MAT 2440 : Théorie des nombres

Courbes elliptiques (2)

Exercice 1 Chacun des points suivants est d'ordre fini sur la courbe elliptique donnée. Trouver son ordre.

1. $P = (0, 4)$ sur $y^2 = 4x^3 + 16$
2. $P = (2, 8)$ sur $y^2 = 4x^3 + 16x$
3. $P = (2, 3)$ sur $y^2 = x^3 + 1$
4. $P = (3, 8)$ sur $y^2 = x^3 - 43x + 166$
5. $P = (3, 12)$ sur $y^2 = x^3 - 14x^2 + 81x$

Exercice 2 Trouver l'ordre du groupe des $\mathbb{F}_p$-points sur la courbe $y^2 = x^3 - x$ pour chaque nombre premier p entre 3 et 23.

Exercice 3 Calculer le groupe des $\mathbb{F}_p$-points sur la courbe $y^2 = x^3 + x + 1$ pour $p = 3, 7, 11$ et 13.

Exercice 4 Montrer qu'il y a $p+1$ $\mathbb{F}_p$-points sur la courbe $y^2 = x^3 - x$ si $p \equiv 3 \bmod 4$.

Exercice 5 Soit $a \in \mathbb{Z}$ et p un nombre premier tel que $p \equiv 2 \bmod 3$.

1. Montrer que pour tout $b \in \mathbb{F}_p$, il existe un unique $x \in F_p$ tel que $x^3 = b$ (utiliser une racine primitive modulo p).
2. Montrer que la courbe elliptique d'équation $y^2 = x^3 - a$ sur $\mathbb{F}_p$ possède $p + 1$ points.