University Center of Mila
Department of Mathematics

2023/2024
M2-S03

Elliptic Curves
Work Sheet 02

Exercise 1. Let $E/\mathbb{Q} : y^2 = x^3 + Ax + B. \quad A, B \in \mathbb{Z}$ be an (EC) over $\mathbb{Q}$.

① Suppose $P = (p_1, p_2), Q = (q_1, q_2) \in E(\mathbb{Q})$. Find the rationale points $P + Q, 2P$, and $-P$.

② Write $\hat{E}$ the (WF) of E in homogeneous coordinates (i.e. in $\mathbb{P}^2(\mathbb{Q})$).

Exercise 2. Let $E/\mathbb{Q} : y^2 = x^3 + 1$ an (EC) over $\mathbb{Q}$, and let $P = (2, 3)$.

① Prove that $P \in E/\mathbb{Q}$.

② Calculate in $E(\mathbb{Q})$ the points $nP, n \geqslant 2$.

Exercise 3. Soit $E/\mathbb{F}_{23} : y^2 = x^3 + x + 1$ an (EC) over $\mathbb{F}_{23}$.

① Find all the points of $E(\mathbb{F}_{23})$.

② Let $P = (9, 7), Q = (3, 10)$ be tow points of $\mathbb{F}_{23}$. Calculate $P + Q, 2Q$.

Exercise 4. Let $\mathbb{F}_{2^4}$ be the quotient field $\mathbb{F}_2[X]/ < x^4 + x + 1 >$. Suppose every elements of $\mathbb{F}_{2^4}$ is a power of g. And let $E/\mathbb{F}_{2^4}$ be an (EC) given by

$$y^2 + xy = x^3 + g^4x^2 + 1.$$

① Find all the points of $E(\mathbb{F}_{2^4})$.

② Suppose $P = (g^6, g^8), Q = (g^3, g^{13})$, calculate $P + Q, and\ 2P$.