Université Bordeaux I – 2012/2013
Master 1 Cryptologie et Sécurité Informatique

Courbes elliptiques
Yu. Bilu / J. Gillibert

DS du 19 mars 2013, 14h – 16h

Durée : 2 heures. Les notes de cours et les programmes GP sont autorisés.

- Pour répondre aux questions, créer un seul fichier pour tout le sujet et séparer les exercices. Nommer le fichier `login.gp`, où login est votre identifiant informatique. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans le fichier `login.gp`.
- Pour rendre votre travail, envoyez le fichier par courriel à la fin de l'épreuve à l'adresse

  `jean.gillibert@math.u-bordeaux1.fr`
- Rappelons que la clarté des programmes et la pertinence des commentaires sont des éléments importants d'appréciation.

Exercice 1
Soit E la courbe elliptique définie sur $\mathbb{F}_{61}$ par les coefficients

$$E = [0, 1, 1, -3, 1]$$

1. Quelle est la structure de $E(\mathbb{F}_{61})$ en tant que groupe abélien fini ?
2. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$?
3. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$?
4. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/27\mathbb{Z})$?
5. Existe-t-il un entier n tel que $E(\mathbb{F}_{61^n})$ soit un groupe cyclique ?

Exercice 2
Soit H la courbe elliptique définie sur $\mathbb{F}_{2423}$ par les coefficients

$$H = [0, 1, 0, -3, -2]$$

Soit $R(X)$ le polynôme donné par la commande $\texttt{ffinit}(2423, 2)$, et soit t la classe de X modulo $R(X)$. On considère les points ci-dessous, à coordonnées dans $\mathbb{F}_{2423^2}$

$$P = (1205 * t + 168, 1033 * t + 1637)$$

$$Q = (1073 * t + 770, 519 * t + 2276)$$

1. En utilisant le théorème de Hasse, donner un majorant de l'ordre du groupe $H(\mathbb{F}_{2423^2})$.
2. On admet que Q appartient au groupe cyclique engendré par P. En utilisant l'algorithme de Shanks, trouver un entier n tel que $[n]P = Q$.
3. Déterminer l'ordre de P.
4. Les points P et Q engendrent-ils le même sous-groupe de $H(\mathbb{F}_{2423^2})$?

Exercice 3
Soit $A(X) \in \mathbb{F}_{5003}[X]$ le polynôme défini par

$$A(X) = X^3 + X^2 + X + 2$$

1. Expliquez brièvement pourquoi $\mathbb{F}_{5003}[X]/A(X)$ est isomorphe à $\mathbb{F}_{5003^3}$.
2. Soit x la classe de X modulo $A(X)$. A l'aide de la fonction `fforder`, dites si x est un générateur du groupe $(\mathbb{F}_{5003^3})^\times$.
3. On admet que $x^3 + 1$ est un générateur de $(\mathbb{F}_{5003^3})^\times$. A l'aide de la fonction `fflog`, déterminer un entier m tel que
$$(x^3 + 1)^m = x$$