TD6 - Courbes elliptiques en caractéristique 2

Exercice 1. On pose $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ où α est la classe de X dans le quotient $\mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$. On considère alors

$$E\colon y^2 + xy = x^3 + x^2 + 1.$$

1. Vérifier que $X^3 + X + 1 \in \mathbb{F}_2[X]$ est bien irréductible.
2. Trouver un point d'ordre de 2 sur E. Que peut-on en déduire sur $\#E(\mathbb{F}_8)$?
3. Énumérer tous les points de $E(\mathbb{F}_8)$ à coordonnées dans $\mathbb{F}_2$.
4. Montrer que le point $P = (\alpha^2 + 1, \alpha^2 + 1)$ appartient à E.
5. Calculer $8P$ à l'aide des coordonnées de Lopez-Dahab.
6. En déduire la valeur de $\#E(\mathbb{F}_8)$.
7. Donner le développement τ-adique de 7 dans l'anneau $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \simeq \mathbb{Z}[\tau]$ où $\tau(x, y) = (x^2, y^2)$ est le Frobenius sur E identifié avec $\frac{1+\sqrt{-7}}{2}$ (on rappelle que τ satisfait $\tau^2 - \tau + 2 = 0$).
8. Montrer que pour tout point $Q \in E(\mathbb{F}_8)$ on a $\tau^2(Q) + \tau(Q) + Q = 7Q$.
9. En déduire que pour tout point $Q \in E(\mathbb{F}_8)$, $7Q$ est à coordonnées dans $\mathbb{F}_2$ et retrouver le résultat de la question 6.

Exercice 2. On considère $E\colon y^2 + xy = x^3 + x^2 + 1$ définie sur $\mathbb{F}_{2^{163}}$. On admet que $\#E(\mathbb{F}_{2^{163}}) = 2p$ avec p un nombre premier de 162 bits.

1. Montrer que le groupe $E(\mathbb{F}_{2^{163}})$ et cyclique.
2. Montrer que E est une courbe bonne pour la cryptographie. Quel est son niveau de sécurité ?
3. Expliquer comment trouver un point d'ordre p sur E.