1 produit d'idéaux

Explication du code

March 8, 2024

(Cette partie est finalement pas utilisée telle quelle, la fonctionnalité étant implémentée en sage) Si $I = (a, b + id)$ et $J = (c, f + ig)$ on les représente via une forme normale de hermite:

$$I = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

$$J = \begin{pmatrix} c & f \\ 0 & g \end{pmatrix}$$

Pour calculer leur produit, on regarde l'idéal produit

$$IJ = (ac, af + iag, cb + icd, bf - dg + i(cd + bg))$$

Qu'on représente en:

$$IJ = \begin{pmatrix} ac & af & cb & bf - dg \\ 0 & ag & cd & cd + bg \end{pmatrix}$$

Dont on calcule la forme normale de hermite pour obtenir

$$IJ = (N(IJ), x + if)$$

(Tout est transposé dans le code car FLINT effectue la réduction hnf sur les lignes)

2 Calcul du groupe de classe

Les idéaux d'ordres, le calcul de produit et la composition de forme quadratiques n'étant pas implémentés en sage. Je l'ai fait en C à l'aide de FLINT.
On utilise l'algorithme de Pohlig-Hellman couplé à rho-pollard. L'implémentation est faite à l'aide du module qfb de FLINT qui permet de calculer dans le groupe de classe de formes quadratiques binaires de discriminant donné.