

TP2 TANC - Volcans d'isogénie

Exercice 1. On pose $K = \mathbb{Q}(\sqrt{-130})$ et $\mathcal{O}_K = \mathbb{Z}[\sqrt{-130}]$ son ordre maximal. On considère $k = \mathbb{F}_{2081}$.

1. Calculer $H_{\mathcal{O}_K} \in k[X]$, le polynôme de classes de Hilbert modulo 2081.
2. Montrer que $H_{\mathcal{O}_K}$ est scindé à racines simples dans k .
3. Que peut-on dire d'une courbe elliptique ayant pour j -invariant une racine de $H_{\mathcal{O}_K}$?
4. Représenter, à l'aide de Magma, sur une feuille tous les 2-volcans d'isogénies sur \mathbb{F}_{2081} pour les j -invariants de courbes elliptiques avec CM par un ordre de K .

Exercice 2. Soit $p = 883$ et $j = -1 \in \mathbb{F}_p$. On pose E une courbe elliptique sur \mathbb{F}_p de j -invariant j .

1. Justifier que son Frobenius engendre un ordre de conducteur 6 dans $\mathbb{Z}[\sqrt{-89}]$. Quels sont les conducteurs possibles pour $\text{End}(E)$?
2. Quelles sont les profondeurs possibles des ℓ -volcans pour les courbes elliptiques à multiplication complexe dans $\mathbb{Q}(\sqrt{-89})$? Discuter les cas $\ell = 2, 3$ et les autres.
3. Montrer que j se trouve sur le cratère du 3-volcan sur lequel il se trouve.
4. Montrer que j se trouve sur le sol du 2-volcan sur lequel il se trouve.
5. En déduire que $\text{End}(E)$ est de conducteur 2 dans $\mathbb{Z}[\sqrt{-89}]$.