

# Explication du code

March 10, 2024

## 1 produit d'idéaux

(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 réseau de relations

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.

## 3 Paramètres

Les candidats sont calculés à l'aide de `gen_conductor_choices` dans `lib/ideals`. Chaque fichier `candidate_conductorsN` contient les candidats pour les  $N$  premiers nombres premiers décomposés dans  $\mathbb{Z}[i]$ . L'évaluation de chaque candidats est effectué par `eval_candidate` présent dans `lib/eval_candidate` à l'aide de ECM avec abandon et 30 processus en parallèle qui sont terminés au bout d'une seconde si ils n'ont pas finis.

### 3.1 Paramètre de 40 et 80 bits

Pour  $n_1 + n_2 = 11$  j'ai pris

$$\alpha = 3014688773870022715669219i + 73018318326246924528693954$$

avec  $f \approx 2^{81}$  et  $f - (\frac{-1}{f})$  qui est  $2^{30}$ -lisse. Pour  $n_1 + n_2 = 17$  j'ai pris

$$\begin{aligned} \alpha = & 606346906079138499752787264655000342496041920427i \\ & + 375198466882833042822684243162077125238505408858 \end{aligned}$$

avec  $f \approx 2^{161}$  et  $f - (\frac{-1}{f})$  qui est  $2^{36}$ -lisse.

La table des logs discrets est `txt/dlogs_N_bits.md`.

## 4 Commandes

Pour lancer le calcul du réseau de relation, depuis le dossier `Clib`:

- `make`
- `./bin/lattice_relations`  
`../txt/conductor_N_bits.md ../txt/sqrts_M_primes.md ../txt/dlogs_N_bits.md`

Pour  $N = 40$  mettre  $M = 11$  et pour  $N = 80$  mettre  $M = 17$ .