Université de Paris 7 | **TP19** | **agreg 2017 (F.Han [1])**

Exercice I: Utiliser des commandes pari sous xcas

Les fonctions d'arithmétiques spécialisées ne sont pas forcément directement accessibles depuis xcas, mais elles sont souvent déjà implémentées dans le logiciel pari. Elles sont donc accessibles depuis xcas ainsi :

— On peut les activer en tapant : `pari()`
— On cherche dans le menu `Aide>Manuel>PARI-GP` le nom de la fonction qui nous intéresse. Par exemple dans l'onglet 'Arithmetic functions' on remarque la fonction pari : `znstar`.
— Pour utiliser `znstar` sous xcas on fait : `pari_znstar`

Exercice II: Codes de Golay ; résidus quadratiques. Colle 1

COLLE1 : PRÉSENTEZ/ILLUSTREZ LE CODE DE GOLAY EN VOUS AIDANT DES QUESTIONS SUIVANTES.

1) Nous allons étudier le code de Golay G_{23}, qui est un code cyclique en caractéristique 2, de longueur 23. Il est de plus 3 correcteur parfait.

a) En factorisant $x^{23}-1$ dans $\mathbb{Z}/2\mathbb{Z}[x]$ on trouve deux facteurs irréductibles de degré 11. On en choisit un, noté g.

b) Comment peut on obtenir la liste des facteurs d'un polynôme dans $\mathbb{Z}/2\mathbb{Z}[x]$?

c) Pourquoi les racines de g sont elles d'ordre 23 ? Combien y a t'il de carrés dans $(\mathbb{Z}/23\mathbb{Z})^\times$? Lesquels ? En déduire que $x^{23}-1$ avait forcément des diviseurs de degré 11 dans $\mathbb{Z}/2\mathbb{Z}[x]$. Exprimer les racines de g en fonction d'une. (On prouvera ces résultats de manière théorique, en utilisant le frobenius, et on illustrera ces résultats en prenant une racine de g dans $\mathbb{F}_{2^{11}}$.

2) On considère le code de Golay G_{23} défini par l'idéal (g) de $\mathbb{F}_2[x]/(x^{23}-1)$ vu comme un $\mathbb{F}_2$ espace vectoriel. (Dans la suite, toutes les coordonnées seront prises dans la base $1, x, \ldots, x^{22}$) Quel est le nombre d'éléments de G_{23} ?

a) Déduire de la liste des carrés et du critère de minoration de la distance d'un code cyclique (Cf cours) que G_{23} est de distance au moins 5

b) Donner une matrice génératrice [2] de G_{23}.

3) a) Donner une matrice génératrice GE du code étendu $\widetilde{G_{23}}$ [3] de G_{23}

b) Trouver une matrice vérificatrice VE de $\widetilde{G_{23}}$. On notera $\widetilde{G_{23}}^\perp$ le code engendré par VE. (Appelé code dual de $\widetilde{G_{23}}$).

c) Montrer que $\widetilde{G_{23}} = \widetilde{G_{23}}^\perp$.

d) En déduire que si m et m' sont des mots de $\widetilde{G_{23}}$ de poids [4] nul modulo 4 alors $m+m'$ aussi. [5]

e) Montrer que $\widetilde{G_{23}}$ est de distance 8 et que G_{23} est de distance 7.

Exercice III: polynômes irréductibles. (compléments/révisions racines et orbites)

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

2) Soit n un entier premier avec 3. Expliquez le lien entre les orbites de $<3,.>$ agissant sur $\mathbb{Z}/n\mathbb{Z}$ par multiplication et les facteurs de X^n-1 dans $\mathbb{F}_3[X]$.

a) 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 ?

b) 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) Dans cette question nous cherchons à construire un corps intéressant pour pouvoir illustrer l'algorithme d'extraction de racine carrée.

a) 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.

1. http ://www.math.jussieu.fr/∼han/agreg
2. ie une base de l'espace vectoriel G_{23}
3. On ajoute un bit de parité
4. c'est le nombre de coordonnées non nulles
5. On remarquera que le produit scalaire $2(m.m')$ est dans $4\mathbb{Z}$

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

Exercice IV: Ecrit 2007, Colle 2

1) Choisir un nombre premier p à 13 chiffres, tel que[6] le problème du log discret soit difficile modulo p.

2) Choisir un entier b et un secret e et rendre publique $(b, b^e[p])$. Commentez votre choix de b.

3) Remarquer que les lettres $A \dots Z$ ont des codes ASCII consécutifs. Comment obtenir les codes de chaque lettre d'un mot ? (et si l'on veut que A soit représenté par 0 et Z par 25 ?)

4) Votre voisin choisit un message, tire des k au hasard et code chaque lettre x avec $(b^k[p], x.(b^e)^k)[p])$ (sans connaitre e, seulement avec b et b^e

5) a) Décoder le message grâce à e.

b) Préparer un exposé de 20 minutes expliquant la méthode et son intérêt. (temps pour crypter, décryper avec et sans e, puissances rapides. Statitiques sur les lettres du message crypté...)

Exercice V: Ordre d'un élément, Colle 3

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

2) Dans cette question on suppose que l'ordinateur est capable de factoriser m et de calculer $\Phi(n)$. 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).

3) Les fonctions d'arithmétiques spécialisées ne sont pas forcément directement accessibles depuis xcas, mais elles sont souvent déjà implémentées dans le logiciel pari. Elles sont donc accessibles depuis xcas ainsi :

- On peut les activer en tapant : `pari()`
- On cherche dans le menu `Aide>Manuel>PARI-GP` le nom de la fonction qui nous intéresse. Par exemple dans l'onglet 'Arithmetic functions' on remarque la fonction pari : `znstar`.
- Pour utiliser `znstar` sous xcas on fait : `pari_znstar`

Quelle est la structure du groupe $(\mathbb{Z}/16\mathbb{Z})^\times$? Trouvez une fonction pari qui donne l'ordre d'un élément dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et verifiez la votre.

Exercice VI: Localisation des zéros. Th Rolle, Suites de Sturm. Colle 4

Définition : *Soit $R \in \mathbb{R}(x)$. On dit que R a un saut de $-\infty$ à $+\infty$ en un réel t si $\lim_{x\to t, x<t} R(x) = -\infty$ et $\lim_{x\to t, x>t} R(x) = +\infty$. On appelle indice de Cauchy $I_{a,b}(R)$ le nombre de sauts dans $]a,b[$ de $-\infty$ à $+\infty$ moins le nombre de sauts dans $]a,b[$ de $+\infty$ à $-\infty$.*

Exemple : Si R n'a que des pôles simples, $I_{a,b}(R)$ est la somme des signes des résidus des pôles de R qui sont dans $]a,b[$.

On considère une famille $P_1 \dots P_n$ d'éléments de $\mathbb{R}[x]$ et deux réels a, b avec $a < b$. On dit que $(P_1, \dots, P_n)$ est de Sturm sur $[a,b]$ si :

- $\forall k \in \{2, \dots, n-1\}, \forall x \in]a,b[, P_k(x) = 0 \Rightarrow P_{k-1}(x)P_{k+1}(x) < 0$
- $\forall x \in]a,b[, P_n(x) \neq 0$

On dira que c'est une suite de sturm généralisée s'il existe un élément d de $\mathbb{R}[x]$ divisant tous les P_i pour i appartenant à $\{1, \dots, n\}$ tel que (P_i/d) soit de Sturm.

Proposition : *Si $(P_i)_{1\le i\le n}$ est une suite de Sturm généralisée sur $[a,b]$ telle que $P_1(a).P_1(b) \neq 0$, alors $I_{a,b}(R) = V(a) - V(b)$ où $V(x)$ est le nombre de variation de signes dans la suite des termes non nuls de $P_1(x), \dots, P_n(x)$*

Application : On souhaite trouver le nombre de zéros d'un polynôme P dans l'intervalle $[a,b]$. On pose $P_1 = P$ et $P_2 = P'$. Puis on note pour $i > 2$ P_i l'opposé du reste de la division de P_{i-2} par P_{i-1}. Alors P_i est de Sturm généralisé sur $[a,b]$ et l'indice de Cauchy de P_1/P_2 est le nombre de zéros de P dans $[a,b]$.

6. ou que vous supposez tel que

1) Etudier les fonctions `sign` (quelle est la valeur retournée, ou -1,0,2) et `horner`. Comment evaluer un polynôme du type : `P:=2*x^3+4*x-5` en $\sqrt{3}$?

2) Ecrire un programme qui calcule les P_i.

3) En déduire un programme qui calcule le nombre de zéros de P dans $[a, b]$. (On n'utilisera pas la commande sturm de votre logiciel.)

4) Etudier la commande xcas correspondante ainsi que sa documentation. Quelle différence constatez vous ?

Exercice VII: Coût [7] des opérations élementaires

Préparez un exposé sur les résultats suivants :

- Modèle à coût fixe : Ex les flottants, les opérations dans $\mathbb{Z}/N\mathbb{Z}$.
- Modèle à coût bilinéaire :

Opérations dans $\mathbb{Z}$:

$M \pm N$	$O(\sup(\log N, \log M))$
$M.N, M \leq N$	Méthode classique : $O(\log N.\log(M))$; T.F discrète : $O(\log N.\log^3(\log N))$
$M/N, M \leq N$	$O(\log M.\log(N/M))$
$N = a^n$	$O(\log n)$ multiplications, donc le coût est en : $O(n^2) = O((\log N)^2)$
$u \wedge v$, Bezout, $u, v \leq N$	$O((\log N)^2)$. Cas le pire et suite de Fibonacci

(NB : pour TF discrete, on peut ameliorer le $O(\log N.\log^3(\log N))$. Cf Knuth vol2 page 311)

Opérations dans $\mathbb{Z}/N\mathbb{Z}$

$\pm$	$O(\log N)$
. ou /	$O((\log N)^2)$
a^n	$O((\log n.(\log N)^2)$

- Pivot de Gauss sur une matrice de taille n : $O(n^3)$ multiplications et additions de coefficients.
- Symbole de Jacobi : même ordre de grandeur que le pgcd.

7. Il faut connaitre ces résultats et savoir les démontrer sauf éventuellement le cout de la multiplication rapide.