TP1 TANC - Ordres quadratiques imaginaires

Exercice 1 (Ordre maximal)**.**

1. Définir le corps quadratique $K = \mathbb{Q}\left(\sqrt{-105}\right)$.
2. Définir son ordre maximal $\mathscr{O}_K = \mathbb{Z}[\omega]$. Quel est son discriminant ?
3. Définir les idéaux $\mathfrak{a} = \langle 15, 5\omega \rangle$ et $\mathfrak{b} = \langle 30, 35\omega \rangle$.
4. Montrer que $\mathfrak{a} = \mathfrak{b}$. L'idéal $\mathfrak{a}$ est-il principal ? Premier ? Inversible ? Si oui déterminer son inverse.
5. Montrer que $\mathfrak{a} = \mathfrak{p}_1 \cdot \mathfrak{p}_2^2$ est la factorisation en idéaux premiers de $\mathfrak{a}$ avec $\mathfrak{p}_1 = \langle 3, \omega \rangle$ et $\mathfrak{p}_2 = \langle 5, \omega \rangle$.
6. Définir le groupe des classes de $\mathrm{Cl}(\mathscr{O}_K)$.
7. Quel est son cardinal ?
8. Calculer $\mathfrak{c}^2$ pour tout $\mathfrak{c} \in \mathrm{Cl}(\mathscr{O}_K)$. En déduire que $\mathrm{Cl}(\mathscr{O}_K) \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
9. Définir l'idéal $\mathfrak{c} = \langle 1590, 1065 + 5\omega \rangle$ et montrer que $[\mathfrak{a}] = [\mathfrak{c}] \in \mathrm{Cl}(\mathscr{O}_K)$ où $[\mathfrak{a}]$ désigne la classe de $\mathfrak{a}$ dans le quotient.

Exercice 2 (Ordre non-maximal)**.**

1. Définir le corps quadratique $K = \mathbb{Q}\left(\sqrt{-1}\right)$.
2. Définir son ordre maximal $\mathscr{O}_K = \mathbb{Z}[\omega]$ ainsi que les sous-ordres $R = \mathbb{Z}[2\omega]$ et $S = \mathbb{Z}[s] = \mathbb{Z}[4\omega]$. On pose aussi $\mathfrak{a} = \langle 4, s - 2 \rangle$ et $\mathfrak{b} = \langle 2, s \rangle$ deux idéaux de S.
   (a) Quelle est la norme de $\mathfrak{a}$ et $\mathfrak{b}$? Sont-ils principaux ?
   (b) Montrer que $\mathfrak{a}$ est inversible tandis que $\mathfrak{b}$ ne l'est pas (on pourra utiliser le fait que $\mathfrak{c}$ inversible si et seulement si $\mathfrak{c}\bar{\mathfrak{c}}$ principal).
   (c) Que peut-on en déduire sur $h(S) = \#\,\mathrm{Cl}(S)$? Calculer $h(S)$ à l'aide de Magma.
   (d) Montrer que l'anneau multiplicateur de $\mathfrak{b}$ est R.
   (e) Calculer $h(R)$.
   (f) Peut-on affirmer que $\mathfrak{b}R$ est un idéal principal de R ?

Exercice 3. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$, on note π_E son discriminant. On rappelle que $\chi_E = X^2 - t_E X + q \in \mathbb{Z}[X]$ annule π_E avec t_E la trace de E.

1. Écrire un programme qui prend en argument une courbe elliptique E sur un corps fini et qui renvoie `false` si la courbe est supersingulière et `true` suivi du discriminant de $\mathbb{Z}[\pi_E]$ sinon.
2. Calculer le discriminant de l'ordre engendré par le Frobenius de toutes les courbes ordinaires sur $\mathbb{F}_3$.
3. Montrer que pour toute courbe elliptique ordinaire E définie sur $\mathbb{F}_3, \mathrm{End}_{\overline{k}}(E)$ est maximal (on pourra s'appuyer sur l'exercice 3 du TD1 pour obtenir un encadrement de $\mathrm{End}(E)$). Peut-on affirmer la même chose pour les courbes définies sur $\mathbb{F}_5$?