Université Bordeaux I – 2012/2013 | Courbes elliptiques
Master 1 Cryptologie et Sécurité Informatique | Yu. Bilu / J. Gillibert

TD n° 3 — Points d'ordre fini et logarithme discret

Exercice 1
Soit E la courbe elliptique sur $\mathbb{Q}$ définie par l'équation

$$y^2 + xy = x^3 - x^2 - x + 1$$

1. Vérifier que le point $P = (0, 1)$ est un point d'ordre infini dans $E(\mathbb{Q})$. On admet que P engendre $E(\mathbb{Q})$, qui est donc isomorphe à $\mathbb{Z}$.
2. Pour tous les premiers p de 31 à 1000, calculer $E_p(\mathbb{F}_p)$, et déterminer l'ordre de la réduction $\tilde{P}$ de P modulo p (on utilisera la fonction `ellorder`). Que peut-on observer ?
3. Soit F la courbe elliptique sur $\mathbb{Q}$ définie par l'équation

$$y^2 = x^3 + 109858299531561$$

Que peut-on dire des points $P_1 = (735532, 630902573)$, $P_2 = (49704, 15252915)$, $P_3 = (-4578, 10476753)$, $P_4 = (-15260, 10310419)$ et $P_5 = (197379, 88314450)$?
4. Faire des expériences similaires à celles de la question 2 avec cette nouvelle courbe et ces cinq points.

Exercice 2
L'objectif de cet exercice est de programmer des procédures pour calculer l'ordre d'un point sur une courbe elliptique E.

1. Écrire une procédure `ellpointorder`(E, P, m) qui détermine l'ordre d'un point P à partir d'un entier m tel que $[m]P = 0$ (se servir de la factorisation de m).
2. On considère la courbe elliptique $E = [0, 1, 0, 4, 4]$ définie sur le corps $\mathbb{F}_{523}$. En se servant de la procédure précédente, calculer l'ordre des points $P1 = (309, 347)$, $P2 = (137, 433)$ et $P3 = (282, 132)$. Comment choisir l'entier m ?

Exercice 3
L'objectif de cet exercice est de rechercher des points d'ordre grand sur une courbe elliptique sur un corps fini. Dans tout l'exercice, p est un premier et q est une puissance de p.

1. Soit E une courbe elliptique sur $\mathbb{F}_p$. Écrire une fonction `RandomPoint`(E, n) qui renvoie un point aléatoire $P \in E(\mathbb{F}_{p^n})$.
2. Soit $P \in E(\mathbb{F}_q)$. Montrer que si l'ordre m de P satisfait

$$q + 1 - 2\sqrt{q} \leq m \leq q + 1 + 2\sqrt{q}$$

alors $E(\mathbb{F}_q)$ est cyclique d'ordre m, engendré par P (on pourra supposer que q est suffisamment grand).

3. En déduire une procédure `ChercheGen`(E, n) qui cherche un générateur potentiel du groupe $E(\mathbb{F}_q)$ et un entier $m \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ satisfaisant $[m]P = 0$.
4. Tester cette procédure sur la courbe $E = [0, -1, 1, 0, 0]$ définie sur $\mathbb{F}_{2^n}$ avec des valeurs de n de plus en plus grandes.

Exercice 4

L'objectif de cet exercice est de programmer la méthode « *baby-step giant-step* », ou algorithme de Shanks, pour calculer les logarithmes discrets.

Soient E une courbe elliptique sur un corps K. Soit $P \in E(K)$ un point d'ordre fini, et soit Q un point appartenant au sous-groupe cyclique $\langle P \rangle$ engendré par P. On cherche à déterminer un entier n tel que $[n]P = Q$. Bien sûr, un tel entier n n'est pas unique.

1. Étant donnés une courbe elliptique E, deux points P et Q comme ci-dessus, et deux entiers naturels i_{min} et i_{max}, écrire une procédure déterminant un entier n satisfaisant $[n]P = Q$ et $i_{min} \leqslant n \leqslant i_{max}$. Appelez-la `babygiant`$(E, P, Q, imin, imax)$.
2. Appliquer la procédure précédente à la courbe $E = [1, -1, 1, 4, 6]$ définie sur le corps $\mathbb{F}_{2017}$, avec les points $P = (582, 722)$ et $Q = (860, 1428)$. Quelles valeurs de *imin* et de *imax* peut-on choisir ?
3. En déduire une procédure déterminant l'ordre d'un point connaissant un encadrement d'un multiple de l'ordre.
4. En déduire une procédure `ellorderff`(E, P) déterminant l'ordre d'un point sur une courbe elliptique sur un corps fini.
5. Appliquer la procédure précédente à la courbe elliptique définie sur $\mathbb{F}_{173^3} = \mathbb{F}_{173}[X]/(X^3 + X^2 - 2X - 1)$ par
$$y^2 + y = x^3 - x^2 - 10x - 20$$
et au point $P = (133t^2 + 138t + 99, 146t^2 + 101t + 44)$, où t désigne la classe de X modulo $X^3 + X^2 - 2X - 1$.