

## TD n° 2 — Courbes elliptiques

---

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 distinctes peuvent définir la même courbe elliptique, et que le discriminant est rattaché à l'équation, et pas à la courbe elle-même.

### Exercice 1

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

$$y^2 + y = x^3 - x^2 - 10x - 20 \tag{1}$$

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  $F = \text{ellchangecurve}(E, [1/3, 0, 0, 0])$ . Comparer le discriminant et l'invariant  $j$  de  $F$  avec ceux de  $E$ .

### Exercice 2

1. Pour quels premiers  $p$  l'équation (1) 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  $E(\mathbb{Q})_{\text{tors}}$ , et donner la liste explicite de ses éléments.
4. L'application de réduction modulo  $p$

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

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

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

est injective pour tout premier  $p$  ne divisant pas  $2\Delta$ .

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.

### Exercice 3

1. Effectuer dans gp la commande  $E = \text{ellinit}("1112a1")$ . 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 `ellpow`.
4. En calculant  $[n]P$  pour des petites valeurs de  $P$ , montrer que  $P$  est d'ordre infini.

### Exercice 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 `ellpow`. 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  $P = (1/2, 1/2)$ . Expliquer pourquoi cela ne contredit pas le théorème de Nagell-Lutz.
5. Même question avec  $E : y^2 = x^3 - 43x + 166$  et  $P = (3, 8)$ .