TD1 : Crible par Corps de Nombres, quelques exercices simples

4I905: Représentation des Nombres et Algorithmes : application à la cryptographie.

Exercice 1. Algèbre linéaire VS Algèbre linéaire creuse

Question 1 : Les algorithmes de résolution de systèmes linéaires creux fonctionnent en multipliant successivement (au plus) n matrices creuses de taille $n \times n$ avec un vecteur qui diffère pour chacune des matrices. Que signifie mathématiquement le fait que les matrices soient creuses ? Combien de multiplications (de scalaires) vont être nécessaire pour calculer la multiplication d'une de ces matrices creuses par un vecteur ? Quelle est la complexité finale de ces algorithmes ?

Question 2 : Rappelez le nom de la méthode la plus simple (id est, que l'on vous a enseignée en L1) pour résoudre un système d'algèbre linéaire général de taille $n \times n$ et sa complexité. Comparez avec la question précédente.

Exercice 2. Petite, moyenne et grande caractéristique

Question 1 : Rappelez les définitions de petite, moyenne et grande caractéristique. Vérifiez que tous les cas possibles sont bien couverts.

Question 2 : Que peut-on dire du corps à 3^{5*497} éléments ? D'un corps à p éléments, avec p un nombre premier ? Du corps à 103^3 éléments ? Du corps à 1009^3 éléments ? Donnez un p premier pour lequel $\mathbb{F}_{p^3}$ est de grande caractéristique.

Question 3 : Il faut garder à l'esprit que les qualificatif de taille pour les caractéristiques sont toujours données *relativement* à la taille du corps fini considéré. En considérant qu'il en va de même pour le degré d'extension, proposez des définitions de petite, moyenne et grande extension qui soient compatibles avec celles de la question 1.

Exercice 3. Complexité asymptotique et attaque pratique

Question 1 : En moyenne caractéristique, l'algorithme le plus performant asymptotiquement est le Crible par Corps de Nombres Multiple qui s'appuie sur la sélection polynomiale par conjugaison (2015). Il atteint une complexité de :

$$L_Q\left(\frac{1}{3}, \left(\frac{8 \cdot (9 + 4\sqrt{6})}{15}\right)^{1/3}\right).$$

En grande caractéristique, la meilleure complexité est atteinte par une variante similaire du Crible par Corps de Nombres Multiple (2014). Il s'agit de[1] :

$$L_Q\left(\frac{1}{3}, \left(\frac{2 \cdot (46 + 13\sqrt{13})}{27}\right)^{1/3}\right).$$

[1] Pour l'anecdote culturelle, il s'agit aussi exactement de la complexité du meilleur algorithme de factorisation à ce jour connu.

En petite caractéristique, les meilleurs algorithmes sont passés d'une complexité en $L_Q(1/3, (32/9)^{1/3})$ (Crible par Corps de Fonctions, 2006) à $L_Q(1/4)$ (Algorithme par Représentation Frobéniale, début 2014) à $L_Q(l)$ où la caractéristique est donnée par $L_Q(l)$ (Variante quasi-polynomiale du même algorithme, été 2014) .

Tracez les graphes de $L_Q(\alpha, c)$ pour plusieurs α et c judicieusement choisis.

Question 2 : En moyenne et en grande caractéristiques, quel est le maximum que peut prendre Q pour garantir que $L_Q(\alpha, c) < 2^{80}$? Quelle réalité pratique cette inégalité traduit-elle ?