

## Examen

Session de mai 2004

Durée : 1 h 30  
Tous documents autorisés

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  $y^2 = x^3 + ax + b$ , où  $a$  et  $b$  sont deux entiers relatifs, et soit  $P \neq O$  un point rationnel. 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  $\tilde{E}$  la réduction de  $E$  modulo  $p$ . Alors, via le morphisme de réduction,  $E(\mathbb{Q})_{tors}$  s'identifie à un sous-groupe de  $\tilde{E}(\mathbb{F}_p)$ . En particulier,  $\#E(\mathbb{Q})_{tors}$  divise  $\#\tilde{E}(\mathbb{F}_p)$ .*

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

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

☞ *Il est conseillé de sauvegarder votre fichier Maple, incluant vos réponses, régulièrement. Il sera nommé exam-OPA-mon\_nom.mws et envoyé par courrier électronique en fin de séance à hausberg@math.univ-montp2.fr et à pev@math.univ-montp2.fr.*

### Préliminaires

- 1 Écrire une procédure `ordres(E)` renvoyant FAIL si la courbe  $E := [a, b]$  d'équation  $y^2 = x^3 + ax + b$  n'est pas une courbe elliptique et une liste  $[N, M]$ , où  $N = \#E(\mathbb{Q})_{tors}$  et  $M$  est le nombre d'éléments d'ordre 2, sinon.
- 2 Quelles sont les différentes valeurs possibles pour le couple  $(N, M)$ ? Indiquer la correspondance entre les couples  $(N, M)$  et la structure de  $E(\mathbb{Q})_{tors}$ .

☞ On pourra utiliser librement les procédures écrites en TP en les modifiant si nécessaire.

### Application

- 3 Tester la procédure `ordres` sur des exemples connus en comparant avec le résultat de NagellLutz.
- 4 Pour chaque courbe elliptique  $E_i$  ci-dessous, déterminer  $E_i(\mathbb{Q})_{tors}$  :
  - $E_1 : y^2 - y = x^3 - x^2$ ;
  - $E_2 : y^2 + xy + y = x^3 - x^2 - 14x + 29$ ;
  - $E_3 : y^2 + xy = x^3 - 45x + 81$ ;
  - $E_4 : y^2 + 43xy - 210y = x^3 - 210x^2$ ;
  - $E_5 : y^2 + 5xy - 6y = x^3 - 3x^2$ ;
  - $E_6 : y^2 + 17xy - 120y = x^3 - 60x^2$ .
- 5 En faisant varier  $a$  et  $b$  et en utilisant votre procédure `ordres`, montrer que tous les cas possibles prédits par le théorème de Mazur apparaissent. On donnera un couple  $(a, b)$  pour chaque structure possible.