TD3 : structure de groupe et torsion

Exercice 1. Déterminer des formules pour la loi de groupe sur la courbe elliptique $y^2 = x^3 - x$.

Exercice 2. On considère la courbe elliptique $y^2 = x^3 + x + 1$ sur $\mathbb{F}_5$. Montrer quelle possède neuf points. Quelle est la structure de groupe de $E(\mathbb{F}_5)$?

Exercice 3. Déterminer tous les points sur $\mathbb{F}_5$ de la courbe elliptique $E : y^2 = x^3 + 4x + 1$. Quelle est la structure du groupe $E(\mathbb{F}_5)$?

Exercice 4. On considère la cubique $y^2 = x^3 + x + 3$. Pour quels p cette cubique définit-elle une courbe elliptique ? Déterminer la structure de groupe de $E(\mathbb{F}_5)$ et $E(\mathbb{F}_7)$ ainsi que des générateurs.

Exercice 5. Soit E la courbe elliptique sur $\mathbb{F}_7$ d'équation $y^2 = x^3 + 2$. Déterminer la structure de groupe de $E(\mathbb{F}_7)$.

Exercice 6. On considère, sur le corps $\mathbb{F}_5$, la cubique plane E d'équation $Y^2Z = X^3 - XZ^2 + Z^3$.

1. Montrer que E est une courbe elliptique sur $\mathbb{F}_5$.
2. Décrire l'ensemble $E(\mathbb{F}_5)$.
3. Déterminer la classe d'isomorphisme du groupe $E(\mathbb{F}_5)$.
4. Déterminer la fonction zêta de E sur $\mathbb{F}_5$.
5. Combien y a-t-il de points sur $\mathbb{F}_{25}$?
6. Montrer que $E[2] \subseteq E(\mathbb{F}_{25})$.
7. En déduire que $E(\mathbb{F}_{25})$ n'est pas un groupe cyclique.
8. En admettant qu'il existe un point d'ordre quatre de E non défini sur $\mathbb{F}_{25}$, en déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{25})$.

Exercice 7. Une courbe elliptique sur $\mathbb{F}_{p^r}$ peut-être avoir un nombre de points qui est un nombre premier ? Y a-t-il des conditions sur p, sur r ? Chercher des exemples.