

Courbes elliptiques

TD 02

Exercice 1. Soit $E/\mathbb{Q} : y^2 + 43xy - 210y = x^3 - 210x^2$. Trouver un changement de variables inversible qui transforme E vers la (FW): $y^2 = x^3 + Ax + B$.

Exercice 2. Soit $(E, \mathcal{O}) : y^2 = x^3 + Ax + B$. $A, B \in \mathbb{Z}$ une (CE) sur $\mathbb{Q}$.

- ① Soient $P = (p_1, p_2), Q = (q_1, q_2) \in E(\mathbb{Q})$. Trouvez les points rationnels $P + Q, 2P$, et $-P$.
- ② Trouvez $\hat{E}$ la (FW) de E dans les coordonnées homogènes (i.e. dans $\mathbb{P}^2(\mathbb{Q})$).
- ③ Soit $L : y = ax + b$ une droite. Montrez que si L coupe E en 2 points, alors L coupe E en 3^{ème} point.

Exercice 3. Soit $(E, \mathcal{O}) : y^2 = x^3 + 1$ une (CE) sur $\mathbb{Q}$, et soit $P = (2, 3)$.

- ① Montrez que $P \in E/\mathbb{Q}$.
- ② Calculer dans $E(\mathbb{Q})$ les points $nP, n \geq 2$.

Exercice 4. Soit $(E, \mathcal{O}) : y^2 = x^3 + x + 1$ une (CE) sur $\mathbb{F}_{23}$.

- ① Trouvez tous les points de $E(\mathbb{F}_{23})$.
- ② Soient $P = (9, 7), Q = (3, 10)$, calculer $P + Q, 2Q$.

Exercice 5. Soient le corps $\mathbb{F}_{24}$ généré par la racine α du polynôme irréductible $x^4 + x + 1$ sur $\mathbb{F}_2$, et la (CE) sur $\mathbb{F}_{24}$ définie par

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

- ① Trouvez tous les points de $E(\mathbb{F}_{24})$.
- ② Soient $P = (\alpha^6, \alpha^8), Q = (\alpha^3, \alpha^{13})$, calculer $P + Q$, et $2P$.