TP : courbes elliptiques

Ce TP propose de découvrir quelques manipulations élémentaires de courbes elliptiques avec le logiciel SageMath [1].

Premiers pas

1. Consulter l'aide de la commande `EllipticCurve`. Définir la courbe elliptique E d'équation $y^2 = x^3 + x^2 - x$ sur le corps $\mathbb{Q}$.
2. Tracer le graphe de la courbe E dans le plan (utiliser la commande `plot`).
3. Consulter la documentation de SageMath sur les courbes elliptiques. Définir un point P de votre choix dans $E(\mathbb{Q})$.
4. Représenter P et E sur le même dessin (la commande `+` permet de les superposer).

Courbes elliptiques sur un corps fini

1. Définir la courbe elliptique E d'équation $y^2 = x^3 + x + 1$ sur le corps fini $\mathbb{F}_5$.
2. Grâce à l'aide contextuelle (touche TAB après le nom de l'objet suivi d'un point), calculer le discriminant de E.
3. Calculer l'ensemble $E(\mathbb{F}_5)$ des points de E (regarder la commande `.points`).
4. SageMath permet d'additionner des points sur une courbe elliptique grâce à la commande `+`. Vérifier à l'aide de SageMath que $(E(\mathbb{F}_5), +)$ vérifie bien les axiomes d'un groupe commutatif.
5. Calculer l'ordre de chacun des points de $E(\mathbb{F}_5)$ et la structure de groupe sur $E(\mathbb{F}_5)$ (regarder la commande `.abelian_group`).
6. Pour chacune des équations suivantes :
   (a) $y^2 = x^3 + 2x$
   (b) $y^2 = x^3 + 2x + 1$
   (c) $y^2 = x^3 + 2$

   vérifier que ce sont des équations de courbes elliptiques sur $\mathbb{F}_5$. Pour chacune de ces courbes, déterminer le groupe $E(\mathbb{F}_5)$ et discuter la structure.
7. Trouver 5 courbes elliptiques sur $\mathbb{F}_5$ telles que $\#E(\mathbb{F}_5)$ vaut respectivement $2, 3, 5, 7, 8$.
8. Revenons à la courbe d'équation $y^2 = x^3 + x + 1$ sur $\mathbb{F}_5$. Sans utiliser la commande `.points`, déterminer à l'aide de SageMath et par une méthode naïve l'ensemble des points $E(\mathbb{F}_5)$. Comparer ce résultat à celui obtenu par SageMath.
   Même question pour la courbe elliptique sur le corps $\mathbb{F}_{3571}$ définie par $y^2 = x^3 + x + 2$.
9. Trouver exactement 11 équations de Weierstrass semi-généralisées sur $\mathbb{F}_3$ qui sont deux à deux non équivalentes. Pour chacune, déterminer le groupe $E(\mathbb{F}_3)$.

1. Téléchargeable à l'adresse `https://www.sagemath.org/`