

## Feuille de travaux pratiques N°3

### Autour du groupe de Mordell-Weil

Vous avez vu que le groupe de Mordell-Weil  $E(\mathbb{Q})$  des points rationnels d'une courbe elliptique  $E$  définie sur  $\mathbb{Q}$  est un groupe abélien de type fini (théorème de Mordell). On peut donc écrire

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors},$$

où l'entier  $r$  est par définition le rang de la courbe elliptique et où  $E(\mathbb{Q})_{tors}$  désigne le sous-groupe de torsion. Si le calcul du rang pose problème, la détermination de  $E(\mathbb{Q})_{tors}$  est aisée, à l'aide du :

**Théorème** (Nagell-Lutz). *Soit  $E$  une courbe elliptique définie sur  $\mathbb{Q}$  par une équation de Weierstrass courte  $y^2 = x^3 + ax + b$ , où  $a$  et  $b$  sont deux entiers relatifs, et soit  $P \neq O$  un point rationnel d'ordre fini. Alors  $P = (x, y)$  a des coordonnées entières vérifiant ou bien  $y = 0$  ou bien  $y^2 \mid \Delta = 4a^3 + 27b^2$ .*

Alternativement, le résultat suivant peut s'avérer pertinent dans certains cas :

**Proposition.** *Soit  $p$  un nombre premier ne divisant pas  $2\Delta$  et  $\bar{E}$  la réduction de  $E$  modulo  $p$ . Alors, via le morphisme de réduction,  $E(\mathbb{Q})_{tors}$  s'identifie à un sous-groupe de  $\bar{E}(\mathbb{F}_p)$ . En particulier,  $\#E(\mathbb{Q})_{tors}$  divise  $\#\bar{E}(\mathbb{F}_p)$ .*

Enfin, la structure de  $E(\mathbb{Q})_{tors}$  n'est pas arbitraire :

**Théorème** (Mazur). *La partie de torsion du groupe de Mordell-Weil d'une courbe elliptique définie sur  $\mathbb{Q}$  est isomorphe à l'un des groupes abstraits suivants :  $\mathbb{Z} \mid n\mathbb{Z}$  (pour  $1 \leq n \leq 10$ ),  $\mathbb{Z} \mid 12\mathbb{Z}$ , ou  $\mathbb{Z} \mid 2\mathbb{Z} \times \mathbb{Z} \mid 2n\mathbb{Z}$  (pour  $1 \leq n \leq 4$ ).*

### Procédures et algorithmes

Ouvrir le fichier OpA2005-TP3.mws ; on y trouve les procédures suivantes :

- `appart(E,P)` : vérifie l'appartenance du point  $P := [x, y]$  (ou  $P := \text{Origine}$ ) à la courbe elliptique  $E := [a, b]$  d'équation  $y^2 = x^3 + ax + b$ ;
- `somme(E,P,Q)` : renvoie  $P + Q$ ;
- `candidatsy(E)` : donne la liste  $[y_1, \dots, y_n]$  des entiers naturels  $y$  tels que  $y = 0$  ou  $y^2 \mid \Delta$ ;
- `trouverx(E,y)` : donne la liste  $[x_1, \dots, x_m]$  des entiers  $x$  tels que  $x^3 + ax + b = y^2$  (Maple utilise les formules de Cardan ; on teste si la racine est entière) ;
- `nbpointsmodp(E,p)` : renvoie  $\#\bar{E}(\mathbb{F}_p)$  ;
- `appartmodp(E,P,p)` : vérifie si  $P \in \bar{E}(\mathbb{F}_p)$  ;
- `sommemodp(E,P,Q,p)` : renvoie  $P + Q$ , calculé dans  $\bar{E}(\mathbb{F}_p)$  ;
- `ordremodp(E,P,p)` : renvoie l'ordre de  $P$  dans  $\bar{E}(\mathbb{F}_p)$  ;
- `pointsmodp(E,p)` : donne la liste  $[N, [\text{Origine}, 1], [[x_1, y_1], r_1], \dots, [[x_n, y_n], r_n]]$  des  $N$  éléments de  $\bar{E}(\mathbb{F}_p)$ , qui sont, outre  $O$  (d'ordre 1), les  $[x_i, y_i]$ , d'ordre  $r_i$ .

- 1** On désire déterminer l'ordre d'un point  $P \in E(\mathbb{Q})$  dont les coordonnées  $(x, y)$  sont entières : on calcule donc les multiples  $nP$  successivement. Si  $P$  est d'ordre infini, rappeler pourquoi on trouvera un point  $nP$  n'ayant plus ses coordonnées entières au bout de quelques itérations. Pourquoi est-il suffisant d'aller jusqu'à  $n = 12$ ? En déduire un algorithme de calcul de l'ordre. La procédure `ordre(E, P)` renverra FAIL si  $P \notin E(\mathbb{Q})$ , infinity si  $P$  est d'ordre infini, et l'entier égal à l'ordre de  $P$  sinon.

Tester votre procédure : sachant que la cubique de Fermat  $X^3 + Y^3 = Z^3$  est isomorphe à la courbe elliptique  $E : y^2 = x^3 - 432$ , le groupe de Mordell-Weil  $E(\mathbb{Q})$  est de cardinal égal à trois. Vérifier que  $P = (12, 36)$  est d'ordre 3.

- 2** Ecrire une procédure `NagellLutz(E)` renvoyant la liste formatée comme suit :  $[N, [[\text{Origine}, 1], [[x_1, y_1], r_1], \dots, [[x_n, y_n], r_n]]]$  des  $N$  éléments de  $E(\mathbb{Q})_{tors}$ , qui sont, outre  $O$  (d'ordre 1), les  $[x_i, y_i]$ , d'ordre  $r_i$ .

☞ Quelques commandes Maple utiles : `type`, `integer`.

### Applications

- 3** Pour chaque courbe elliptique  $E$  suivante, déterminer la structure de la partie de torsion du groupe de Mordell-Weil. On utilisera deux méthodes : d'une part, la réduction de  $E$  modulo différents  $p$  (procédures `...modp`), d'autre part Nagell-Lutz.

–  $E : y^2 = x^3 + 3$ ;

–  $E : y^2 = x^3 + x$ ;

–  $E : y^2 = x^3 - 43x + 166$  (peut-on conclure sans déterminer un point rationnel non-trivial?).

- 4** A la vue du théorème de Mazur, suffit-il de connaître  $\#E(\mathbb{Q})_{tors}$  pour connaître la structure de  $E(\mathbb{Q})_{tors}$ ? Donner un critère permettant de trancher les cas indécidables.

- 5** La procédure `transf(f)` du fichier OPA2005-TP3.mw transforme une équation de Weierstrass longue  $f := y^2 + ay + bxy = x^3 + cx^2 + dx + e$  en une équation de Weierstrass courte. Notant  $E$  et  $E'$  les courbes elliptiques correspondantes avant et après transformation, pourquoi les groupes de Mordell-Weil de  $E$  et  $E'$  sont-ils isomorphes? Calculer  $E(\mathbb{Q})_{tors}$  dans les cas suivants :

–  $E : y^2 + 7xy = x^3 + 16x$ ;

–  $E : y^2 + xy - 5y = x^3 - 5x^2$ .

On appliquera une dernière transformation du type  $x \rightsquigarrow x/d^2, y \rightsquigarrow y/d^3$  afin de se ramener à une équation à coefficients entiers (tout en restant toujours dans la même classe d'isomorphisme).

☞ Quelques commandes Maple utiles : `ifactor`, `subs`.

### Les nombres congruents

On rappelle qu'un entier naturel  $n$  non nul est «congruent» s'il s'écrit  $n = \frac{XY}{2}$  pour un triplet Pythagoricien rationnel  $(X, Y, Z)$  (i.e.  $X^2 + Y^2 = Z^2$ , où  $X, Y$  et  $Z$  sont trois nombres rationnels positifs non nuls). Par ailleurs, tout triplet Pythagoricien primitif (i.e.  $X, Y$  et  $Z$  sont de plus entiers et premiers entre eux dans leur ensemble) est de la forme  $(a^2 - b^2, 2ab, a^2 + b^2)$ , où  $a > b$  sont deux entiers premiers entre eux avec  $ab$  pair. Enfin, la proposition suivante établit le lien entre nombres congruents et courbes elliptiques :

**Proposition.** *Les assertions suivantes sont équivalentes :*

- (i)  $n = \frac{XY}{2}$ , pour un triplet Pythagoricien rationnel  $(X, Y, Z)$  ;
- (ii) la courbe elliptique  $E_n$  donnée par l'équation de Weierstrass  $y^2 = x^3 - n^2x$  possède un point rationnel distinct des solutions triviales  $(\pm n, 0)$ ,  $(0, 0)$  (qui correspondent aux points d'ordre 2) et du point à l'infini.

On démontre que  $E_n(\mathbb{Q})_{tors} = \{O, (0, 0), (\pm n, 0)\}$  ; autrement dit,  $n$  est congruent si et seulement si  $E_n$  possède un point rationnel d'ordre infini.

- 6** Montrer que tout nombre congruent  $n$  est de la forme  $n = s^2m$ , où  $s \in \mathbb{Q}^\times$  et  $m$  est un nombre congruent correspondant à un triplet Pythagoricien primitif.
- 7** Avec les notations des rappels précédents, faisant varier  $a$  et  $b$  entre 1 et 10, dresser une liste de nombres congruents.

*Remarque.* Cela ne permet en rien de déterminer si un nombre donné  $n$  est congruent : en effet, on ne sait pas à quel moment un  $m$  tel que  $n = s^2m$  va apparaître dans la liste.

- 8** Soit  $n$  un nombre congruent correspondant à un triplet Pythagoricien  $(X, Y, Z)$ . Vérifier par le calcul que  $(\frac{Z^2}{4}, \frac{(X^2 - Y^2)Z}{8})$  est un point rationnel de la courbe elliptique  $E_n$ . Pourquoi est-il d'ordre infini ?
- 9** Soit  $E$  la courbe elliptique d'équation  $y^2 = x^3 - 30^2x$ . Vérifier par Nagell-Lutz que  $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Exhiber un point rationnel qui ne soit pas de torsion.
- 10** Vérifier que  $(\frac{41^2}{7^2}, \frac{720 \cdot 41}{7^3})$  est un point de la courbe elliptique  $E_{31}$  et qu'il est d'ordre infini. En déduire que 31 est congruent.

☞ Quelques commandes Maple utiles : `igcd`, `even`, `sort`, `algsubs`, `normal`.