Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Travaux dirigés
Alain Kraus

Exercices - Chapitre IV

Courbes elliptiques

Exercice 1

Soit E la courbe projective plane définie sur $\mathbb{Q}$ d'équation

$$y^2z = x^3 + 2xz^2 + z^3.$$

1) Montrer que E est une courbe elliptique.

Les points $P = [1, 2, 1]$ et $Q = [0, 1, 1]$ appartiennent au groupe $E(\mathbb{Q})$ des points de E rationnels sur $\mathbb{Q}$. Soit D la droite du plan projectif passant par P et Q.

2) Quelle est l'équation de D ?
3) Déterminer $D \cap E$.
4) Quelles sont les coordonnées des points $P + Q$ et $P + 2Q$?
5) Le groupe $E(\mathbb{Q})$ a-t-il un point d'ordre 2 ?

Exercice 2

Pour tout nombre premier $p \geq 5$, soit E la courbe projective plane sur $\mathbb{F}_p$ d'équation

$$y^2z = x^3 - 3xz^2 + 4z^3.$$

1) Montrer que E est une courbe elliptique sur $\mathbb{F}_p$.

Supposons désormais $p = 5$.

2) Déterminer le groupe $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$.
3) Soit $\phi_5 : E \to E$ l'endomorphisme de Frobenius de E. Quel est son polynôme caractéristique ?

Notons $E[5]$ le groupe des points de 5-torsion de E.

4) Soit P un point de E. Montrer que P est dans $E[5]$ si et seulement si on a $\phi_5(P) = -P$.
5) En déduire que $E[5]$ est contenu dans le groupe $E(\mathbb{F}_{25})$, où $\mathbb{F}_{25}$ est le corps de cardinal 25 dans une clôture algébrique de $\mathbb{F}_5$ choisie implicitement.
6) Quel est l'ordre du groupe $E(\mathbb{F}_{25})$?

7) En déduire la classe d'isomorphisme du groupe abélien $E(\mathbb{F}_{25})$.

Exercice 3

Soit E la courbe projective plane définie sur $\mathbb{F}_5$ d'équation

$$y^2z = x^3 - 2z^3.$$

1) Montrer que E est une courbe elliptique définie sur $\mathbb{F}_5$.

Soient $\overline{\mathbb{F}_5}$ une clôture algébrique de $\mathbb{F}_5$ et α un élément de $\overline{\mathbb{F}_5}$ tel que $\alpha^2 + 3\alpha - 1 = 0$.

2) Expliciter, en fonction de α, le sous-groupe $E[2]$ des points de 2-torsion de E.
3) Déterminer une base de $E[2]$ sur $\mathbb{Z}/2\mathbb{Z}$.
4) Expliciter dans cette base la matrice de l'endomorphisme de Frobenius de E restreint à $E[2]$.

Exercice 4

Soit E une courbe elliptique définie sur $\mathbb{F}_p$. Soit t la trace du Frobenius de E.

1) Montrer que pour tout $n \geq 1$, on a

$$|E(\mathbb{F}_{p^n})| \equiv 1 - t^n \text{ mod. } p.$$

Indication : On pourra reprendre la démonstration du théorème 4.9 du cours.

2) Supposons E ordinaire i.e. que le groupe $E[p]$ des points de p-torsion de E soit d'ordre p. En déduire que $\mathbb{F}_p(E[p])$ est l'extension de $\mathbb{F}_p$ de degré l'ordre de t modulo p.

Exercice 5

Soit E une courbe elliptique définie sur $\mathbb{F}_q$ (q est une puissance d'un nombre premier). On suppose que l'ordre de $E(\mathbb{F}_q)$ est $q + 1$.

1) Que vaut la trace du Frobenius de E ?
2) Soit $\phi_q : E \to E$ l'endomorphisme de Frobenius de E. En déduire que pour tout point $P \in E$ on a

$$\big(\phi_q \circ \phi_q\big)(P) = -qP.$$

3) Soient $n \geq 1$ un entier et $E[n]$ le sous-groupe des points de n-torsion de E. Supposons qu'il existe un point $P \in E(\mathbb{F}_q)$ d'ordre n. Montrer que $E[n]$ est contenu dans $E\big(\mathbb{F}_{q^2}\big)$, où $\mathbb{F}_{q^2}$ est le corps de cardinal q^2 dans une clôture algébrique de $\mathbb{F}_q$.

4) **Application.** Supposons que q soit un nombre premier congru à 3 modulo 4. Soit E la courbe elliptique définie sur $\mathbb{F}_q$ d'équation

$$y^2z = x^3 + xz^2.$$

4.1) Montrer que $E(\mathbb{F}_q)$ est un groupe d'ordre $q+1$.

4.2) Quels sont les points de 2-torsion de E rationnels sur $\mathbb{F}_q$? En déduire que le groupe $E(\mathbb{F}_q)$ est cyclique.

4.3) Quel est l'ordre de $E\big(\mathbb{F}_{q^2}\big)$?

4.4) En déduire que l'on a $E[q+1] = E\big(\mathbb{F}_{q^2}\big)$.

Exercice 6

Soit E la courbe projective plane sur $\mathbb{F}_5$ d'équation

$$y^2z = x^3 - xz^2 + z^3.$$

1) Montrer que E est une courbe elliptique définie sur $\mathbb{F}_5$.
2) Décrire l'ensemble $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$.
3) Déterminer la classe d'isomorphisme du groupe abélien $E(\mathbb{F}_5)$.
4) Quel est le polynôme caractéristique du Frobenius de E ?

Soit $\mathbb{F}_{25}$ le corps de cardinal 25 dans une clôture algébrique de $\mathbb{F}_5$.

5) Quel est l'ordre du groupe $E(\mathbb{F}_{25})$ des points de E rationnels sur $\mathbb{F}_{25}$?
6) Montrer que le groupe des points de 2-torsion de E est contenu dans $E(\mathbb{F}_{25})$.
7) En déduire que $E(\mathbb{F}_{25})$ n'est pas un groupe cyclique.
8) Admettons qu'il existe un point d'ordre 4 de E qui n'est pas rationnel sur $\mathbb{F}_{25}$[1] . En déduire la classe d'isomorphisme du groupe abélien $E(\mathbb{F}_{25})$.

[1] Soit $E[4]$ le groupe des points de 4-torsion de E, qui est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Étant donné un point (x, y) de E, on peut démontrer qu'il est d'ordre 4 si et seulement si on a

$$(x+1)(x+3)(x^4 + x^3 + 3x^2 + 1) = 0.$$

(On obtient une équation de degré 6, ce qui est conforme au fait qu'il y a douze éléments d'ordre 4 dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.) Posons $f = X^4 + X^3 + 3X^2 + 1 \in \mathbb{F}_5[X]$. On vérifie que f est irréductible sur $\mathbb{F}_5$. Soit α une racine de f. On constate alors que

$$P = (-1, 1) \quad \text{et} \quad Q = (\alpha, \alpha^3 + \alpha - 1)$$

sont deux points d'ordre 4 de E et que (P, Q) est une base du $\mathbb{Z}/4\mathbb{Z}$-module $E[4]$. En particulier, on a $\mathbb{F}_5(E[4]) = \mathbb{F}_5(\alpha)$ qui est de degré 4 sur $\mathbb{F}_5$. Soit ϕ_5 l'endomorphisme de Frobenius de E. On a $\phi_5(P) = P$ et $\phi_5(Q) = P + Q$. La matrice de $(\phi_5)_4$ dans la base (P, Q) est donc $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On retrouve ainsi avec cet exemple l'énoncé du théorème 4.7.

Exercice 7

Soient K un corps fini de cardinal q et E une courbe elliptique définie sur K. On suppose qu'il existe un entier $n \geq 1$ tel que les groupes

$$E(K) \quad \text{et} \quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

soient isomorphes. Posons

$$t = q + 1 - n^2.$$

1) Montrer que l'on a $t \equiv 2$ mod. n.

Posons

$$t = 2 + rn \quad \text{avec } r \in \mathbb{Z}.$$

2) Montrer que l'on a $|r| \leq 2$.

3) En déduire que q est l'un des entiers

$$n^2 + 1, \quad n^2 + n + 1, \quad n^2 - n + 1, \quad (n+1)^2, \quad (n-1)^2.$$

4) Supposons $q \equiv 11$ mod. 12. Montrer que l'hypothèse faite n'est jamais réalisée.

Exercice 8

Soient $\mathbb{F}_q$ un corps de cardinal q (une puissance d'un nombre premier) et E une courbe elliptique définie sur $\mathbb{F}_q$. Soit ℓ un nombre premier vérifiant les conditions suivantes :

(1) ℓ ne divise pas $q(q-1)$.

(2) ℓ divise $|E(\mathbb{F}_q)|$.

1) Soit $n \geq 1$ un entier. Montrer que le groupe $E[\ell]$ des points de ℓ-torsion de E est contenu dans $E(\mathbb{F}_{q^n})$ si et seulement si ℓ divise $q^n - 1$.

Soit E la courbe elliptique sur $\mathbb{F}_7$ d'équation

$$y^2 z = x^3 + xz^2 + 3z^3.$$

2) Déterminer le groupe $E(\mathbb{F}_7)$.

3) En déduire que 3 divise $|E(\mathbb{F}_7)|$ et que $E[3]$ n'est pas contenu dans $E(\mathbb{F}_7)$.

L'hypothèse que ℓ ne divise pas $q-1$ est donc indispensable dans l'énoncé de la première question ; on notera aussi que cet énoncé est faux si $\ell = q$.
De même, l'hypothèse que ℓ divise $|E(\mathbb{F}_q)|$ est nécessaire dans l'énoncé de cette question. En effet, soit E la courbe elliptique définie sur $\mathbb{F}_5$ intervenant dans l'exercice 6. On a $|E(\mathbb{F}_5)| = 8$ et $|E(\mathbb{F}_{25})| = 32$. Ainsi, avec $q = 5$ et $\ell = 3$, la condition (1) est

satisfaite, mais pas la condition (2). Par ailleurs, 3 divise 5^2-1 et le groupe $E[3]$, qui est d'ordre 9, n'est pas contenu dans $E(\mathbb{F}_{25})$.

4) Considérons le polynôme $f = X^3 - X^2 + 3X + 2 \in \mathbb{F}_7[X]$. Il est irréductible sur $\mathbb{F}_7$ (justifier pourquoi). Soit α une racine de f dans une clôture algébrique de $\mathbb{F}_7$. Posons

$$P = (-1, 1) \quad \text{et} \quad Q = (\alpha, \alpha - 1).$$

Montrer que (P, Q) est une base de $E[3]$.

5) Soit ϕ_7 l'endomorphisme de Frobenius de E. Expliciter la matrice de $(\phi_7)_3$ dans la base (P, Q).

Exercice 9

Soit E la courbe projective plane sur $\mathbb{F}_5$ d'équation

$$y^2z = x^3 - xz^2.$$

1) Montrer que E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) Décrire le groupe $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$. En déduire que $E(\mathbb{F}_5)$ est d'ordre 8.

3) Quels sont les points d'ordre 2 de $E(\mathbb{F}_5)$?

4) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_5)$.

5) Quelle est la trace du Frobenius de E ? Quel est le polynôme caractéristique du Frobenius de E ?

Soit $\overline{\mathbb{F}_5}$ une clôture algébrique de $\mathbb{F}_5$. Notons $\mathbb{F}_{25}$ le corps de cardinal 25 dans $\overline{\mathbb{F}_5}$.

6) Calculer l'ordre de $E(\mathbb{F}_{25})$.

7) Soit $P = (x, y)$ un point de $E\big(\overline{\mathbb{F}_5}\big)$.

7.1) Supposons $y \neq 0$. Calculer les coordonnées de $2P$.

Précision : En posant $2P = (u, v)$, on exprimera u et yv comme des fractions rationnelles en x.

7.2) En déduire que P est d'ordre 4 si et seulement si on a $x^6 + 1 = 0$.

Soit α un élément de $\overline{\mathbb{F}_5}$ tel que $\alpha^2 = 2$.

8) Justifier pourquoi on a $\mathbb{F}_{25} = \mathbb{F}_5(\alpha)$. Déterminer l'élément $w \in \mathbb{F}_5$ tel que $(1+\alpha)^3 = w$.

Posons

$$P = (2, 1), \quad Q = (3, 2) \quad \text{et} \quad R = (1 + \alpha, 2 + \alpha).$$

9) Vérifier que les points P, Q, R appartiennent à $E(\mathbb{F}_{25})$ et sont d'ordre 4.

10) Quel est le nombre d'éléments d'ordre 4 du groupe produit $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}, +)$?

11) En déduire que $E(\mathbb{F}_{25})$ n'est pas isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$.

12) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{25})$.

Soit $\mathbb{F}_{125}$ le corps de cardinal 125 dans $\overline{\mathbb{F}_5}$.

13) Calculer l'ordre de $E(\mathbb{F}_{125})$.

14) Déterminer la classe d'isomorphisme du groupe $E(\mathbb{F}_{125})$.

Exercice 10

Soit E la courbe projective plane sur $\mathbb{F}_5$ d'équation

$$y^2z = x^3 + xz^2 + z^3.$$

1) Montrer que E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) Décrire le groupe $E(\mathbb{F}_5)$ des points de E rationnels sur $\mathbb{F}_5$.

3) Pour tout point non nul $P \in E(\mathbb{F}_5)$, calculer les coordonnées de $2P$.

4) En déduire la description du sous-groupe des points de 3-torsion de $E(\mathbb{F}_5)$.

5) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_5)$.

6) Quel est le polynôme caractéristique du Frobenius de E ?

Notons $\mathbb{F}_{5^n}$ le corps de cardinal 5^n dans une clôture algébrique de $\mathbb{F}_5$.

7) Calculer les ordres des groupes $E(\mathbb{F}_{25})$ et $E(\mathbb{F}_{125})$.

Posons

$$f = X^2 - X + 2 \in \mathbb{F}_5[X].$$

C'est un polynôme est irréductible sur $\mathbb{F}_5$ (le justifier). Soit α une racine de f dans $\mathbb{F}_{25}$. Posons

$$Q = (\alpha + 3, 2\alpha + 3).$$

8) Vérifier que Q est un point de $E(\mathbb{F}_{25})$.

9) Calculer les coordonnées de $2Q$.

10) Posons $P = (2, 1)$. Montrer que (P, Q) est une base sur $\mathbb{F}_3$ du groupe des points de 3-torsion de E.

11) En déduire la classe d'isomorphisme du groupe $E(\mathbb{F}_{25})$.

12) Montrer que le polynôme $X^3 + X + 1 \in \mathbb{F}_5[X]$ est irréductible sur $\mathbb{F}_5$.

13) Quel est le corps de rationalité du groupe des points de 2-torsion de E ?

14) Déterminer la classe d'isomorphisme du groupe $E(\mathbb{F}_{125})$.

Exercice 11

Soit $p \geq 5$ un nombre premier vérifiant la congruence

$$p \equiv 3 \text{ mod. } 4.$$

Soit E la courbe projective plane définie sur $\mathbb{F}_p$ d'équation

$$y^2 z = x^3 - 6xz^2.$$

1) Montrer que E est une courbe elliptique définie sur $\mathbb{F}_p$.
2) Montrer que l'ordre du groupe $E(\mathbb{F}_p)$ est $p+1$.
3) Montrer que E a tous ses points d'ordre 2 rationnels sur $\mathbb{F}_p$ si et seulement si p est congru à 19 ou 23 modulo 24.
4) En déduire que le groupe $E(\mathbb{F}_p)$ est cyclique si et seulement si p est congru à 7 ou 11 modulo 24.

Soit $Q = (u, v)$ un point de $E(\mathbb{F}_p)$ tel que $v \neq 0$; on a $v^2 = u^3 - 6u$.

5) Montrer que l'abscisse de $2Q$ est

$$\left(\frac{u^2+6}{2v}\right)^2.$$

Le point $P = (-2, 2)$ appartient à $E(\mathbb{F}_p)$.

6) Supposons $p \equiv 7$ mod. 24. Montrer qu'il n'existe pas de points $Q \in E(\mathbb{F}_p)$ tels que l'on ait $2Q = P$.

Supposons qu'il existe un entier ℓ tel que l'on ait $p = 2^\ell - 1$ (autrement dit que p soit un nombre premier de Mersenne).

7) Vérifier que l'on a $p \equiv 7$ mod. 24.
8) Montrer que P est un générateur de $E(\mathbb{F}_p)$.

Indication : Utiliser le fait que si G un groupe cyclique additif, non réduit à l'élément neutre et d'ordre une puissance de 2, ses générateurs sont exactement les éléments qui ne sont pas de la forme $2x$ où $x \in G$.

9) Déterminer les coordonnées de $2^{\ell-1}P$.

Exercice 12 (Cryptosystème de Menezes-Vanstone)

Une personne Alice souhaite pouvoir se faire envoyer des messages confidentiels chiffrés sous forme d'éléments de $\mathbb{F}_p \times \mathbb{F}_p$. Pour cela, elle choisit une courbe elliptique E définie sur $\mathbb{F}_p$ et un point $P \in E(\mathbb{F}_p)$, de sorte que le problème du logarithme discret soit a

priori difficile à résoudre dans le sous-groupe de $E(\mathbb{F}_p)$ engendré par P. Elle choisit par ailleurs un entier $s > 0$ et calcule le point

$$A = sP.$$

Alice rend public le triplet (E, P, A), qui la clé publique de l'algorithme, et garde secret l'entier s, qui est la clé secrète.

Supposons que Bob souhaite faire parvenir à Alice le message $m = (m_1, m_2) \in \mathbb{F}_p \times \mathbb{F}_p$. Pour cela, il choisit un entier $k > 0$ et calcule les points

$$kP \quad \text{et} \quad kA = (x, y),$$

de sorte que xy soit non nul. Il envoie alors à Alice le point kP et le couple $(m_1 x, m_2 y)$ de $\mathbb{F}_p \times \mathbb{F}_p$ (qui n'est pas a priori un point de $E(\mathbb{F}_p)$).

1) Comment Alice peut-elle déchiffrer le message m ?

Exemple : Soit E la cubique définie sur $\mathbb{F}_{11}$ d'équation

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

2) Montrer que E est une courbe elliptique sur $\mathbb{F}_{11}$.
3) Déterminer l'ordre du groupe $E(\mathbb{F}_{11})$.

On constate que le point $P = (2, 7)$ appartient à $E(\mathbb{F}_{11})$. Bob souhaite envoyer le message $m = (9, 1) \in \mathbb{F}_{11} \times \mathbb{F}_{11}$ à Alice en utilisant le cryptosystème précédent avec le couple (E, P). La clé secrète d'Alice est l'entier $s = 7$.

4) Calculer la clé publique d'Alice.
5) Bob choisit l'entier $k = 6$. Quel est le message chiffré envoyé par Bob ?
6) Comment Alice retrouve-t-elle le message m ?