TP1 - Courbes elliptiques et diviseurs

Magma est un logiciel de calcul formel destiné à résoudre des problèmes d'algèbre, de géométrie algébrique et de combinatoire. Ce logiciel accessible via un terminal dans les salles info. Vous pouvez également lancer des sessions en ligne à l'adresse

`http://magma.maths.usyd.edu.au/calc/`.

Vous pouvez (devez) accéder à l'aide en ligne à l'adresse

`http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`

(ou en tapant **magma help** sur un moteur de recherche). Si vous n'avez jamais pratiqué magma, lisez le fichier **First Steps in Magma** disponible dans la rubrique Documents du site de la formation (vous pouvez aussi consulter les tutoriels de D. Kohel ou de S. Pauli). N'hésitez pas à faire des petits essais pour mettre en pratique cette lecture un peu fastidieuse.

Exercice 1.

1. Définir la courbe elliptique $E\colon y^2 = x^3 + x^2 + 1$ sur $\mathbb{Q}$.
2. Calculer son discriminant.
3. Calculer son j-invariant.
4. On considère E' sur $\mathbb{Q}$ définie par

$$E'\colon y^2 = x^3 + \frac{3j(E)}{1728 - j(E)}x + \frac{2j(E)}{1728 - j(E)}.$$

   (a) Vérifier que E et E' sont isomorphes sur $\overline{\mathbb{Q}}$.

   (b) Vérifier que E et E' ne sont pas isomorphes sur $\mathbb{Q}$.

Exercice 2.

(A) Reprendre l'Exercice 3 du TD1 et faites toutes les questions à l'aide de Magma.

(B) Les courbes E et E' sont-elles isomorphes sur $\mathbb{F}_{25}$?

(C) Vérifier les formules données dans l'Exercice 4 sont correctes pour la courbe E.

Exercice 3.

1. Définir la courbe $E\colon y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_{23}$.
2. Calculer le cardinal de $E(\mathbb{F}_{23})$.
3. Vérifier que $P = (2, 17)$ et $Q = (9, 9)$ sont deux points de E et calculer $P + Q$.
4. Déterminer l'ordre de P dans $E(\mathbb{F}_{23})$. Que peut-on en déduire sur la structure du groupe $(E(\mathbb{F}_{23}), +)$?
5. Déterminer toutes les courbes elliptiques (à isomorphisme près) sur $\mathbb{F}_{23}$ isomorphes à E sur $\overline{\mathbb{F}_{23}}$ mais pas sur $\mathbb{F}_{23}$ (en anglais *tordues* se dit *twists*).
6. Déterminer toutes les courbes elliptiques (à isomorphisme près) sur $\mathbb{F}_{23}$ qui ont le même nombre de points que E.