TP : Utilisation de l'ordinateur (Sage ?)

Les exercices suivants servent à expérimenter avec l'outil informatique, par exemple avec SageMath, qui est open source et gratuit.

La manière la plus simple d'utiliser Sage est `https://sagecell.sagemath.org/`, qui fonctionne entièrement en ligne et fournit directement une petite console (parfait pour quelques lignes). Pour les choses moins simples, on peut utiliser `https://cocalc.com/` (en ligne, nécessité de créer un compte), ou bien simplement on peut l'installer sur sa machine (voir `sagemath.org`). La doc de Sage pour les courbes elliptiques est ici :

`https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/ell_field.html`

Aucune compétence en Sage n'est nécessaire pour l'évaluation de cette partie de l'UE. C'est juste pour expérimenter et ça peut être utile pour vérifier ses résultats sur les exercices « classiques », ou éventuellement pour la troisième partie de l'UE (?)
Attention cependant, habituez-vous à faire des calculs simples à la main, car vous n'aurez pas l'outil informatique à l'examen de cette partie du cours.

Exercice 1. (Faisable à la main) On considère la courbe projective d'équation affine $y^2 = x^3 - x$, sur le corps $\mathbb{F}_9$. Combien y a-t-il de points ?

Exercice 2. (Faisable à la main) On considère, sur $\mathbb{F}_{11}$, la courbe elliptique $y^2 = x^3 + x + 3$. Calculer le nombre de points sur $\mathbb{F}_{11}$, montrer que le groupe $E(\mathbb{F}_{11})$ est cyclique et déterminer un générateur.

Exercice 3. On considère, sur $\mathbb{F}_{101}$, la courbe elliptique $y^2 = x^3 + 7x + 1$. Calculer l'ordre du point $(0,1)$ et en déduire $|E(\mathbb{F}_{101})|$.

Exercice 4. On considère, sur $\mathbb{F}_{557}$, la courbe elliptique $y^2 = x^3 - 10x + 21$. Calculer l'ordre du point $(2,3)$ et en déduire $|E(\mathbb{F}_{557})|$.

Exercice 5.

Exercice 6.
1. Soit $p = 1000033$. Vérifier que p est premier puis que 69 est un carré dans $\mathbb{F}_p$ et en trouver une racine carrée dans $\mathbb{F}_p$.
2. En déduire un point de la courbe elliptique $y^2 = x^3 + 33x + 69$ sur $\mathbb{F}_p$. Quel est l'ordre de ce point ?

Exercice 7. On considère sur $\mathbb{F}_{2011}$ la courbe $y^2 + xy + 3y = x^3 + 2x^2 + 4x + 5$.
1. Calculer le discriminant et le j-invariant de E.
2. Montrer que les points $P = (1,2)$ et $Q = (2,470)$ sont sur la courbe.
3. Calculer le nombre de points sur $\mathbb{F}_{2011}$.
4. Déterminer une formule pour la loi de groupe sur la courbe. Calculer $2P$. Trouver un entier N tel que $Q = NP$.

Exercice 8. Montrer que la courbe elliptique $y^2 = x^3 + 4x + 1$ définie sur $\mathbb{F}_5$ a un groupe de 5-torsion non trivial, en trouvant de la 5-torsion sur $\mathbb{F}_{5^8}$.

Exercice 9. Sur $\mathbb{F}_7$ on considère la courbe elliptique E d'équation $y^2 = x^3 - x - 2$. Combien de points possède-t-elle sur $\mathbb{F}_7$? La courbe est-elle supersingulière ? Quelle est la plus petite extension sur laquelle E possède de la 7-torsion ?

Exercice 10. Soit $p = 100003$. Pour $b \in \{5, 9, 11, 12, 13, 16, 25, 33\}$, on considère sur $\mathbb{F}_p$ la courbe elliptique

$$E_b : \quad y^2 = x^3 + x + b.$$

1. Écrire un programme pour calculer le nombre de points.
2. Montrer à chaque fois que le groupe $E(\mathbb{F}_p)$ est cyclique et exhiber un générateur.