Elements mathématiques pour le codage

seconde séance : appli

1. Etude des corps $F_p[X]/P(X)$- suite

Théorème 1. *Soit un corps premier F_p et un polynôme P(X) à coefficients dans F_p, **irréductible** et de degré d;*

On désigne par $K = F_p[X]/P(X)$ l'ensemble des classes de congruence de $F_p[X]$ modulo P(X).

1) Si on munit K=$F_p[X]/P(X)$ de l'addition modulo P(X) et de la multiplication modulo P(X) il devient un corps.

2) Par ailleurs $K = F_p[X]/P(X)$ est un F_p espace vectoriel de base $\left(\bar{1}, \bar{X}, \overline{X^2}, ..., \overline{X^{d-1}}\right)$; par suite il possède p^d éléments.

3) Il contient F_p=$\{\bar{0}, \bar{1}, ..., \overline{p-1}\}$.

On peut démontrer qu'il n'y a qu'un seul type de corps possédant p^d éléments, on le notera F_{p^d}

4) L'ensemble K^*=$K \backslash \{0\}$, formé par les éléments non nuls de K est un groupe multiplicatif cyclique.

Exemple 2. On reprend le corps $F_3[X]/(X^2+1)$

On désigne par μ la classe de X+1

1. Montrons que les éléments non nuls sont tous de puissances de ω:

puissance de μ	classe de
μ^0	1
μ^1	$X+1$
μ^2	$-X$
μ^3	$-X+1$
μ^4	-1
μ^5	$-X-1$
μ^6	X
μ^7	$X-1$
μ^8	1

2. Ce tableau permet désormais de gagner du temps pour les multiplications:

$\mu^m \odot \mu^n = \mu^{m+n \text{ modulo } (8)}$

3. Ce tableau permet désormais de gagner du temps pour le calcul de l'inverse:

comme $\mu^8 = 1$ l'inverse de μ^k s'écrit tout simplement μ^{8-k}.

Au placard Euclide amélioré !!!!

4. Reste l'addition elle se fait en additionnant les coefficients modulo 3:

cl(X+1)$\oplus$cl$(X+1) = cl(-X-1)$....

Exercice 1. $F_3[X]$

1. Vérifier que le polynôme $X^3 - X^2 + X + 1$ est irréductible dans $F_3[X]$

2. Déterminer le nombre d'éléments du corps $F_3[X]/(X^3 - X^2 + X + 1)$

3. Vérifier avec maxima que la classe μ de X est bien un générateur du groupe $(F_3[X]/(X^3 - X^2 + X + 1)\setminus\{0\}, \odot)$

On pourra s'aider de la procédure ci-jointe

test(P):=block([Q,k,L],Q:P,k:1,L:[P],while(k<27)do(Q:second(divide(Q*P,X^3-X^2+X+1)),L:endcons(Q,L),k:k+1),return(L))dollar

Remarque 3. Le package de maxima pour les corps finis

avant tout charger le package : load(gf);

puis définir le corps fini

exemple: la commande « gf_set_data(5,x^3+x+1) » va définir que l'on travaille modulo 5 (c'est à dire avec F_5[X] et que le polynôme P(X)=X^3+X+1.

Si P(X) est irréductible dans F_5[X] on va travailler dans F_5[X]/P(X).

exemple: a:X^2+1; b:X+1; gf_mult(a,b); donnera -x-1;

de même gf_add(a,b); donnera 2X^2+X+1;

et gf_inv(a); donnera l'inverse

la division euclidienne sera donnée par gf_div(a,b):

on peut créer des matrices comme d'habitude

m:matrix([x+1,x^2+x,x],[x^2+1,x^2+x,1]);

les multiplier par gf_matmult(m,n).

inverser par gf_matinv(m) ou ......(cf la version)

2. Les Corps F_{2^d}

Tout devient plus facile en remplaçant 3 par 2 : F_2

1. D'une part les additions dans F_2 et $F_2[X]$ sont faciles (1+1=0,1+0=1,0+0=0) c'est l'addition booléenne

2. Donc dans $F_2[X]/P(X)$ la loi $\oplus$ sera simple, plus encore que modulo 3

3. D'autre part le groupe des éléments non nuls, au lieu d'être engendré par un élément pas simple, et pas simple à trouver, sera tout simplement engendré par la classe de X.

Proposition 4. *Liste de polynômes irréductibles dans* $F_2[X]$ *(il y en a d'autres à chaque degré)*

degré 2: X^2*+X+1*

degré 3: X^3*+X+1*

degré 4: X^4*+X+1*

degré 5: X^5+X^2+1

degré 6: X^6+X+1

degré 7: X^7+X^3+1

degré 8: $X^8+X^4+X^3+X^2+1$

Théorème 5. *Soit un polynôme P(X) irréductible, de degré d, dans* $F_2[X]$ *et le corps* $F_2[X]/P(X)$

1) Si on désigne par ω *la classe de X,* $K=\{a_0+a_1\omega+a_2\omega^2+....+a_{d-1}\omega^{d-1},(a_0,a_1,....,a_{d-1})\in\{0,1\}^d\}$

2) P(X) est le polynôme unitaire de plus bas degré qui admette ω *comme racine.*

3) K possède 2^d *éléments*

4) K, muni de l'addition modulo P(X) et de la multiplication modulo P(X) est un corps

5) K est désigné par F_{2^d}

6) ω *engendre le groupe multiplicatif* $K^*=K\backslash\{0\}$*, c'est à dire* $K=\{0,\omega,\omega^2,....,\omega^{d-1}=1\}$

Remarque 6. Contrairement au cas de F_3 la classe de X est un générateur du groupe des éléments non nuls, ce qui allège les calculs.

3. Exemple F_8

On prend par exemple le polynôme irréductible X^3+X+1 et on considère $F_2[X]/(X^3+X+1)$

On note ω la classe de X

ses éléments s'écrivent a+b$\omega+c\omega^2$ (où a,b,c valent 0 ou 1)

1) l'addition est banale

2) exemple de multiplication $(1+\omega+\omega^2)\odot(1+\omega^2)=\omega+\omega^2$

rappel : deux méthodes de calcul: soit on multiplie et on garde le reste modulo P(X), soit on remplace chaque fois X^3 par -(1+X), c'est à dire ici (modulo 2).

3) table des puissances de ω:

$\omega,\omega^2,\omega^3=1+\omega,\omega^4=\omega^2+\omega,\omega^5=1+\omega+\omega^2,\omega^6=1+\omega^2,\omega^7=1$

4) par exemple : l'inverse de $1+\omega+\omega^2=\omega^5$ est ω^2

Problème 1. Dans $F_2[X]/(X^3+X+1)$

1. Déterminer l'expression de $(1+\omega)\odot(\omega+\omega^2)$ sous la forme a+b$\omega+c\omega^2$
2. Déterminer l'expression de l'inverse de $1+\omega^2$ sous la forme a+b$\omega+c\omega^2$

Exemple 7. $\boldsymbol{F_{16}}$ (sera utilisé pour les codes correcteurs)

On part de $F_2[X]/(X^4+X+1)$

1. On vérifie que X^4+X+1 est irréductible.
2. On pose $\theta=$classe(X), chaque élément s'écrit alors $a+b\theta+c\theta^2+d\theta^3$, où (a,b,c,d) valent 0 ou 1.
3. On peut écrire les puissances de θ sous cette forme:

θ^0	1	[0001]
θ^1	θ	[0010]
θ^2	θ^2	[0100]
θ^3	θ^3	[1000]
θ^4	$1+\theta$	[0011]
θ^5	$\theta+\theta^2$	[0110]
θ^6	$\theta^2+\theta^3$	[1100]
θ^7	$1+\theta+\theta^3$	[1011]
θ^8	$1+\theta^2$	[0101]
θ^9	$\theta+\theta^3$	[1010]
θ^{10}	$1+\theta+\theta^2$	[0111]
θ^{11}	$\theta+\theta^2+\theta^3$	[1110]
θ^{12}	$1+\theta+\theta^2+\theta^3$	[1111]
θ^{13}	$1+\theta^2+\theta^3$	[1101]
θ^{14}	$1+\theta^3$	[1001]
0	0	[0000]

Travaux Dirigés

Exercice 2. On travaille avec $F_2[X]$

1. Vérifier que X^3+X^2+1 est irréductible

2. Vérifier que X^4+X^2+1 n'est pas irréductible

3. Vérifier que X^4+X^3+1 est irréductible

Exercice 3. Etude de $F_2[X]/(X^3+X^2+1)$

0. On admettra le théorème du cours et on note ω pour la classe de X

1. Liste des éléments sous la forme a+b$\omega+c\omega^2$

2. Liste des correspondances avec les puissances de ω.

3. Liste des inverses sous la forme a+b$\omega+c\omega^2$

Exercice 4. Etude de $F_2[X]/(X^4+X^3+1)$

0. On admet ce que dit le théorème du cours et on note θ pour la classe de X

1. Liste des éléments sous la forme a+b$\theta+c\theta^2+d\theta^3$

2. Liste des correspondances avec les puissances de θ.

3. Liste des inverses sous la forme a+b$\theta+c\theta^2+d\theta^3$

Exercice 5. Etude de l'ensemble M des matrices 2x2 à coefficients dans $F_2[X]/(X^4+X^3+1)$

1. Nombre d'éléments.

2. Soit A=$\begin{pmatrix} 1+\theta & \theta^3 \\ \theta^2 & 1+\theta^2 \end{pmatrix}$. Déterminer si A est inversible.

3. Soit B=$\begin{pmatrix} 1+\theta^2 & \theta \\ \theta^2 & 1+\theta^2 \end{pmatrix}$. Déterminer si B est inversible.

4. Soit X=$\begin{pmatrix} x \\ y \end{pmatrix}$, résoudre le système BX=(0).

Exercice 6. (avec maxima) à préparer !!!!!!!

on utilisera le package gf qui sera chargé par load(gf)

Etude de $K=F_2[X]/(X^7+X^3+1)$

nombre d'éléments (sans maxima)

table de multiplication

produit des matrices $\begin{pmatrix} 1+\theta+\theta^4 & \theta^3 \\ \theta+\theta^6 & 1+\theta^2+\theta^4 \end{pmatrix}$ et $\begin{pmatrix} 1+\theta^4+\theta^5 & \theta^3 \\ \theta+\theta^2 & 1+\theta^3+\theta^6 \end{pmatrix}$

Exercice 7. (suite du 6) Un essai de codage

on décide d'un principe de codage:

on choisit une matrice de codage G=$\begin{pmatrix} g_1 & g_2 \\ h_1 & h_2 \end{pmatrix}$ à coefficients dans K, puis tout message (a1,a2) (dont les éléments sont dans K) est transformé en $G\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$.

a. Sachant que le message reçu est $\begin{pmatrix} \theta^6+\theta^4+\theta^3+\theta^2 \\ \theta^5 \end{pmatrix}$ et que G=$\begin{pmatrix} \theta & \theta^3+\theta^2 \\ \theta^4+1 & \theta^5 \end{pmatrix}$, quel était le message original?

4. Cryptage fondé sur les propriétés du groupe $F_{2^d}^*$

Diffie-Hellman-ElGamal

Alice et Bob

4.1 Choix commun du groupe F_{2^d} et d'un générateur θ

(ceci revient à choisir le degré d et un polynôme irréductible dans $F_2[X]$ de degré 2.)

4.2 Alice choisit secrètement un exposant $\alpha \in \{2, ..., 2^d - 2\}$

et publie officiellement *($F_{2^d}, \theta, y_A = \theta^\alpha$)*

4.3 Bob choisit secrètement un exposant $\beta \in \{2, \ldots, 2^d - 2\}$

et publie officiellement *($F_{2^d}, \theta, y_B = \theta^\beta$)*

4.4 Bob veut envoyer à Alice le message m$\in F_{2^d}$; il le crypte : s=my_A^β

4.5 Alice décrypte s$y_B^{-\alpha}$ ce qui donne m$y_A^\beta y_B^{-\alpha} = m\theta^{\alpha\beta}\theta^{-\beta\alpha} = m$!

Remarque 8. La force de cet algorithme de cryptage réside dans le fait qu'il n'est pas possible facilement de trouver α quand on connait θ^α ou β quand on connait θ^β; c'est le problème du logarithme discret.

Une analyse montre que la difficulté du problème du logarithme discret est beaucoup plus grande lorsque le nombre d'éléments $2^d - 1$ du groupe $F_{2^d}^*$ est premier, ce qui nous ramène aux nombres de Mersenne.

Exemple 9.

Pour d= 7 $2^7 - 1$ est premier

conséquence F_{2^7} est un corps de 128 éléments et le groupe multiplicatif possède 127 éléments, il est cyclique.

Pour le « fabriquer » il faut un polynôme irréductible dans $F_2[X]$ de degré 7.

Il existe des listes de polynômes irréductibles dans $F_2[X]$ des divers degrés j'en ai vus jusqu'à d =11:

par exemple P(X)= (X^7+X^3+1).

Remarque 10.

Le groupe multiplicatif $G=F_{2^d}^*$ a pour cardinal 127, qui est premier, donc tous ses éléments, à part 1, sont d'ordre 127.

Choisissons g=θ, la classe de X.....