TD n° 5 — Couplage de Weil

Dans toute la feuille, E est une courbe elliptique sur un corps fini de caractéristique p, et m est un entier premier à p.

Le couplage de Weil (ou pairing de Weil) est une application $\mathbb{Z}$-bilinéaire alternée et non dégénérée

$$e_m : E(\overline{\mathbb{F}_p})[m] \times E(\overline{\mathbb{F}_p})[m] \longrightarrow \mu_m(\overline{\mathbb{F}_p})$$

où $\mu_m(\overline{\mathbb{F}_p})$ désigne le groupe multiplicatif des racines m-ièmes de l'unité dans $\overline{\mathbb{F}_p}$.

Les e_m sont compatibles les uns avec les autres quand on fait varier m. Plus précisément, soit m' un autre entier premier à p, et soient deux points $P \in E[m]$ et $Q \in E[mm']$. Alors

$$e_{mm'}(P, Q) = e_m(P, m'Q).$$

Exercice 1

1. Comment se traduit la bilinéarité de e_m ?
2. Comment se traduit l'alternance de e_m ?
3. Comment se traduit la non-dégénérescence de e_m ?
4. Montrer que e_m est antisymétrique, c'est-à-dire que

   $$e_m(Q, P) = e_m(P, Q)^{-1}$$

   pour tout couple $(P, Q) \in E[m]^2$.
5. À quel groupe est isomorphe $\mu_m(\overline{\mathbb{F}_p})$? Montrer qu'il existe un entier k tel que

   $$\mu_m(\overline{\mathbb{F}_p}) = \mu_m(\mathbb{F}_{p^k})$$

   Quelle propriété arithmétique k doit-il satisfaire ? Quel est le plus petit k possible ?
6. Soient P et Q deux points de m-torsion. Déterminer une relation entre l'ordre de $e_m(P, Q)$, l'ordre de P et l'ordre de Q.
7. Soit $P \in E(\overline{\mathbb{F}_p})$ un point d'ordre m. Montrer qu'il existe un autre point Q d'ordre m tel que $e_m(P, Q)$ soit une racine primitive m-ième de l'unité.

Exercice 2

Soit E la courbe elliptique sur $\mathbb{F}_{23}$ définie par les coefficients

$$E = [1, 0, 0, -4, -1]$$

1. Consulter l'aide de la fonction `ellweilpairing`.
2. On considère les points $P = (5, 8)$ et $Q = (-2, 1)$ appartenant à $E(\mathbb{F}_{23})$. Vérifier que P est d'ordre 4 et que Q est d'ordre 2. Calculer $e_4(P, Q)$ et en déduire que Q n'est pas un multiple de P.
3. Quel entier k faut-il choisir pour que $\mathbb{F}_{23^k}$ contienne les racines 4-ièmes de l'unité ?

4. Que sont les polynômes de n-division de E ? En utilisant la fonction `elldivpol`, calculer le polynôme de 4-division de E.
5. En utilisant les fonctions `factorff` et `ellordinate`, vérifier que les points de 4-torsion de E sont tous définis sur $\mathbb{F}_{23^2}$.
6. Trouver un point R d'ordre 4 dans $E(\mathbb{F}_{23^2})$ tel que $e_4(P, R)$ soit une racine primitive 4-ième de l'unité.

Exercice 3
Le but de cet exercice est d'attaquer le log discret sur la courbe E en se ramenant au log discret dans le groupe $\overline{\mathbb{F}_p}^\times$.

Soit $P \in E(\mathbb{F}_p)$, et soit Q un point appartenant au sous-groupe cyclique $\langle P \rangle$ engendré par P. On cherche à déterminer un entier l tel que $Q = lP$. On suppose (comme dans la méthode rho de Pollard) que l'on connaît déjà l'ordre m du point P.

1. Soit $R \in E(\overline{\mathbb{F}_p})$ un point d'ordre m tel que $e_m(P, R)$ soit une racine primitive m-ième de l'unité (un tel point existe bien d'après l'exercice 1). Soit r un entier tel que $e_m(Q, R) = e_m(P, R)^r$. Montrer que $Q = rP$.
2. Imaginer quelles seraient les étapes d'une procédure qui, étant donné P, calcule R. On ne demande pas de la programmer.
3. En déduire une procédure qui résout le log discret sur E à partir de la fonction `fflog`.

Exercice 4
Soit $q = p^n$ une puissance de p, et soit E une courbe elliptique sur $\mathbb{F}_q$, munie d'un point P d'ordre N premier suffisamment grand (en particulier, $N \neq p$). On se demande dans quelle mesure l'attaque du log discret sur E via le couplage de Weil est efficace.

1. En combien de temps sait-on résoudre le problème du log discret (DLP) dans un groupe cyclique d'ordre N ?
2. En combien de temps sait-on résoudre le DLP dans le groupe des racines N-ièmes de l'unité $\mu_N(\overline{\mathbb{F}_q})$?
3. Soit d le plus petit entier tel que $\mu_N(\overline{\mathbb{F}_q}) \subseteq \mathbb{F}_{q^d}^\times$. Soit

$$t_q = q + 1 - \#E(\mathbb{F}_q)$$

   Quel est l'ordre de grandeur de t_q ? Montrer que :

$$(t_q - 1)^d \equiv 1 \pmod{N}$$

4. On suppose que $P \in E(\mathbb{F}_p)$ et que $\#E(\mathbb{F}_p) = p + 1$ (quand $p \geq 5$, c'est ce qu'on appelle une courbe supersingulière). Pourquoi est-ce a priori une mauvaise idée d'implémenter Diffie-Hellman sur une telle courbe elliptique ?
5. Quelles contraintes doit satisfaire une courbe elliptique pour être *pairing-friendly* ?