,7) + (4,7) = (9,3)$.

□

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) $(12,2)$.

Solution:

(a) Enumerate multiples of $(1,5)$ one by one using the table:

$$\langle(1,5)\rangle = \{\mathcal{O}, (1,5), (2,10), (9,7), (12,2), (12,11), (9,6), (2,3), (1,8)\}$$

Hence, $|(1,5)| = 9$.

(b) Enumerate multiples of $(9,6)$ one by one using the table:

$$\langle(9,6)\rangle = \{\mathcal{O}, (9,6), (9,7)\}.$$

Hence, $|(9,6)| = 3$.

(c) Enumerate multiples of $(12,2)$ one by one using the table:

$$\langle(12,2)\rangle = \{\mathcal{O}, (12,2), (1,8), (9,7), (2,3), (2,10), (9,6), (1,5), (12,11)\}.$$

Hence, $|(12,2)| = 9$.

□