TD4 - Forme de Montgomery et forme d'Edward

Exercice 1. Soit $E\colon y^2 = x^3 + ax + b$ une courbe elliptique sur un corps k. On suppose que $x^3 + ax + b$ possède une racine α dans k telle que $3\alpha^2 + a$ est un carré dans k.

1. Rappeler pourquoi E possède un point k-rationnel d'ordre 2.
2. Montrer que E peut-être mise sous forme de Montgomery.
3. On pose la courbe $y^2 = x^3 - x + 2$ sur $k = \mathbb{F}_{11}$.
   (a) Calculer le cardinal de $E(\mathbb{F}_{11})$.
   (b) Montrer que -3 est une racine de $X^3 - X + 2 \in \mathbb{F}_{11}[X]$.
   (c) Justifier que E peut être mise sous forme de Montgomery et donner cette forme.
   (d) Utiliser la multiplication scalaire de Montgomery pour calculer l'abscisse de $6P$ avec $P = (3, 2) \in E$ (on doit trouver 6).

Exercice 2. Soit $E\colon y^2 = x^3 + 21x + 3$ définie sur $\mathbb{F}_{47}$.

1. Soit $P = (12, 3) \in E(\mathbb{F}_{47})$. Montrer que l'ordre de P est 23 ou 46 en vous inspirant de l'algorithme pas de bébé - pas de géant (on a $48P = (1, 5)$).
2. En utilisant la borne de Hasse, calculer $\#E(\mathbb{F}_{47})$.

Exercice 3. On rappelle qu'une courbe sous forme d'Edward est donnée par

$$C\colon u^2 + v^2 = c^2(1 + du^2v^2)$$

avec $c, d \in \mathbb{F}_p$ tel que c est non nul et d n'est pas un carré dans $\mathbb{F}_p$.

La loi de groupe sur C est donnée par

$$(u_1, v_1) + (u_2, v_2) = \left(\frac{u_1v_2 + u_2v_1}{c(1 + du_1u_2v_1v_2)}, \frac{v_1v_2 - u_1u_2}{c(1 - du_1u_2v_1v_2)} \right).$$

1. Vérifier qu'une telle courbe C a tous ses points affines lisses.
2. Vérifier que le point $(0, c)$ appartient bien à C et est bien l'élément neutre de C pour la loi '+'.
3. Vérifier que le point $(c, 0)$ appartient bien à C et est d'ordre 4.
4. Montrer qu'on peut toujours choisir $c = 1$.
5. Retrouver les formules de dédoublement en coordonnées projectives à l'aide de celles en coordonnées affines. Combien d'opérations nécessitent ces formules ?
6. En utilisant le modèle de C en coordonnées projectives simplifier les formules trouvées dans la question précédente et retrouver le nombre d'opérations annoncé en cours ($3M + 4S$).