TD2 : Le groupe $(\mathbb{Z}/N\mathbb{Z})^*$

À retenir
- Complexité pratique des opérations élémentaires dans $\mathbb{Z}$ et $K[x]$,
- Définition du pgcd, du ppcm, théorème de Bezout,
- Connaître parfaitement et *sans note* l'algorithme d'Euclide étendu, pour les entiers et les polynômes,
- Savoir analyser un algorithme élémentaire, par exemple un algorithme de tri, ou un algorithme simple pour les graphes,
- Algorithmique élémentaire de $(\mathbb{Z}/N\mathbb{Z})$,
- Exponentiation rapide,
- Cardinal du groupe des inversibles de $(\mathbb{Z}/N\mathbb{Z})$,
- N est premier si et seulement si $\#(\mathbb{Z}/N\mathbb{Z}) = N - 1$,
- Critère de Fermat, nombres de Charmichael,
- Groupe engendré par un élément, ordre d'un élément, groupe cyclique,
- Si N est premier alors $(\mathbb{Z}/N\mathbb{Z})^*$ est cyclique,
- Algorithme *pas de bébé, pas de géant* de Shanks,
- Théorème de Lagrange,

1 L'anneau $\mathbb{Z}/N\mathbb{Z}$

Calculer $2^{12345678987654321} \bmod 101$.

⋆⋆⋆

Vérifiez que 561 est un nombre de Carmichael. Pouvez vous expliquer ce phénomène ?

⋆⋆⋆

Donnez la liste des inversibles de $\mathbb{Z}/35\mathbb{Z}$. Le groupe $(\mathbb{Z}/35\mathbb{Z})^*$ est il cyclique ?

⋆⋆⋆

Calculer à la main l'inverse de 7 modulo 12 en utilisant l'algorithme d'Euclide étendu.

⋆⋆⋆

Donnez un générateur g de $(\mathbb{Z}/11\mathbb{Z})^*$. Écrivez la table de l'exponentielle en base g. Écrivez la table du logarithme en base g.

2 Groupes

Soit G est un groupe et $H \subset G$ un sous-groupe. On définit une relation $\mathcal{R}$ sur G par $x\mathcal{R}y$ si et seulement si $x^{-1}y \in H$.

Montrer que c'est une relation d'équivalence.

Montrer que toutes les classes d'équivalence ont le même cardinal, soit $\#H$.

En déduire une preuve du théorème de Lagrange.

⋆⋆⋆

Soit G est un groupe abélien. Soit $g \in G$ un élément d'ordre M. Soit $h \in G$ un élément d'ordre N. On suppose que M et N sont premiers entre eux. Que peut-on dire de l'ordre de gh ?