DM - Courbes elliptiques - Les a-miroirs

Dans toute la composition on pourra citer librement le cours ainsi que toute connaissance des cours précédents. En particulier, il est vivement recommandé de revoir le cours de M1 que vous avez suivi sur le symbole de Legendre et les lois de réciprocité quadratique (l'essentiel de ce qu'il faut savoir est rappelé en Appendice du polycopié de cours en ligne sur Moodle). Par ailleurs, tous les résultats énoncés dans les TD peuvent être utilisés librement (qu'ils aient été faits ou non en TD). Enfin, à moins que ça ne soit explicitement précisé (i.e. la question 1.5.c), une commande Magma ne suffira pas pour répondre à une question. Il est toutefois recommandé d'utiliser Magma pour guider votre réflexion et votre intuition sur votre brouillon.

Ce devoir maison est à rendre pour le **09/11**, il pourra être fait seul, à deux ou à trois (s'il est fait à plusieurs une seule copie comportant tous les noms pourra être rendue).

Introdution

Soit $q = p^s$ avec p **impair**. On pose $S_q = \left\{x^2, x \in \mathbb{F}_q \setminus \{0\}\right\}$ l'ensemble des carrés non-nuls de $\mathbb{F}_q$. Soit $a \in \mathbb{F}_q \setminus \{0\}$, on dit qu'un élément $x \in S_q$ est un a-miroir si $x - a \in S_q$ et $x + a \in S_q$. On pose $M(a) = \{x \in S_q, a\text{-miroir}\}$, l'ensemble des a-miroirs et $m(a) = \#M(a)$. L'objectif de ce devoir est de montrer que lorsque $q = -1 \mod 4$ alors pour tout $a, b \in \mathbb{F}_q \setminus \{0\}, m(a) = m(b)$. Enfin, dans ces cas là, nous déterminerons $m(a)$ explicitement en fonction de q. Dans tout le DM a désignera un élément non-nul de $\mathbb{F}_q$.

1 Quelques exemples

1. Montrer que le cardinal de S_q est $\frac{q-1}{2}$. Montrer que -1 est un carré dans $\mathbb{F}_q$ si, et seulement si $q = 1 \mod 4$. Montrer que 2 est un carré si, et seulement si $q^2 = 1 \mod 16$.
2. Énumérer les carrés non nuls de $\mathbb{F}_7$. Montrer que $\mathbb{F}_7$ ne contient aucun a-miroir pour $a \in \mathbb{F}_7 \setminus \{0\}$.
3. Énumérer les carrés non nuls de $\mathbb{F}_{11}$. Montrer que $\mathbb{F}_{11}$ contient exactement un a-miroir pour tout $a \in \mathbb{F}_{11} \setminus \{0\}$.
4. Énumérer les carrés non nuls de $\mathbb{F}_{13}$. Montrer que $\mathbb{F}_{13}$ ne possède pas de 1-miroir mais qu'il a des 2-miroirs.
5. (a) Montrer que le polynôme $X^3 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$. On pose $\mathbb{F}_{27} = \mathbb{F}_3[\alpha] = \mathbb{F}_3[X]/\left\langle X^3 - X - 1\right\rangle$ (α est la classe de X dans le quotient).
   (b) Montrer que $\alpha^4 = \alpha^2 + \alpha$ et $\alpha^{10} = \alpha^2 - \alpha$. En déduire que α^2 est un α-miroir.
   (c) À l'aide de Magma, donner le nombre de a-miroir pour chaque $a \in \mathbb{F}_{27}$.

2 Étude des courbes C_a

On pose $C_a(\mathbb{F}_q)$ le sous-ensemble de $\mathbb{P}^3(\mathbb{F}_q)$ des éléments $[x_0 : x_1 : x_2 : z]$ tels que

$$\begin{cases} x_1^2 = x_0^2 + az^2 \\ x_2^2 = x_0^2 - az^2. \end{cases}$$

1. Montrer que chaque a-miroir correspond à 8 éléments de C_a de la forme $[x_0 : x_1 : x_2 : 1]$ avec $x_i \neq 0$.
2. Supposons $q = 3 \mod 4$. Montrer que 2 est un carré dans $\mathbb{F}_q$ si, et seulement si, C_a possède exactement 4 éléments $[x_0 : x_1 : x_2 : 1]$ avec l'un des x_i nul.
3. En déduire que lorsque $q = 3 \mod 4$ on a $\#C_a(\mathbb{F}_q) = 8m(a) + 4 + 4\delta_2$ où $\delta_2 = 1$ si 2 est un carré dans $\mathbb{F}_q$ et 0 sinon.

On considère la courbe elliptique $E_a : y^2 = x(x-a)(x+a)$. On **admettra** que les applications ϕ_a et ψ_a sont des bijections réciproques (leur expression est donnée à titre indicatif uniquement. Cela n'a aucune importance pour la suite de l'exercice).

$$\begin{array}{rccl} \phi_a : & C_a(\mathbb{F}_q) & \longrightarrow & E_a(\mathbb{F}_q) \\ & [x_0 : x_1 : x_2 : z] & \longmapsto & [x_0x_1z - x_0x_2z - x_1x_2z + x_2^2z + az^3 : \\ & & & -2x_0x_1x_2 + 2x_0x_2^2 + 2ax_0z^2 + 2x_1x_2^2 + ax_1z^2 - 2x_2^3 - 3ax_2z^2 : z^3]. \end{array}$$

et

$$\begin{array}{rccl} \psi_a : & E_a(\mathbb{F}_q) & \longrightarrow & C_a(\mathbb{F}_q) \\ & [x : y : z] & \longmapsto & [\frac{1}{2}x^2y + \frac{a^2}{2}yz^2 : \frac{1}{2}x^2y + axyz - \frac{a^2}{2}yz^2 : -\frac{1}{2}x^2y + axyz + \frac{a^2}{2}yz^2 : \\ & & & x^3 - a^2xz^2]. \end{array}$$

3 Étude des courbes E_a

1. Justifier le fait que E_a est une courbe elliptique pour $a \in \mathbb{F}_q \setminus \{0\}$ (i.e. que la cubique est lisse).
2. Montrer que $j(E_a) = 2^6 3^3$. Les courbes E_a et E_b sont-elles isomorphes sur $\overline{\mathbb{F}_q}$ pour $a, b \in \mathbb{F}_q \setminus \{0\}$?
3. On fixe $a, b \in \mathbb{F}_q \setminus \{0\}$. On cherche à expliciter des isomorphismes entre $E_a : y^2 = x(x-a)(x+a)$ et $E_b : Y^2 = X(X-b)(X+b)$.
   (a) On pose les applications

$$\begin{array}{rcl} E_a & \longrightarrow & E_b \\ (x,y) & \longmapsto & \left(\frac{b}{a}x, \sqrt{\frac{b}{a}}^3 y\right) \end{array} \quad \text{et} \quad \begin{array}{rcl} E_a & \longrightarrow & E_b \\ (x,y) & \longmapsto & \left(\frac{-b}{a}x, \sqrt{\frac{-b}{a}}^3 y\right) \end{array}$$

   où $\sqrt{\frac{b}{a}}$ (resp. $\sqrt{\frac{-b}{a}}$) est une racine de $\frac{b}{a}$ (resp. de $\frac{-b}{a}$) dans $\overline{\mathbb{F}_q}$. Montrer qu'elles définissent des isomorphismes entre E_a et E_b sur $\mathbb{F}_q\left(\sqrt{\frac{b}{a}}\right)$ et $\mathbb{F}_q\left(\sqrt{\frac{-b}{a}}\right)$ respectivement.
   (b) En déduire que si -1 n'est pas un carré alors E_a et E_b sont isomorphes sur $\mathbb{F}_q$.
   (c) En déduire que $m(a) = m(b)$ lorsque $q = -1 \mod 4$ et que, pour q quelconque, m ne peut prendre que deux valeurs distinctes au plus sur $\mathbb{F}_q \setminus \{0\}$.

4 Calcul explicite de $m(a)$ lorsque $q = -1 \mod 4$

On suppose que $q = -1 \mod 4$.

1. Montrer que
$$\sum_{x \in \mathbb{F}_q} \left(\frac{x(x-a)(x+a)}{q}\right) = 0$$
   (On pourra remarquer que $x \mapsto -x$ est une bijection de $\mathbb{F}_q$).
2. En déduire que $\#E(\mathbb{F}_q) = q + 1$ et que $m(a) = \frac{q+1-4-4\delta_2}{8}$.
3. Montrer que pour tout carré non nul de $\mathbb{F}_{3^9}$ possède exactement 2460 a-miroirs pour tout $a \in \mathbb{F}_{3^9} \setminus \{0\}$ (on a $3^9 = 19683$).