Université de Paris 7 | **TP12 Corps finis** | **agreg 2010 (F.Han[1])**

Exercice I:

1) Trouver dans la documentation de xcas une instruction permettant de créer un corps fini, et de travailler dedans. Par exemple, créer un corps $\mathbb{F}_3[a]$ isomorphe à $\mathbb{F}_{3^6}$. Calculer $(1+a)^{17}$,

2) Factoriser $x^3 - x + 1$ dans $\mathbb{F}_3$ et F_{3^6}, et $x^3 - x + a$ dans F_{3^6}.

3) Trouver en utilisant `Factor` un polynôme irréductible de degré 5. Arrivez vous à créer $\mathbb{F}_{3^{20}}$

Exercice II: polynômes irréductibles

1) Factoriser $X^8 + 1$ sur $\mathbb{Z}$ et sur $\mathbb{F}_3$

2) a) On considère l'ensemble `l:={1,2,3,4,3,4};` Remarquer que la différence avec `l:=[1,2,3,4,3,4];` et obtenir le complémentaire de $\{1,3\}$ dans l ainsi que celui de l dans l.

b) Soit n un entier premier avec 3. Faire une procédure qui affiche les orbites de $< 3, . >$ agissant sur $\mathbb{Z}/n\mathbb{Z}$ par multiplication.

c) Pour plusieurs valeurs de n, comparer ces orbites avec la factorisation de $X^n - 1$ dans $\mathbb{F}_3[X]$

d) Pour n allant de 1 à 8, quel est l'ordre de 3 dans $(\mathbb{Z}/2^n\mathbb{Z})^\times$? Ce groupe est il cyclique ? Commentez avec le cas général.

e) Quel est l'ordre maximal d'un élément de $(\mathbb{Z}/2^n\mathbb{Z})^\times$? (NB : ce groupe se surjecte sur $(\mathbb{Z}/4\mathbb{Z})^\times$)

f) Pour ces n, factoriser sur $\mathbb{Z}$ $X^{2^n} - 1$. Quels sont les polynômes cyclotomiques Φ_{2^n} ? Sont ils irréductibles sur $\mathbb{F}_3[X]$?

3) Trouver un i pour que $3^i - 1$ soit divisible par 2^8 mais pas par 2^9. On notera q cette valeur de 3^i.

4) Trouver un polynôme P irréductible de degré i dans $\mathbb{F}_3[X]$, où i est la valeur choisie dans la question précédente.

Exercice III: Racine carrée dans $\mathbb{F}_q$

1) a) Faire une fonction `puiss` qui calcule la puissance n-ième d'un élément g de $\mathbb{F}_q$ où $q = 3^i$, où i est l'entier fixé que vous avez choisi dans l'exercice précédent, et où n peut être grand. (On n'utilisera pas `GF`). On fera cette fonction 2 fois. Une où l'on programme les puissances rapides, l'autre ou l'on utilise `powmod`.

b) Faire une procédure `testcarre` qui teste si g est un carré dans $\mathbb{F}_q$.

c) Trouver un élément g d'ordre 2^8 dans $(\mathbb{F}_q)^\times$.

d) Faire une fonction `inve` pour caluler un inverse dans $\mathbb{F}_q$.

e) Prendre un élément z de $\mathbb{F}_q$ qui soit un carré.

f) Trouver z_1 et z_2 tels que $z = z_1.z_2$ et z_1 soit d'ordre un diviseur de 2^8 et z_2 d'ordre impair. Vérifier votre résultat.

g) Calculer la racine carrée de z_2 puis de z_1, et obtenir une racine carrée de z.

Exercice IV: Ordre d'un élément

1) Comment récupérer la liste des facteurs premiers d'un entier ?

2) Faire une procédure `ord(x,n)` calculant l'ordre d'un élément x de $(\mathbb{Z}/n\mathbb{Z})^\times$. On partira d'un élément m tel que $x^m = 1[n]$. On s'arrangera pour qu'un élément de petit ordre soit trouvé rapidement. Par exemple l'ordre de -1 dans $(\mathbb{Z}/2^{1000}\mathbb{Z})^\times$. (On utilisera une fonction de puissance rapide modulaire deja programmée).

[1] http ://www.math.jussieu.fr/∼han/agreg