TD3 TANC - Nombre de points des courbes elliptiques sur les corps finis

Exercice 1 (Méthode CM)**.** Trouver une courbe elliptique E définie sur $\mathbb{F}_{11}$ avec $N = 10$ points rationnels. On donne

$$H(X) = H_{\mathbb{Z}[\sqrt{-10}]}(X) = X^2 - 425692800X + 9103145472000 \in \mathbb{Z}[X].$$

Exercice 2 (Algorithme de Schoof)**.** On considère la courbe $E\colon y^2 = x^3 - 4x - 1 = f(x)$ sur $\mathbb{F}_{13}$. On note a sa trace et $\pi(x, y) = (x^{13}, y^{13})$ son morphisme de Frobenius.

1. Justifier qu'il suffit de connaître $a \mod \ell$ pour $\ell = 2, 3, 5$ pour en déduire a.
2. Montrer que $f(5) = 0$. En déduire que $a = 0 \mod 2$.
3. Montrer que le point $P = (-4, 4)$ est un point de E et calculer l'abscisse de $2 \cdot P$.
4. En déduire que P est un point de 3 torsion. Que peut-on en déduire sur $a \mod 3$?
5. Montrer que 2 n'est pas un carré dans $\mathbb{F}_{13}$. On pose alors $K = \mathbb{F}_{13^2} = \mathbb{F}_{13}[X]/\left\langle X^2 - 2\right\rangle$ et $\alpha \in \mathbb{F}_{13}$ tel que $\alpha^2 = 2$ (i.e. α est une racine de 2 dans K). On considère $Q = (-1, \alpha)$.
   (a) Montrer que $Q \in E(K)$. On **admet** que Q est d'ordre 5.
   (b) Que valent $\pi(Q)$ et $\pi^2(Q) = \pi(\pi(Q))$?
   (c) Montrer que $\pi(Q) = \pi^2(Q) - 2 \cdot Q$.
   (d) En déduire $a \mod 5$.
6. En déduire la trace de E.