Travail préparatoire au DS

Exercice 1
Soit E la courbe elliptique définie sur $\mathbb{F}_{61}$ par les coefficients

$$E = [0, 1, 1, -3, 1]$$

1. Quelle est la structure de $E(\mathbb{F}_{61})$ en tant que groupe abélien fini ?
2. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$?
3. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$?
4. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/27\mathbb{Z})$?
5. Existe-t-il un entier n tel que $E(\mathbb{F}_{61^n})$ soit un groupe cyclique ?

Exercice 2
On considère la courbe elliptique E définie le corps $\mathbb{F}_2$ par l'équation

$$y^2 + xy = x^3 + x^2 + 1$$

C'est un cas particulier de courbe de Koblitz. Dans les recommandations du NIST (National Institute of Standards and Technology), cette courbe est proposée pour implémenter un certain cryptosystème. Il est précisé que :

- le corps $\mathbb{F}_{2^{163}}$ est isomorphe à $\mathbb{F}_2[X]/X^{163} + X^7 + X^6 + X^3 + 1$
- le groupe $E(\mathbb{F}_{2^{163}})$ contient un point P d'ordre

$$n = 5846006549323611672814741753598448348329118574063$$

Les recommandations du NIST donnent aussi la valeur de P, mais pour des raisons de sécurité il est conseillé d'engendrer soi-même un tel point P.

1. Vérifier que le polynôme $X^{163} + X^7 + X^6 + X^3 + 1$ est irréductible sur $\mathbb{F}_2$.
2. Le nombre n est-il premier ?
3. Trouver un point P d'ordre n (on pourra le choisir aléatoirement).
4. Quel est l'ordre du groupe $E(\mathbb{F}_{2^{163}})$? (indication : c'est l'unique multiple de n qui appartient à l'intervalle donné par les bornes de Hasse).
5. Le groupe $E(\mathbb{F}_{2^{163}})$ est-il cyclique ?

Exercice 3
Soit E la courbe elliptique définie sur $\mathbb{Q}$ par les coefficients

$$E = [1, -1, 0, -167, 616]$$

1. Quel est le discriminant Δ de E ?

— Rappellons que l'on obtient, en réduisant l'équation de E modulo un premier p ne divisant pas Δ, une courbe elliptique sur $\mathbb{F}_p$, que l'on notera E_p dans tout le texte.

2. Soient $P = (-12, 34)$ et $Q = (24, 88)$. Vérifiez que P et Q sont sur la courbe E. Montrez que ce sont des points d'ordre infini dans le groupe $E(\mathbb{Q})$.

— Si p est un nombre premier ne divisant pas Δ, on note $\tilde{P}$ et $\tilde{Q}$ les points obtenus en réduisant modulo p les points P et Q. On note $\langle \tilde{P}, \tilde{Q} \rangle$ le sous-groupe de $E_p(\mathbb{F}_p)$ engendré par ces deux points.

3. Donner un exemple de nombre premier p pour lequel $\langle \tilde{P}, \tilde{Q} \rangle = E_p(\mathbb{F}_p)$.

4. Donner un exemple de nombre premier p pour lequel $\langle \tilde{P}, \tilde{Q} \rangle \neq E_p(\mathbb{F}_p)$.