Exercices sur les courbes elliptiques

Les exercices qui suivent sont indépendants et sont de difficultés variables. Plusieurs d'entre eux sont des exercices d'application directe du cours. Tous les exercices sont classés en thèmes. Chacun de ces thèmes contient un ou plusieurs exercices. Vous ne pouvez réellement profiter de leurs corrigés que si vous les avez préalablement cherchés.

Equations de Weierstrass en caractéristique 2 et 3

1. Soit E une courbe de Weierstrass définie sur un corps $\mathbb{K}$ de caractéristique $p = 2$ ou 3 par l'équation affine $(E) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Montrer que E est équivalente à une courbe E' d'équation de la forme :

1) $E' : y'^2 = x'^3 + a'_2x'^2 + a'_6$ si $p = 3$ et $a_1^2 + a_2 \neq 0$ et on a $\Delta(E') = -a'^3_2a'_6$
2) $E' : y'^2 = x'^3 + a'_4x' + a'_6$ si $p = 3$ et $a_1^2 + a_2 = 0$ et on a $\Delta(E') = -a'^3_4$
3) $E' : y'^2 + x'y' = x'^3 + a'_2x'^2 + a'_6$ si $p = 2$ et $a_1 \neq 0$ et on a $\Delta(E') = a'_6$
4) $E' : y'^2 + a'_3y' = x'^3 + a'_4x' + a'_6$ si $p = 2$ et $a_1 = 0$ et on a $\Delta(E') = a'^4_3$

2. Soit E une courbe de Weierstrass définie sur un corps $\mathbb{K}$ de caractéristique 2 ou 3. On suppose que $\Delta(E) = 0$. Montrer que E n'est pas lisse en montrant qu'elle admet un unique point singulier que l'on précisera.

3. Soit $\mathbb{K}$ un corps de caractéristique égale à 2 ou 3. Montrer que deux courbes de Weierstrass E et E' définies sur $\mathbb{K}$, de discriminants respectifs $\Delta \neq 0, \Delta' \neq 0$ et d'invariants modulaires $j = j'$, sont équivalentes sur $\overline{\mathbb{K}}$.

Lissité et discriminant de courbes de Weierstrass

4. Soit $\mathbb{K}$ un corps algébriquement clos de caractéristique $\neq 2, 3$.

1) Démontrer qu'un polynôme $P \in \mathbb{K}[X]$ a une racine multiple si et seulement si P et et son polynôme dérivé P' ont une racine commune.
2) Démontrer que le polynôme $P = X^3 + aX + b$ à coefficients dans $\mathbb{K}$, n'a pas de racines multiples si et seulement si $4a^3 + 27b^2 \neq 0$
3) Démontrer que la courbe de Weierstrass E définie sur $\mathbb{K}$ par l'équation affine $y^2 = P(x) = x^3 + ax + b$ est lisse si et seulement si $4a^3 + 27b^2 \neq 0$

Loi de groupe sur les courbes elliptiques

5. On considère la courbe E définie sur $\mathbb{Q}$ par l'équation $E : y^2 = x^3 - 25x$. Vérifier que cette courbe est lisse et calculer $P + Q$ pour $P = (-4, 6)$ et $Q = (0, 0)$.

6. On considère la courbe E définie sur $\mathbb{F}_{17}$ par l'équation $E : y^2 = x^3 + x + 7$.

1) Vérifier que E est lisse et que les points $P = (6, 5), Q = (2, 0)$ appartiennent à E.

2) Calculer les points $2P, 2Q, P + Q, P - Q, Q - P$

7. On considère la courbe elliptique E définie sur $\mathbb{F}_7$ par l'équation $E : y^2 = x^3 - x + 1$. Établir la liste des points du groupe $E(\mathbb{F}_7)$.

Fonctions rationnelles sur $\mathbb{P}^1$

8. Soit $r(x)$ une fraction rationnelle de $\mathbb{K}(x)$. Démontrer que si $\mathrm{ord}_\infty(r) = d$ alors $r(x)$ s'écrit sous la forme $r(x) = \left(\frac{1}{x}\right)^d s(x)$ avec $s(x)$ une fonction rationnelle de $\mathbb{K}(x)$ non nulle pour laquelle ∞ n'est ni zéro ni pôle.
Application : pour $r(x) = (x - 1)(x + 1)$ trouver l'entier d et la fonction s.

9. Soit le polynôme $F = \beta X - \alpha T \in \mathbb{K}[\mathbb{P}^1]$ et $P = [a : b] \in \mathbb{P}^1$. Calculer $\mathrm{ord}_P(F)$.

10. Soit $\mathbb{P}^1$ la droite projective sur $\mathbb{K} = \mathbb{R}$. Montrer que l'application

$$\varphi : \mathbb{P}^1 \longrightarrow \mathbb{R}^2,\ t \longmapsto \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$$

définit une bijection notée encore φ de $\mathbb{P}^1$ sur un ensemble S que l'on déterminera et expliciter la bijection réciproque φ^{-1}.

Morphismes et applications rationnelles de courbes

11. Soient la courbe plane (lisse) C définie sur $\mathbb{R}$ par l'équation homogène $X^2 + Y^2 - T^2 = 0$ et soit $F = \dfrac{X + T}{Y} \in \mathbb{R}(C)$.

1) Montrer que dans $\mathbb{R}(C)$ on a l'égalité $\dfrac{X + T}{Y} = \dfrac{-Y}{X - T}$

2) Définir le morphisme ou l'application rationnelle $f : C \to \mathbb{P}^1$ correspondant à F

3) Calculer les pôles et zéros de f

4) Reprendre les deux dernières questions avec $(C) : X^3 + X^2T - Y^2T = 0$ et $F = \dfrac{Y}{X}$

12. On considère la courbe C définie sur $\mathbb{R}$ par l'équation homogène (C) et on considère le morphisme $\phi : \mathbb{P}^1 \longrightarrow C$ défini sur $\mathbb{R}$ où

$$(C) : X^2 + Y^2 - XT = 0$$

$$\phi : \mathbb{P}^1 \longrightarrow C \ , \ [X : T] \longmapsto \phi([X : T]) = [T^2 : XT : X^2 + T^2]$$

1) Calculer $\phi(P)$ pour $P = [\alpha : 1]$ et pour $P = [1 : \gamma]$

2) Montrer que ϕ est un isomorphisme en calculant son inverse

3) Calculer l'homomorphisme de corps $\phi^* : \mathbb{R}(C) \longrightarrow \mathbb{R}(\mathbb{P}^1)$ associé à ϕ

Fonctions rationnelles sur les courbes elliptiques

13. On considère la courbe elliptique E définie sur $\mathbb{K} = \mathbb{F}_{11}$ par l'équation $E : y^2 = x^3 + 6$ et on considère la fonction $f(x, y) = -2x - y + 4 \in \mathbb{K}[E]$ et le point $P = (-2, 8) \in E$. Calculer $\mathrm{ord}_P(f)$ et en déduire $2P$.

14. Soit E une courbe de Weierstrass sur $\mathbb{K}$, $P \in E$ un point ordinaire. Si la fonction rationnelle $f(x, y) \in \overline{\mathbb{K}}(E)$ est une fonction $r(x)$ en x seulement, montrer que $\mathrm{ord}_P(f) = \mathrm{ord}_{x_P}(r)$ puis que cette propriété est fausse si P est un point spécial ?

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

$$E : y^2 = x^3 - 7x + 6$$

et soit la fonction polynôme $h(x, y) = x^3 - (x^2 - 1)y - 1 \in \mathbb{Q}[E]$

1) Calculer les points spéciaux de E.

2) Soit $P = (1, 0) \in E$. Calculer $\mathrm{ord}_P(h)$ en mettant la fonction h sous la forme $h = u^d r$ pour une uniformisante u en P et une fonction r qui n'a ni zéro, ni pôle en P.

3) On note (C) la courbe d'équation $h(x, y) = 0$. Que peut-on dire des courbes E et (C) au point P. Retrouver ce résultat directement.

16. Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $\neq 2$ par l'équation $y^2 = x^3 + ax + b$. Soit $Q = (u, v) \in E$ et soit $g(x, y) \in \overline{\mathbb{K}}(E)$ la fonction rationnelle définie par

$$g(x, y) = \frac{y - v}{x - u}$$

Quelle est la valeur de $g(Q)$?

17. Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $\neq 2$ et soit $f(x, y) \in \overline{\mathbb{K}}(E)$ la fonction rationnelle sur E définie par

$$f(x, y) = \frac{x^2 + y}{yx}$$

Calculer $\mathrm{ord}_{\mathcal{O}}(f)$ en écrivant $f = u^d r$ avec u une uniformisante en $\mathcal{O}$ et $r(\mathcal{O}) \neq 0, \infty$.

18. Soit $P = (x_0, y_0)$ un point ordinaire d'une courbe elliptique E définie sur un corps $\mathbb{K}$ de caractéristique $\neq 2$. Soit $f(x, y) \in \overline{\mathbb{K}}[E]$ une fonction polynôme sur E dont la forme réduite est $f(x, y) = p(x) + yq(x)$. Démontrer que si P est un zéro de f et si x_0 n'est pas à la fois racine de $p(x)$ et de $q(x)$, alors $\overline{f}(P) \neq 0$.

Diviseurs sur les courbes elliptiques

19. Montrer que toute fonction rationnelle non nulle f sur la droite projective $\mathbb{P}^1$ peut s'écrire sous la forme $f = \prod_i (\beta_i X - \alpha_i T)^{n_i}$ où les ni sont dans $\mathbb{Z}$ puis calculer $\mathrm{div}(f)$

20. On considère sur le corps $\mathbb{F}_{11}$ la courbe elliptique E d'équation

$$E : y^2 = x^3 + x + 3$$

et on considère les points $P = (1, 4), Q = (3, 0), R = (0, 6), S = (1, 7)$ de E.

1) Calculer $\mathrm{div}(g)$ où $g(x, y)$ est la droite passant par S et $-S$.
2) Calculer $\mathrm{div}(t)$ où $t(x, y)$ est la tangente à la courbe en R.
3) Calculer $\mathrm{div}(h)$ où $h(x, y)$ est la droite passant par P et Q.
4) Calculer $\mathrm{div}(\ell)$ où $\ell(x, y)$ est la tangente à la courbe en P.
5) Calculer $\mathrm{div}(d)$ où $d(x, y)$ est la tangente à la courbe en Q.

21. Soit E la courbe elliptique sur $\mathbb{F}_{11}$ définie par l'équation

$$E : y^2 = x^3 + 5x + 4$$

Vérifier que les points $P_1 = (10, 3)$ et $P_2 = (5, 0)$ appartiennent à E et calculer $P_3 = P_1 + P_2$. Donner une fonction de $\mathbb{F}_{11}(E)$ dont le diviseur est $D = (P_1) + (P_2) - (P_3) - (\mathcal{O})$.

22. Soit E la courbe elliptique sur $\mathbb{F}_5$ définie par l'équation

$$y^2 = x^3 + x + 4$$

On considère les points $P = (1, 1), Q = (2, 2), R = (0, 3)$ de E.

1) Calculer $S = P + Q, T = P + R, U = P + Q + R$
2) Soit le diviseur $D = (Q) - (S) - (R) + (T)$. Montrer que D est principal et donner une fonction de $f(x, y) \in \mathbb{F}_5(E)$ telle que $\mathrm{div}(f) = D$.

23. Soit E la courbe elliptique définie sur $\mathbb{F}_{11}$ par l'équation

$$E : y^2 = x^3 + 6x + 8$$

Vérifier que $P := (1, 2) \in E$ et calculer $\mathrm{div}(\ell)$ pour $\ell(x, y) = 2x + 4y + 1$.

24. Soit $P = (x_0, y_0)$ un point ordinaire d'une courbe elliptique E définie sur un corps $\mathbb{K}$ algébriquement clos de caractéristique $\neq 2$, par l'équation $y^2 = x^3 + ax + b$. Soit $Q = -2P$. On suppose que la droite (PQ) a pour équation

$$f(x, y) = u(x - x_0) + v(y - y_0)$$

1) Montrer que $v \neq 0$ et donner des expressions de u et v.
2) Montrer que $\mathrm{ord}_P(f) \geqslant 2$. En déduire $\mathrm{ord}_P(f), \mathrm{ord}_Q(f)$ et $\mathrm{div}(f)$.

25. Soit E la courbe elliptique sur $\mathbb{F}_{11}$ définie par l'équation

$$E : y^2 = x^3 + 2x$$

Soit $P = (1, 5) \in E$ et $Q = (0, 0) \in E$.

1) Calculer $U = 2P$ et vérifier que $3P = \mathcal{O}$ où $\mathcal{O}$ est le point à l'infini de E.
2) Soit la fonction de $\mathbb{F}_{11}(E)$ définie par $f(x, y) = 5x - y + 1$. Déterminer l'ordre de f en U puis calculer $\mathrm{div}(f)$.
3) Déterminer une fonction f_1 telle que $(P) + (Q) = (P + Q) + (\mathcal{O}) + \mathrm{div}(f_1)$

4) Déterminer une fonction f_2 telle que $(P) + (P+Q) = (2P+Q) + (\mathcal{O}) + \text{div}(f_2)$

5) Déterminer une fonction f_3 telle que $(P) + (2P+Q) = (Q) + (\mathcal{O}) + \text{div}(f_3)$

6) En déduire une fonction g telle que $\text{div}(g) = 3(P) - 3(\mathcal{O})$.

26. Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ algébriquement clos par l'équation

$$E : y^2 = x^3 + ax + b$$

Soit $P = (\alpha, 0)$ un point spécial et $s(x)$ un polynôme de $\mathbb{K}[x]$ tel que $s(\alpha) = 0$. Démontrer que l'ordre de s en P est pair.

27. Soit E une courbe elliptique définie sur un corps algébriquement clos $\mathbb{K}$ de caractéristique $\neq 2$ et soit $f \in \mathbb{K}[E]$ une fonction polynôme non constante. Démontrer que f a toujours au moins deux zéros, ou au moins un zéro d'ordre $\geqslant 2$.

28. Soit E une courbe elliptique définie sur un corps algébriquement clos $\mathbb{K}$ de caractéristique $\neq 2$, par l'équation

$$E : y^2 = x^3 + ax + b$$

Soit $Q = (x_0, y_0) \in E$ et soit $\lambda \in \mathbb{K}(E)$ la fonction définie par

$$\lambda(x, y) = \frac{y - y_0}{x - x_0}$$

1) On suppose que Q est un point spécial. Montrer que λ a un pôle d'ordre (-1) en Q et déterminer le diviseur $\text{div}(\lambda)$ de λ.

2) On suppose que Q est un point ordinaire (donc $y_0 \neq 0$). Quelle est la valeur de $\lambda(x, y)$ en Q ? Déterminer le diviseur de λ ?

29. Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ algébriquement clos de caractéristique $\neq 2$ et soit $f(x, y) \in \mathbb{K}(E)$. On pose $f(x, y) = r(x) + ys(x)$ sa forme réduite. Démontrer que si f n'a pas de pôle fini, alors c'est une fonction polynôme *i.e.* $f \in \mathbb{K}[E]$. (On distinguera les cas $s = 0$ et $s \neq 0$.)

Ramification de morphismes de $\mathbb{P}^1$

30. Soient $\mathbb{K}$ un corps de caractéristique $p > 0$. On considère le morphisme

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1; [X : T] \longmapsto \phi(X, T) = [X^n : T^n]$$

Définir le morphisme $\phi^* : \mathbb{K}(\mathbb{P}^1) \longrightarrow \mathbb{K}(\mathbb{P}^1)$ et calculer $e_\phi(P)$ où $P = [\alpha : 1] \in \mathbb{P}^1$.

31. Soit $\mathbb{K}$ un corps de caractéristique $\neq 2, 3, 5$. On considère le morphisme

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1 \,;\, [X : T] \longmapsto [X^3(X-T)^2 : T^5]$$

1) Définir le morphisme $\phi^* : \mathbb{K}(\mathbb{P}^1) \longrightarrow \mathbb{K}(\mathbb{P}^1)$ associé à ϕ
2) Calculer les images réciproques $\phi^{-1}([1:0])$ et $\phi^{-1}([0:1])$
3) Calculer $e_\phi([0:1]), e_\phi([1:1]), e_\phi([1:0])$ et $e_\phi([a:1])$ pour $a \neq 0, 1$

Propriétés de la forme réduite de l'isogénie $[n]$

32. Soit E une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $\neq 2$ par l'équation

$$y^2 = F(x) = x^3 + ax + b$$

et soit n un entier naturel non nul. On note $(r_n(x), ys_n(x))$ la forme réduite de l'isogénie

$$[n] : E \longrightarrow E \,;\, P = (x, y) \longmapsto [n](P) = nP = (r_n(x), ys_n(x))$$

1) Calculer la forme réduite $(r_2(x), ys_2(x))$ de l'isogénie [2]
2) En déduire l'indice de ramification de l'isogénie [2]
3) Montrer par récurrence sur n que l'on a $r_n'(x) = ns_n(x)$
4) En déduire que l'isogénie $[n]$ est séparable si et seulement si n n'est pas multiple de la caractéristique du corps $\mathbb{K}$.
5) Montrer que pour tout entier $n \geqslant 2$ on a

$$r_n'' = \frac{n^2(3r_n^2 + a) - r_n'(3x^2 + a)}{2(x^3 + ax + b)} \tag{1}$$

6) Montrer que si n n'est pas multiple de la caractéristique du corps $\mathbb{K}$ alors on a

$$\deg(r_n) = 2, \quad \deg(s_n) = 0, \quad \frac{r_n}{x}(\mathcal{O}) = \frac{1}{n^2}, \quad s_n(\mathcal{O}) = \frac{1}{n^3}$$

7) Soit n un entier $\geqslant 2$ et premier à la caractérisique de $\mathbb{K}$ et soit P un point de E. On suppose que nP est un point spécial de E. Montrer que

$$\begin{aligned} s_n(x_P) &= 0 \quad \text{si } P \text{ est un point ordinaire de } E \\ s_n(x_P) &\neq 0 \quad \text{si } P \text{ est un point spécial de } E \end{aligned}$$

8) Si $P = (\alpha, 0) \in E$ est un point spécial et si n est impair alors $s_n(\alpha) = n$.

Isogénies de courbes elliptiques

33. Soit E une courbe elliptique sur un corps $\mathbb{K}$ et soit φ une isogénie de E.

1) Pourquoi si $\ker\varphi$ est infini alors φ est nécessairement l'isogénie nulle $P \to \mathcal{O}$?

2) Montrer que si φ est de degré n alors $\ker\varphi \subset \ker[n]$.

3) Montrer que pour tout entier $n \geqslant 1$, $[n]$ commute avec toute isogénie φ

4) Si $\mathbb{K}$ est fini de cardinal q quel est le noyau du Frobenius φ_q ? En déduire son degré.

34. Soit $\mathbb{K}$ un corps algébriquement clos de caractéristique $\neq 2$, soit $b \in \mathbb{K}^*$ et j une racine cubique primitive de l'unité dans $\mathbb{K}$. On considère la courbe elliptique E définie sur $\mathbb{K}$ par l'équation $E : y^2 = x^3 + b$ et on pose $\varphi(x, y) = (x, jy)$. Justifier les assertions suivantes :

1) φ définit un morphime de E dans E

2) φ est une isogénie de E.

3) φ est une bijection de E sur E

4) φ est non ramifiée

5) φ est degré égal à 1

6) φ est séparable

35. Soit E une courbe elliptique sur un corps $\mathbb{K}$ de caractéristique $\neq 2$. Soit $(r(x), ys(x))$ la forme réduite d'une isogénie φ non nulle de E. Montrer les égalités suivantes sur les degrés en x des fonctions rationnelles r et s de $\overline{\mathbb{K}}(x)$

$$\deg_x(r) = e_\varphi \quad \text{et} \quad \deg_x(s) = \frac{3}{2}(e_\varphi - 1)$$

Puis justifier que la quantité $\dfrac{3}{2}(e_\varphi - 1)$ est toujours entière ?

Le groupe $E[n]$ de n-torsion et les polynômes de division

36. On considère la courbe elliptique E définie sur le corps fini $\mathbb{F}_7$ par l'équation

$$E : y^2 = x^3 - x$$

1) Calculer les points du groupe $E(\mathbb{F}_7)$

2) Déterminer les points du groupe $E[2]$

3) Donner la structure du groupe $E(\mathbb{F}_7)$

37. On considère la courbe elliptique E définie sur le corps fini $\mathbb{F}_5$ par l'équation

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

1) Déterminer les points du groupe $E(\mathbb{F}_5)$

2) On pose $\mathbb{K} = \mathbb{F}_5[X]/(X^2 - 2)$. Montrer que $\mathbb{K}$ est un corps à 25 éléments contenant un élément qu'on notera $\sqrt{2}$ dont le carré est égal à 2 et que $\mathbb{K} = \mathbb{F}_5(\sqrt{2})$.

3) Vérifier que les points $R = (3, 2)$ et $S = (4, \sqrt{2})$ appartiennent à $E(\mathbb{K})$.

4) Calculer $2R$ et $2S$ et en déduire que R et S sont des points de 3-torsion.

5) Démontrer que (R, S) est une base du groupe $E[3]$.

6) En déduire les points du groupe $E[3]$

7) Ecrire la matrice Φ_5 dans la base (R, S) de la restriction de l'isogénie de Frobenius φ_5 au groupe $E[3]$.

8) Vérifier que $tr(\Phi_5) \equiv t(E(\mathbb{F}_5)) \pmod 3$

38. (*Degré des polynômes de division*) Soit n un entier et ψ_n le n^e polynôme de division d'une courbe elliptique E. Pour un point fini P de E on note (x_P, y_P) ses coordonnées.

1) Démontrer que pour tout point P de E on a :

$$\psi_n(P)^2 = n^2 \prod_{R \in E[n] - \{\mathcal{O}\}} (x_P - x_R)$$

2) En déduire que si n est impair, alors la forme réduite de ψ_n est un polynôme en x seulement et que $\deg_x(\psi_n) = \dfrac{n^2 - 1}{2}$

3) En déduire également que si n est pair, alors la forme réduite de ψ_n est de la forme $y f_n(x)$, où f_n est un polynôme en x et $\deg_x(f_n) = \dfrac{n^2 - 4}{2}$.

39. On considère la courbe elliptique E définie sur $\mathbb{F}_{11}$ par l'équation

$$E : y^2 = x^3 + x - 3$$

1) Calculer les points du groupe $E(\mathbb{F}_{11})$

2) Factoriser sur $\mathbb{F}_{11}$ le polynôme de division ψ_3

3) On pose $\mathbb{K} = \mathbb{F}_{11}[X]/(X^2-6)$. Montrer que $\mathbb{K}$ est un corps à 121 éléments contenant un élément qu'on notera $\sqrt{6}$ dont le carré est égal à 6 et que $\mathbb{K} = \mathbb{F}_{11}(\sqrt{6})$.
4) Calculer les points de 3-torsion dans $E(\mathbb{K})$ *i.e.* l'ensemble $E(\mathbb{K})[3]$
5) En déduire que $E[3] = E(\mathbb{K})[3]$ et que $\{(-2,3),(-1,\sqrt{6})\}$ est une base de $E[3]$.
6) Vérifier que $tr(\Phi_5) \equiv t(E(\mathbb{F}_5)) \pmod 3$

40. Soit E la courbe elliptique définie sur $\mathbb{F}_{11}$ par l'équation

$$E : y^2 = x^3 + x + 2$$

1) Calculer le polynôme de division $\psi_4(x,y) = yf_4(x)$
2) Trouver les racines de f_4 dans $\mathbb{F}_{11}$.
3) En déduire les abscisses des points de 4-torsion dans le corps $\mathbb{K} = \mathbb{F}_{11}(\sqrt{7})$.
4) Déterminer les points de 4-torsion dont les coordonnées sont dans $\mathbb{F}_{11}$.
5) Montrer que $R = (1,2)$ et $S = (0,\sqrt{2})$ engendrent $E[4]$ et que $E[4] = E(\mathbb{K})[4]$.

Courbe elliptique sur un corps fini

41. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique $\neq 2$, par

$$(E) : y^2 = x^3 + ax + b$$

1) Qui sont les points d'ordre de 2 de E ? A quelle condition un tel point appartient au groupe $E(\mathbb{F}_q)$?
2) Montrer que la trace $t(E(\mathbb{F}_q))$ est paire si et seulement si le groupe $E(\mathbb{F}_q)$ contient un point d'ordre 2.
3) En déduire que t est impair si et seulement si les polynômes $X^q - X$ et $X^3 + aX + b$ de $\mathbb{F}_q[X]$ sont premiers entre eux.
4) Soit l'application (caractère) $\chi : \mathbb{F}_q \to \{-1,0,1\}$ définie par

$$\chi(z) = \begin{cases} 1 & \text{si } z \text{ est un carré dans } \mathbb{F}_q^* \\ -1 & \text{si } z \text{ n'est pas un carré dans } \mathbb{F}_q^* \\ 0 & \text{si } z = 0 \end{cases}$$

Montrer que

$$\mathrm{Card}(E(\mathbb{F}_q)) = q + 1 + \sum_{x \in \mathbf{F}_q} \chi(x^3 + ax + b)$$

42. Soit p un nombre premier impair $\equiv 2 \pmod 3$ et soit E la courbe elliptique définie sur le corps fini $\mathbb{F}_p$ par l'équation

$$E : y^2 = x^3 + 1$$

1) Démontrer que l'application $f : x \mapsto x^3$ est une bijection de $\mathbb{F}_p$ sur lui même.
2) Montrer que pour tout $y_0 \in \mathbb{F}_p$, il existe un unique point de $E(\mathbb{F}_p)$ d'ordonnée y_0.
3) En déduire que Card $E(\mathbb{F}_p) = p + 1$.

Couplage de Weil sur les courbes elliptiques

43. Soit $T = (\alpha, 0)$ un point spécial d'une courbe elliptique E sur un corps $\mathbb{K}$ et soit $n \geqslant 2$ un entier pair. Donner une expression de la fonction f_T dont le diviseur est $n(T) - n(\mathcal{O})$.

44. Soit $n \geqslant 2$ un entier et e_n le couplage de Weil sur une courbe elliptique E définie sur un corps K. Démontrer que pour tout point $P \in E[n]$ on a $e_n(\mathcal{O}, P) = 1$.

45. Soit $n \geqslant 2$ un entier et e_n le couplage de Weil sur une courbe elliptique E définie sur un corps $\mathbb{K}$ et soit (T_1, T_2) une base du groupe $E[n]$. Démontrer que $e_n(T_1, T_2)$ est une racine primitive n-ième de l'unité *i.e.* un élément d'ordre n dans $\mathbb{K}^*$.

46. (*Un calcul de du couplage de Weil sur un exemple*)
Soit E la courbe elliptique définie sur $\mathbb{F}_7$ par l'équation

$$E : y^2 = x^3 + 2$$

1) Dresser la liste des points de $E(\mathbb{F}_7)$
2) Calculer le polynôme de division ψ_3. En déduire que tous les points finis de $E(\mathbb{F}_7)$ sont d'ordre 3. Quelle est la structure du groupe $E(\mathbb{F}_7)$.
3) Soit $S = (0, 3), T = (5, 1)$. Calculer la fonction unitaire f_S dont le diviseur est $3(S) - 3(\mathcal{O})$ et la fonction unitaire f_T dont le diviseur est $3(T) - 3(\mathcal{O})$
4) En déduire la valeur de $e_3(S, T)$. Vérifier qu'il s'agit bien d'une racine cubique de l'unité dans $\mathbb{F}_7$.

47. (*Loi de réciprocité de Weil sur un exemple*)
On considère la courbe elliptique E définie sur un corps de caractéristique $\neq 2, 3$, par l'équation :

$$E : y^2 = x^3 - 7x + 6$$

1) Déterminer les points spéciaux P_1, P_2, P_3 de E.

2) Soit $P = (x_P, y_P) \in E$ un point ordinaire, soit $Q \in E$ l'un des deux points d'abscisse $x_Q = 0$ et soient $f, g \in \overline{\mathbb{K}}(E)$ les fonctions rationnelles sur E définies par

$$f(x, y) = x - x_P \quad \text{et} \quad g(x, y) = \frac{x^3}{y^2}$$

Calculer $g(\mathcal{O}), \mathrm{div}(f)$ et $\mathrm{div}(g)$.

3) Pour toute fonction non nulle $h \in \overline{\mathbb{K}}(E)$ et pour diviseur $D = \sum_{P \in E} n_P(P) \in \mathrm{Div}(E)$ dont le support est disjoint à celui de $\mathrm{div}(h)$ on définit l'élément $h(D) \in \overline{\mathbb{K}}$ par :

$$h(D) = \prod_{P \in E} h(P)^{n_P}$$

Vérifier, en calculant chaque membre que $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$.