TD 2

Une courbe elliptique E est une équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

où les coefficients $(a_i)_{i\in\{1,\cdots,4,6\}}$ sont des éléments d'un corps $\mathbb{K}$. En abrégé,

$$E = [a_1, a_2, a_3, a_4, a_6].$$

Exercice 1. Soit E une courbe elliptique d'efinie sur un corps $\mathbb{K}$. L'objectif de cet exercice est de calculer, via l'algorithme de la fenêtre flexible, $[n]P$ étant donnés un entier naturel n et un point P de E.

1. Écrire une procédure qui, étant donné un entier naturel non-nul k et un point P de E, calcule le vecteur
$$\left(P, [2]P, [4]P, \cdots, [2^k]P\right).$$
Appelez-là *powinit(E,P,k)*.
2. Écrire une procédure qui, étant donné un entier naturel n et un point P de E, calcule le point $[n]P$. Appelez-là *flexpow(E,P,n)*. Conseil : écrire
$$n = 2^v(2^kq + r)$$
où $0 \leqslant r < 2^k$ est un entier naturel impair, q et v sont deux entiers naturels.
3. Tester sur de nombreux exemples de courbes elliptiques sur des corps finis pour des valeurs de k différentes et comparer avec la fonction *ellpow*. Conseil : Écrire une procédure qui, étant donnée une courbe elliptique E sur le corps fini $\mathbb{F}_q$ avec $q = p^m$ renvoie un point aléatoire sur E i.e. un élément aléatoire de $E(\mathbb{F}_q)$. Appelez-là *ellrand(E,p,m)*.
4. Si E est la courbe elliptique rationnelle, i.e. sur $\mathbb{Q}$, définie par $y^2 = x^3 + 256$ alors calculer son discriminant à l'aide de gp puis vérifier que $P = (0, 16)$ est bien sur la courbe elliptique et est un point de torsion. Calculer son ordre à l'aide de la procédure précédente. Comparer avec la fonction *ellorder*.
5. Si E est la courbe elliptique rationnelle définie par $y^2 = x^3 + x/4$ alors calculer son discriminant à l'aide de gp puis vérifier que $P = (1/2, 1/2)$ est bien sur la courbe elliptique et est un point de torsion. Calculer son ordre à l'aide de la procédure précédente. Comparer avec la fonction *ellorder*.
6. Si E est la courbe elliptique rationnelle définie par $y^2 = x^3-43x+166$ alors calculer son discriminant à l'aide de gp puis vérifier que $P = (3, 8)$ est bien sur la courbe elliptique et est un point de torsion. Calculer son ordre à l'aide de la procédure précédente. Comparer avec la fonction *ellorder*.

Exercice 2. L'objectif de cet exercice est de calculer quelques logarithmes discrets via la méthode ρ de Pollard. Soit E une courbe elliptique sur $\mathbb{F}_q$ avec $q = p^m$. Soient P et Q dans $E(\mathbb{F}_q)$ avec

$$Q \in \langle P\rangle := \{[k]P, k \in \mathbb{Z}\}.$$

On cherche un entier naturel n (modulo l'ordre de $P\ldots$) satisfaisant $Q = [n]P$, i.e. on cherche $\log_P(Q)$. Soit $\langle P\rangle = G_1 \amalg G_2 \amalg G_3$ une partition de $\langle P\rangle$ en trois sous-ensembles de taille equivalente. On définit une marche aléatoire sur $\langle P\rangle$ par $w_0 = P$ et

$$w_{i+1} = \Phi(w_i) = \begin{cases} w_i + Q & \text{si } w_i \in G_1, \\ [2]w_i & \text{si } w_i \in G_2, \\ w_i + P & \text{sinon} \end{cases}$$

pour tout entier naturel i.

1. Imaginer une facon de partitionner $\langle P \rangle$.
2. Montrer que si cette marche aléatoire présente une collision alors vous êtes capables de trouver $\log_P(Q)$.
3. Montrer qu'il existe un entier naturel i grand satisfaisant $w_i = w_{2i}$. Écrire une procédure qui, étant donnés P et Q renvoie n. Appelez-là *pollard(E,P,Q,p,m)*. Discutez ses avantages et ses inconvénients.
4. Écrire une première amélioration sachant qu'il existe un entier naturel i satisfaisant $w_i = w_{\ell(i)-1}$ où $\ell(i)$ est la plus grande puissance de 2 inférieure à i ie $\ell(i) := 2^{E(\log(i))}$ où $E(x)$ est la partie entière de x. Appelez-là *pollard2(E,P,Q,p,m)*. Discutez ses avantages et ses inconvénients.
5. Écrire une deuxième amélioration sachant qu'il existe un entier naturel i satisfaisant $w_i = w_{\ell(i)-1}$ et $3\ell(i)/2 \leqslant i \leqslant 2i$. Appelez-là *pollard3(E,P,Q,p,m)*. Discutez ses avantages et ses inconvénients.
6. Comparer ces diverses procédures sur l'exemple suivant : E est la courbe elliptique définie sur $\mathbb{F}_{173}$ par
$$y^2 = x^3 + 146x + 33$$
et $P = (168, 133)$ et $Q = (147, 74)$.
7. Tester sur vos exemples préférés.

Exercice 3. L'objectif de cet exercice est de calculer quelques logarithmes discrets via la méthode Pas de bébés-Pas de géants. Soient E une courbe elliptique sur un corps $\mathbb{K}$ et P un point d'ordre ℓ. Tout repose sur le fait que si $s = E(\sqrt{l}) + 1$ alors il existe des entiers naturels U et V compris entre 0 et s tels que
$$n = U + Vs.$$
1. Étant donnés une courbe elliptique, $Q \in \langle P \rangle$ sur celle-ci et deux réels i_{min} et i_{max}, écrire une procédure déterminant un entier relatif i satisfaisant $i.P = Q$ et $i_{min} \leqslant i \leqslant i_{max}$. Appelez-là *babygiant(E,P,Q,min,max)*.
2. En déduire une procédure déterminant l'ordre d'un point connaissant un encadrement d'un multiple de l'ordre.
3. En déduire une procédure déterminant l'ordre d'un point sur une courbe elliptique sur un corps fini.
4. Appliquer la procédure suivante à la courbe elliptique définie sur $\mathbb{F}_{173}$ par
$$y^2 = x^3 + 146x + 33$$
et aux points $P = (168, 133)$ et $Q = (147, 74)$.

Exercice 4. L'objectif de cet exercice est d'avoir en stock des procédures permettant de calculer l'ordre d'un point sur une courbe elliptique E sur un corps $\mathbb{K}$.
1. Écrire une procédure déterminant l'ordre d'un point connaissant la factorisation d'un multiple de l'ordre.
2. En déduire une procédure déterminant l'ordre d'un point connaissant un multiple de l'ordre.
3. Appliquer les procédures précédentes à la courbe elliptique définie sur $\mathbb{F}_{173}$ par
$$y^2 = x^3 + 146x + 33$$
et aux points $P = (168, 133)$ et $Q = (147, 74)$.

Exercice 5. L'objectif de cet exercice est de tracer graphiquement les trajectoires des itérés de points choisis aléatoirement sur une courbe elliptique définie sur $\mathbb{F}_p$ où p est un nombre premier (101, 2003, ...).
1. Écrire une procédure représentant graphiquement une courbe elliptique sur $\mathbb{F}_p$ puis représentant graphiquement l'arc
$$P \to [2]P \to [3]P \to \cdots \to [n]P$$
où n est bien choisi et P est un point aléatoire sur la courbe elliptique. Conseil : vous pourriez representer $\mathbb{F}_p$ sur l'axe des abscisses par $\{0, 1, \cdots, p-1\}$ et sur l'axe des ordonnées par $\{-(p-1)/2, \cdots, (p-1)/2\}$.

2. Tester sur quelques courbes elliptiques et sur plusieurs points pour voir si des choses intéressantes se passent.
3. Changez éventuellement de point de vue, i.e. fixer une courbe elliptique E sur $\mathbb{Q}$ et un point P à coefficients dans $\mathbb{Z}$ sur E d'ordre infini. Pour chaque nombre premier p, représenter graphiquement la courbe elliptique $\overline{E}_p$ ie la réduction de la courbe elliptique E sur $\mathbb{F}_p$ ainsi que la trajectoire des itérés de $\overline{P}_p$ ie la réduction modulo p de P. Prendre p de plus en plus grand. Se passent-il des choses intéressantes ?

Exercice 6. Soit E une courbe elliptique définie sur $\mathbb{Q}$ de discriminant Δ sans facteurs carrés et à coefficients dans $\mathbb{Z}$. Pour tout nombre premier p ne divisant pas Δ, on note $\overline{E}_p$ la réduction de E modulo p puis $\overline{E}_p(\mathbb{F}_p)$ le groupe des points $\mathbb{F}_p$-rationnels de $\overline{E}_p$. Vous savez désormais que $\overline{E}_p(\mathbb{F}_p)$ est un groupe fini de cardinal $p+1-t_p$, où t_p est la trace du Frobenius, isomorphe à

$$\mathbb{Z}/d_{1,p}\mathbb{Z} \times \mathbb{Z}/d_{2,p}\mathbb{Z}$$

où $d_{1,p} \mid d_{2,p}$. L'objectif de cet exercice est de deviner numériquement le comportement asymptotique de

$$N_E(X) = \left|\left\{p \leqslant X, p \in \mathcal{P}, p \nmid \Delta, \overline{E}_p(\mathbb{F}_p) \text{ cyclique}\right\}\right|$$

lorsque $X \to +\infty$. Vous avez toutes les cartes en main. Pour tester la cyclicité de $\overline{E}_p(\mathbb{F}_p)$, vous pourriez tirer au hasard un point sur $\overline{E}_p$ puis calculer son ordre et le comparer avec l'ordre de $\overline{E}_p(\mathbb{F}_p)$ par exemple. Essayer de trouver une application cryptographique à ce résultat.

Exercice 7. L'objectif de cet exercice est de vérifier la loi de Sato-Tate prouvée par Taylor. Si E est une courbe elliptique sur $\mathbb{Q}$ de discriminant sans facteurs carrés et à coefficients dans $\mathbb{Z}$ et p est un nombre premier alors vous savez qu'il est possible d'écrire la trace du Frobénius sous la forme

$$t_p = 2\sqrt{p}\cos(\theta_p)$$

où $0 \leqslant \theta_p \leqslant \pi$. Essayer de déterminer le comportement asymptotique de

$$\mathrm{ST}_E(X) = |\{p \leqslant X, p \in \mathcal{P}, \alpha \leqslant \theta_p \leqslant \beta\}|$$

où $0 \leqslant \alpha < \beta \leqslant \pi$.

Exercice 8. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par

$$y^2 + y = x^3 - 7x + 6.$$

1. Quel est le discriminant de cette courbe ?
2. Trouver le groupe de torsion de cette courbe.
3. On se propose de déterminer quelques points rationnels sur cette courbe. Si (x, y) est un point réel de la courbe alors montrer à l'aide de gp que $x \geqslant -3$. En déduire une procédure renvoyant une liste de points rationnels sur la courbe à l'aide de la commande *ellordinate*.