TD3 TANC - Nombre de points des courbes elliptiques sur les corps finis

Exercice 1 (Méthode CM)**.** Trouver une courbe elliptique E définie sur $\mathbb{F}_{11}$ avec $N = 10$ points rationnels. On donne

$$H(X) = H_{\mathbb{Z}[\sqrt{-10}]}(X) = X^2 - 425692800X + 9103145472000 \in \mathbb{Z}[X].$$

La trace d'une telle courbe devrait vérifier $a = 11+1-N = 2$. Le discriminant Δ de l'ordre $\mathbb{Z}[\pi]$ engendré par son Frobenius π serait $\Delta = a^2 - 4 \times 11 = 4 - 44 = -40 = \underbrace{4}_{f^2} \times \underbrace{-10}_{d}$. Le Frobenius engendre donc un ordre qui est maximal. On cherche les courbes sur $\mathbb{F}_{11}$ à multiplication complexe par $\mathbb{Z}[\sqrt{-10}]$. Les j-invariants de ces courbes sont les racines de $H \in \mathbb{F}_{11}[X]$. On réduit les coefficients de H modulo 11. On rappelle qu'un entier $(a_1 a_2 \dots a_n)_{10}$ en base 10 est divisible par 11 si et seulement si $\sum_i a_{2i} = \sum_j a_{2j+1} \mod 11$, on a $4+5+9+8 = 26 = 4 \mod 11$ et $2+6+2 = 10$ donc 425692806 est divisible par 11 et donc $425692800 = -6 \mod 11$. De la même façon on a $9103145472000 = -3 \mod 11$. On en déduit que $H = X^2 - 5X - 3 \in \mathbb{F}_{11}[X]$. On cherche ses racines. Le discriminant de H est $5^2 + 4 \times 3 = 37 = 4 = 2^2$ donc ses racines sont

$$\frac{5 \pm 4}{2} = (5 \pm 2) \times 6 = 7 \text{ ou } -2.$$

On prend $j = -2$. On a bien $j \neq 0$ et $j \neq 1728 = 1 \mod 11$. On a la courbe elliptique

$$E\colon y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j} = x^3 + \frac{-6}{3}x + \frac{-4}{3} = x^3 - 2x - 5.$$

Cette courbe a soit $q + 1 - a = 10$ points soit $q + 1 + a = 14$ points. Les carrés non-nuls de $\mathbb{F}_{11}$ sont $\{1^2, 2^2, 3^2, 4^2, 5^2\} = \{1, 4, 9, 5, 3\}$ On compte les points.

x	$x^3 - 2x - 5$	
0	6	
1	5	$\to$ 2 points
-1	7	
2	-1	
-2	-2	
3	5	$\to$ 2 points
-3	7	
4	7	
-4	5	$\to$ 2 points
5	0	$\to$ 1 point
-5	1	$\to$ 2 points

Notre courbe possède donc 9 points affines plus le point à l'infini soit 10 points au total. On veut donc calculer une tordue quadratique de E. On prend $-1 \in \mathbb{F}_{11}$ qui n'est pas un carré. La courbe

$$\widetilde{E}\colon y^2 = x^3 - 2 \cdot (-1)^2 x - 5 \cdot (-1)^3 = x^3 - 2x + 5$$

a donc 14 points.

Exercice 2 (Algorithme de Schoof)**.** On considère la courbe $E\colon y^2 = x^3 - 4x - 1 = f(x)$ sur $\mathbb{F}_{13}$. On note a sa trace et $\pi(x, y) = (x^{13}, y^{13})$ son morphisme de Frobenius.

1. Justifier qu'il suffit de connaître $a \mod \ell$ pour $\ell = 2, 3, 5$ pour en déduire a.
   Si on connaît a modulo $2, 3, 5$ par le théorème des restes on connaît $a \mod 30$. Or, d'après la borne de Hasse,
   $$-\lfloor 2\sqrt{13} \rfloor = -7 \leq a \leq 7$$
   et il y a au plus un multiple de 30 dans cet intervalle.
2. Montrer que $f(5) = 0$. En déduire que $a = 0 \mod 2$.
   On a $f(5) = 5^3 - 4 \cdot 5 - 1 = \underbrace{-1}_{5^2} \cdot 5 - 20 - 1 = -26 = 0$. Les racines x de f induisent des points $(x, 0) \in E$ qui sont de 2-torsion. Donc $(5, 0)$ est un point de E de 2 torsion donc $2 | \#E(\mathbb{F}_{13}) = 13 + 1 - a$ donc $a = 0 \mod 2$.

3. Montrer que le point $P = (-4, 4)$ est un point de E et calculer l'abscisse de $2 \cdot P$.
On a $f(-4) = -4 \cdot \underbrace{3}_{4^2} + 4 \cdot 4 - 1 = 3 = 4^2$. Donc $P \in E$. L'abscisse x_0 de $2P$ est $m^2 - 2 \cdot (-4)$ où $m = \frac{3 \cdot (-4)^2 - 4}{2 \cdot 4} = -1$ donc $x_0 = 1 + 8 = 9 = -4$.

4. En déduire que P est un point de 3 torsion. Que peut-on en déduire sur $a \mod 3$?
On en déduit que $2P = \pm P$ donc $3P = \infty$ ou $P = \infty$ mais $P \neq \infty$ donc $3P = \infty$ donc P est d'ordre 3.
On en déduit que $q + 1 - a = 0 \mod 3$ i.e. $a = -1 \mod 3$.

5. Montrer que 2 n'est pas un carré dans $\mathbb{F}_{13}$. On pose alors $K = \mathbb{F}_{13^2} = \mathbb{F}_{13}[X] / \langle X^2 - 2 \rangle$ et $\alpha \in \mathbb{F}_{13}$ tel que $\alpha^2 = 2$ (i.e. α est une racine de 2 dans K). On considère $Q = (-1, \alpha)$.
Par les lois de réciprocité quadratique $\left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = -1$ donc 2 n'est pas un carré modulo 13. Une autre méthode consiste à énumérer les carrés de $\mathbb{F}_{13}$ en calculant $1^2, 2^2, 3^2, 4^2, 5^2$ et 6^2 modulo 13 et constater que 2 n'est pas dedans.

   (a) Montrer que $Q \in E(K)$. On **admet** que Q est d'ordre 5.
   On a $f(-1) = (-1)^3 + 4 - 1 = 2 = \alpha^2$ donc $Q \in E(K)$.

   (b) Que valent $\pi(Q)$ et $\pi^2(Q) = \pi(\pi(Q))$?
   $\pi(Q) = ((-1)^p, \alpha^p)$. Le Frobenius de $\mathbb{F}_{13}$ laisse $\mathbb{F}_{13}$ invariant et permute les racines de $X^2 - 2$ qui sont α et $-\alpha$. Donc $\pi(Q) = (-1, -\alpha)$. Puisque Q est à coordonnées dans $K = \mathbb{F}_{13^2}$ la composée deux fois du Frobenius laisse les coordonnées de Q invariantes. Donc $\pi^2(Q) = Q$.

   (c) Montrer que $\pi(Q) = \pi^2(Q) - 2 \cdot Q$.
   On a $\pi^2(Q) - 2Q = -Q = (-1, -\alpha) = \pi(Q)$.

   (d) En déduire $a \mod 5$.
   On note $a_5 = a \mod 5$. On doit avoir

$$\pi^2(Q) - a_5 \pi(Q) + \underbrace{(13 \mod 5)}_{=-2} = 0.$$

   On a donc $a_5 = 1$.

6. En déduire la trace de E.
On a donc $a = 0 \mod 2, a = -1 \mod 3, a = 1 \mod 5$. On énumère tous les entiers $b = 1 \mod 5$ pour $|b| \leq \lfloor 2\sqrt{13} \rfloor = 7$

$$6, 1, -4.$$

On a $6 = 0 \mod 2$ mais $6 = 0 \neq -1 \mod 3$ donc $a = -4$ et donc $\#E(\mathbb{F}_{13}) = 13 + 1 - (-4) = 18$.