TD Courbes Elliptiques 2 et 3

Damien Robert

12 Janvier 2016

1 Résultant

Exercice 1.1. Soit K un corps tel que les polynômes $P(x) = x^3 - 1$ et $Q(x) = x^2 + 3x + 1$ aient une racine commune. Quelle est la caractéristique de K ?

Exercice 1.2. Soit α_1, α_2 et α_3 les trois racines du polynôme $A(x) = x^3 + 5x + 7$. Calculer $B(x) = (x - \alpha_1^2)(x - \alpha_2^2)(x - \alpha_3^2)$.

Exercice 1.3. Soit $C \subset \mathbb{R}^2$ la courbe paramétrisée par les équations

$$x(t) = \frac{4t(1-t^2)^2}{(1+t^2)^3}$$
$$y(t) = \frac{8t^2(1-t^2)^2}{(1+t^2)^3}.$$

Donne une équation de la courbe C.

Exercice 1.4. Calculer le discriminant du polynôme $f(x) = x^3 + ax + b$.

2 Modèle de Weierstrass

Une courbe elliptique E sur un corps K est définie par une équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

où les coefficients a_1, a_2, a_3, a_4, a_6 sont des éléments de K tels le **discriminant** de la courbe E soit non nul. En abrégé,

$$E = [a_1, a_2, a_3, a_4, a_6].$$

Dans le cas où la caractéristique de K est différente de 2 ou 3, toute courbe elliptique sur K admet une équation de la forme

$$y^2 = x^3 + a_4x + a_6$$

Le discriminant de cette courbe est $\Delta = -16(4a_4^3 + 27a_6^2)$.

Il faut enfin noter que deux équations distictes peuvent définir la même courbe elliptique, et que le discriminant est rattaché à l'équation, et pas à la courbe elle-même.

Exercice 2.1. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par l'équation à coefficients entiers

$$y^2 + y = x^3 - x^2 - 10x - 20$$

1. Consulter l'aide de la fonction `ellinit`.

2. Quel est le discriminant de E ? Et son invariant j ?
3. En utilisant un changement de variables admissible, déterminer une équation de la courbe E sous la forme
$$y^2 = x^3 + px + q$$
où p et q sont dans $\mathbb{Q}$.
4. Retrouver le résultat précédent en utilisant la fonction `ellchangecurve`.
5. Soit $F =$ `ellchangecurve`$(E, [1/3, 0, 0, 0])$. Comparer le discriminant et l'invariant j de F avec ceux de E.

Exercice 2.2.

1. Écrire une fonction qui vérifie qu'un point est sur une courbe elliptique.
2. Écrire une fonction qui prend deux points d'une courbe elliptique et retourne leur somme.
3. Tester cette fonction sur la courbe $E : y^2 = x^3 + 17$ et les points $P_1 = (-2, 3)$ et $P_2 = (-1, 4)$.
4. Calculer des multiples $n_1P_1 + n_2P_2$.

Exercice 2.3.

1. Effectuer dans gp la commande $E =$ `ellinit("1112a1")`. Qu'est-ce que cela signifie ? Quelle est l'équation de la courbe E ?
2. Soit $P = (1, 1)$. Vérifier que P est sur la courbe E.
3. Consulter l'aide de la fonction `ellmul`.
4. Calculer $[n]P$ pour des petites valeurs de n.

Exercice 2.4. Soit E une courbe elliptique définie sur un corps K.

1. Écrire une procédure `ellpuissance`(E, P, n) basée sur la méthode d'exponentiation binaire permettant de calculer $[n]P$ où n est un entier naturel et $P \in E(K)$ est un point de E.
2. Comparer la vitesse d'exécution de cette procédure à celle de la fonction `ellmul`. On pourra tester l'exemple $E = 1112a1$ et $P = (1, 1)$
3. Soit $E : y^2 = x^3 + 256$. Vérifier que $P = (0, 16)$ est bien sur la courbe elliptique, et est un point de torsion. Calculer son ordre à l'aide de la procédure précédente.
4. Même question avec $E : y^2 = x^3 + x/4$ et $P = (1/2, 1/2)$.
5. Même question avec $E : y^2 = x^3 - 43x + 166$ et $P = (3, 8)$.

3 Modèle d'Edwards

Le modèle de Weierstrass d'une courbe elliptique E est une équation
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
où les coefficients a_i sont des éléments d'un corps $\mathbb{K}$. En abrégé, $E = [a_1, a_2, a_3, a_4, a_6]$.

On peut cependant utiliser un autre système de coordonnées, les coordonnées d'Edwards, basé sur un modèle du type
$$x^2 + y^2 = c^2(1 + dx^2y^2).$$

où on impose $cd(1-dc^4) \neq 0$. Il n'y a plus que deux paramètres, donc ici $E = [c, d]$.

La loi d'addition est alors donnée par

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right).$$

On remarque que les formules d'addition fournissent directement la formule de duplication, contrairement au cas du modèle de Weierstrass où on utilise la loi corde-tangente. Par contre le modèle d'Edwards est une courbe singulière, pour être complètement rigoureux il faut donc résoudre les singularités pour obtenir une courbe elliptique. On peut cependant utiliser ces coordonnées pour gagner un peu de temps dans les calculs explicites.

Vérifiez que :

1. Le neutre pour l'addition est le point $(0, c)$.
2. L'opposé d'un point (x, y) est le point $(-x, y)$.

Exercice 3.1.

1. Écrire une fonction `Edwardsinit`(c, d) qui initialise un modèle d'Edwards de paramètres c et d. Cette fonction doit afficher l'équation de la courbe en retour.
2. Écrire une fonction `Edwardsisoncurve`(E, P) qui teste si le point P est sur la courbe d'Edwards E.
3. Étant donné une courbe elliptique E et deux points P et Q de E, écrire une fonction `Edwardsadd`(E, P, Q) qui calcule $P + Q$ sur le modèle d'Edwards E en utilisant la nouvelle loi d'addition.
4. Sur un modèle $E = [c, d]$, calculer l'ordre des points $(0, -c)$, $(c, 0)$ et $(-c, 0)$.

Exercice 3.2. On va étudier un exemple de passage d'une forme de Weierstrass à une forme d'Edwards. Tout repose sur la remarque suivante : génériquement, une équation du type $x^2 + y^2 = 1 + dx^2y^2$ est birationnellement équivalente à une équation du type

$$\frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u.$$

Il suffit d'utiliser le changement de coordonnées $(u, v) \mapsto (x, y)$ avec

$$x = 2u/v \qquad \text{et} \qquad y = (u-1)/(u+1)$$

1. On consière la courbe d'équation $E_1 : t^2 = s^3 + 3s^2 + s$. Montrer qu'elle est équivalente à la courbe $E_2 : x^2 + y^2 = 1 + 5x^2y^2$.
2. Écrire une fonction qui transforme les points de E_1 en des points de E_2.
3. Comparer sur de nombreux exemples de corps finis (si possible en grande caractéristique et en petite caractéristique) la vitesse de calcul d'additions et d'itérations de points sur E_1 et sur E_2.

4 Groupe des points d'une courbe elliptique

Exercice 4.1. L'objectif de cet exercice est d'avoir en stock des procédures permettant de calculer l'ordre d'un point sur une courbe elliptique E sur un corps $\mathbb{K}$.

1. Écrire une procédure déterminant l'ordre d'un point connaissant la factorisation d'un multiple de l'ordre.
2. En déduire une procédure déterminant l'ordre d'un point connaissant un multiple de l'ordre.
3. Appliquer les procédures précédentes à la courbe elliptique définie sur $\mathbb{F}_{173}$ par

$$y^2 = x^3 + 146x + 33$$

et aux points $P = (168, 133)$ et $Q = (147, 74)$.

Exercice 4.2.

1. Pour quels premiers p l'équation $y^2 + y = x^3 - x^2 - 10x - 20$ définit-elle une courbe elliptique sur $\mathbb{F}_p$? Si p est un tel premier, on notera E_p la courbe sur $\mathbb{F}_p$ ainsi obtenue.
2. Calculer $E_p(\mathbb{F}_p)$ pour tous les premiers inférieurs à 100. Ce groupe est-il toujours cyclique ?
3. Déterminer le groupe $E(\mathbb{Q})_{tors}$, et donner la liste explicite de ses éléments.
4. L'application de réduction modulo p
$$E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p)$$
est-elle injective ? Est-elle surjective ? Donner des exemples.

Plus généralement, soit E une courbe elliptique donnée par une équation de Weierstrass dont les coefficients a_i sont des entiers. Le théorème de Nagell-Lutz affirme que, si $P = (x, y)$ est un point de torsion défini sur $\mathbb{Q}$, alors x et y sont des entiers, sauf si P est un point de 2-torsion, auquel cas $P = (c/4, d/8)$ avec c et d entiers.

Par conséquent, en utilisant le même argument que précédemment, on trouve que l'application de réduction

$$E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p)$$

est injective pour tout premier p ne divisant pas 2Δ.

Conséquence : si P n'est pas à coordonnées entières ou de la forme $(c/4, d/8)$, alors P est d'ordre infini. Plus généralement, s'il existe un entier $n > 0$ tel que $[n]P$ n'est pas de cette forme, alors P est d'ordre infini.

Exemple : le point $P = (1, 1)$ sur la courbe $E = 1112a1$ est d'ordre infini.