Exercice I: Codes de Golay ; résidus quadratiques

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.

CF colles non faites TP12

Exercice II: Ecrit 2007

(Préparation 40min)

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 $A \ldots Z$ 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. Statitiques sur les lettres du message crypté...)

[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 $4\mathbb{Z}$

[6] ou que vous supposez tel que