Travail préparatoire au DS

Exercice 1
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 $\langle \tilde{P}, \tilde{Q} \rangle \neq E_p(\mathbb{F}_p)$.

Exercice 2
Soit G la courbe elliptique définie sur $\mathbb{F}_{211}$ par les coefficients

$$G = [0, -1, 0, 56, 108]$$

Soit $R(X)$ le polynôme donné par la commande `ffinit`$(211, 3)$, et soit t la classe de X modulo $R(X)$. On considère les points ci-dessous, à coordonnées dans $\mathbb{F}_{211^3}$

$$P = (83 * t^2 + 123 * t + 69, 165 * t^2 + 157 * t + 150)$$

$$Q = (25 * t^2 + 11 * t + 58, 122 * t^2 + 111 * t + 27)$$

1. Déterminer l'ordre de P.
2. On admet que Q appartient au groupe cyclique engendré par P. En utilisant l'algorithme de Shanks, trouver un entier n tel que $[n]P = Q$.