DM - TANC (31/01/2023) – Sujet n° 1

Ce DM comporte deux parties, une première partie que vous devez me rendre sous format papier et une seconde partie informatique que vous devrez déposer sur Moodle. Pour la première partie je vous autorise à me rendre une copie pour 2 ou 3 si vous travaillez à plusieurs. Dans le cas où vous me rendez une copie pour plusieurs jouez le jeu : arrangez vous pour que toute personne qui y dépose son nom comprenne bien tout ce qui s'y trouve. Il ne s'agit ni d'une occasion de donner une bonne note à son camarade ni de se diviser le travail.

Pour la seconde partie vous me déposerez chacun·e un fichier sur Moodle à votre nom (voir le verso pour davantage d'explications). Vos compositions sont à rendre pour le 14/02 cependant si vous parvenez à me rendre le DM papier pour le 08/02 j'essaierai de le corriger pour le 14/02 de manière à ce que vous puissiez avoir vos copies pour l'épreuve du 16/02 (pour laquelle tous les documents seront autorisés).

Composition sur papier

*Barème **indicatif** : 1 point par question sauf 3.e.(ii.) et 5. qui sont sur 2 soit 15 points pour la composition sur papier.*

Soit d un entier impair négatif sans facteur carré tel que $d = 3 \mod 4$ et $-d \geq 5$. On pose $K = \mathbb{Q}\left(\sqrt{d}\right)$.

1. Justifier que $\mathscr{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$. Quel est son discriminant ? On pose $\omega = \sqrt{d}$.
2. On pose $\mathfrak{p} = \langle 2, 1+\omega\rangle$.
   (a) Quelle est sa norme ?
   (b) L'idéal $\mathfrak{p}$ est-il principal ?
   (c) Calculer $\mathfrak{p}^2$. En déduire que 2 divise le cardinal de $\mathrm{Cl}(\mathscr{O}_K)$.
3. On note désormais $-d = p_1 \cdots p_n$ avec p_i des premiers impairs distincts et on suppose que $n \geq 2$. On pose aussi $\mathfrak{p}_i = \langle p_i, \omega\rangle$.
   (a) Montrer que les $\mathfrak{p}_i$ sont des idéaux premiers de norme p_i.
   (b) Montrer que pour tout $i \in \{1, \ldots, n\}$, $\mathfrak{p}_i^2 = \langle p_i\rangle$.
   (c) Soit S un sous-ensemble non vide de $\{1, \ldots, n\}$. Montrer que
   $$\prod_{i\in S} \mathfrak{p}_i = \left\langle \prod_{i\in S} p_i, \omega \right\rangle$$
   (on pourra considérer la norme de l'idéal de droite).
   (d) Montrer que
   $$\frac{\omega}{p_n}\mathfrak{p}_n = \prod_{i\in\{1,\ldots,n-1\}} \mathfrak{p}_i.$$
   Que peut-on en déduire sur $[\mathfrak{p}_n]$ par rapport au sous-groupe de $\mathrm{Cl}(\mathscr{O}_K)$ engendré par les $[\mathfrak{p}_i]$ pour $1 \leq i \leq n-1$?
   (e) i. Montrer que pour tout sous-ensemble **strict** $S \subsetneq \{1, \ldots, n\}$ non vide et pour tout $s_0 \in \{0, 1\}$ l'idéal $\mathfrak{p}^{s_0}\prod_{i\in S}\mathfrak{p}_i$ n'est pas principal.
   ii. Pour $\mathfrak{a}$ un idéal fractionnaire de $\mathscr{O}_K$ on note $[\mathfrak{a}]$ sa classe dans $\mathrm{Cl}(\mathscr{O}_K)$. Déduire de la question précédente que l'application
   $$\begin{aligned} \iota : \quad (\mathbb{Z}/2\mathbb{Z})^n &\longrightarrow \mathrm{Cl}(\mathscr{O}_K) \\ (s_0, s_1, \ldots, s_{n-1}) &\longmapsto [\mathfrak{p}^{s_0}\cdot\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_{n-1}^{s_{n-1}}]. \end{aligned}$$
   est bien définie et qu'il s'agit d'un morphisme de groupes injectif (on pourra partir d'un morphisme de groupes $\mathbb{Z}^n \longrightarrow \mathrm{Cl}(\mathscr{O}_K)$ bien choisi et utiliser des propriétés universelles).
4. Montrer que $\mathrm{Cl}\left(\mathbb{Z}\left[\sqrt{-33}\right]\right)$ contient un sous-groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.
5. **(Question hors barème)** Montrer que $\mathrm{Cl}\left(\mathbb{Z}\left[\sqrt{-33}\right]\right)$ est engendré par $\mathfrak{p} = \left\langle 2, 1+\sqrt{-33}\right\rangle$ et $\mathfrak{p}_1 = \left\langle 3, \sqrt{-33}\right\rangle$ (on pourra utiliser le théorème du cours qui affirme qu'un idéal fractionnaire dans un ordre quadratique R de discriminant Δ a toujours un représentant dans R de norme inférieure à $\sqrt{\frac{-\Delta}{3}}$).
6. En considérant $d = -3\cdot11\cdot13$ justifier à l'aide de `Magma` que le morphisme ι n'est pas systématiquement un isomorphisme (c'est la seule question où une réponse `Magma` est acceptée).

Sur Magma

Énoncé

*Barème **indicatif** : 3 points pour la courbe `E` et 4 points pour l'algorithme de Schoof.*

1. Déterminer une courbe elliptique définie sur $\mathbb{F}_p$ avec $p = 1237940039285380274899124357$ et ayant $N = 1237940039285450643643302022$ points rationnels.
2. Implémenter une fonction `Schoof` qui prend en argument une courbe elliptique E définie sur un corps fini et renvoie son nombre de points rationnels. Vous implémenterez la version efficace de l'algorithme de Schoof (sans calcul explicite de points de torsion de la courbe).

Consignes importantes :

Vous rendrez la partie du DM de la section MAGMA sous forme d'un fichier à déposer sur Moodle appelé `nom_prenom.m`. Votre fichier devra impérativement comporter :

1. Une variable appelée `sujet` valant le numéro de votre sujet (voir le titre).
2. Une courbe elliptique appelée `E` définie sur $\mathbb{F}_p$ et ayant N points rationnels.
3. Une fonction nommée `Schoof` ayant **pour seule entrée** une courbe elliptique définie sur un corps fini et renvoyant son nombre de points rationnels.

Je vous recommande d'accorder une grande importance au nom des variables et des fonctions car la correction de vos fichiers sera semi-automatisée ; je chargerai vos fonctions et je les testerai avec mes fonctions pour voir si vos résultats sont corrects.

Par exemple, pour savoir si votre courbe elliptique `E` est correcte je ferai quelque chose comme :
`#E eq NList[sujet];`
où `NList` est la liste des valeurs de N rangée par sujet. Si vous n'avez pas renseigné le numéro du sujet ou que vous avez appelé votre courbe `Dominique` au lieu de `E` j'aurai une erreur et je ne perdrai pas beaucoup d'énergie à chercher d'où elle vient.

Vous pouvez bien entendu faire apparaître d'autres variables et fonctions sur votre fichier et les nommer comme bon vous semble. Par exemple :

```
p := 5;
k := GF(5);
E := EllipticCurve([k!1,1]);
```

est tout à fait acceptable (je veux juste que `E` soit bien nommée).

Aux petit·es malin·es qui se posent la question, j'ouvrirai tout de même vos fichiers et j'y jetterai un oeil. Inutile donc de terminer votre fonction `Schoof` par `return #E;` je verrai l'arnaque et je sanctionnerai votre audace comme il se doit.

Remarquez aussi que vos sujets ont tous un p et un N différent (c'est la seule différence entre tous les sujets), vous pouvez donc copier-coller la courbe trouvée par un·e camarade je n'y verrai que du feu mais vous aurez 0 à cette question. Vous êtes cependant encouragé·es à collaborer en expliquant la méthode CM à vos camarades qui ne l'auraient pas comprise (encore une fois sans faire le boulot à leur place). Vous pouvez aussi bien sûr me contacter pour discuter de points que vous n'auriez pas bien compris. Je ne vous donnerai pas les solutions mais je vous donnerai des indices.

J'attire votre attention sur le fait que parcourir toutes les courbes elliptiques correspondant au corps $\mathbb{F}_p$ qui vous est donné et compter leur nombre de points devrait prendre environ 10 milliards de milliards d'années à Magma. Il est donc plutôt recommandé d'appliquer la méthode CM qui, elle, prend $0,01$ seconde pour les sujets les moins chanceux.

Pour faire mon cours sur l'algorithme de Schoof je me suis reposé sur les (excellentes) notes de cours suivantes :`https://math.mit.edu/classes/18.783/2022/LectureNotes8.pdf`
L'auteur fournit aussi un lien vers une implémentation `Sage` de l'algorithme. Vous pouvez vous en inspirer pour votre algorithme Magma.