UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du diplôme de **Master**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Mathématiques Appliquées et discrètes

Par

Aimeur Hicham

Sujet

Polynômes irréductibles sur Le corps fini GF(2)
(Algorithme de Berlekamp)

Devant le jury composé de :

A. Amroune	Prof	Président	Univ de M'sila
C. Mihoubi	MC/B	Encadreur	Univ de M'sila
L. Ladjlat	MA/A	Examinateur	Univ de M'sila

Promotion : 2013/2014

Table des matières

Introduction :

Nous présentons d'une manière précise notre travail , en expliquant ce qui nous a guidé à un tel sujet , ainsi en présentant la problématique soulevée et en terminer par un portrait du plan général de ce travail.

Le develeppment de l'electronique , de l'information de la transimission de l'information , de nouveaux champs d'application de l'algèbre ont vu le jour , ces domaines font un grand usage de la structure de polynôme , corps finis.

Les polynômes sont des objet trés simples mais aux propriétés extêrmement , le corps fini intervient dans divers domaines des mathématique en particelier dans la théorie de Galois sur la résolution des équations algébriques , l'algorithme de Berlekamp a été découvert par Elwyn Berlekamp en 1967.

Comme le devoile son intitulé ""polynôme irréductible sur le corps finis F_2 "" , notre objectif est de cerner l'irréductible ou réductible sur un corps finis , pour ce faire nous envisagons de répondre à la problématique suivante :

que peut on dire de l'irreductiilité du polynôme

$$P(x) = a_n\, x^n + a_{n-1}x^{n-1} + \ldots + a_2\, x^2 + a_1 x + a_0 \quad \text{sur } F_2$$

Pour cela nous nous posons les question :

De quelles manières peut-on factoriser un polynôme sur F_2.

Notre modeste travail comporte trois chapitres :

Dans le premier chapitre , nous évoqons les principales propriétés des corps finis.

Dans le deuxiemme chapitre nous parlerons des polynômes irréductibles sur corps fini et dans le troisiemme chapitre nous présentons ""l'algorithme de Berlekamp "" puis nous decrivons d'une manière detaillée la factorisation d'un polynôme en utilisant cet Algorithme.

RESUME

Dans ce mémoire nous considèrons les polynômes sur un corps fini. la question centrale pour les polynôms dans $F_2[x]$, F_2 corps fini , est de décider quand un polynôme donné est irréductible ou non sur F_2 . Notre intention porte sur les polynômes de la forme :

$$P(x) = a_n\, x^n + a_{n-1}x^{n-1} + \ldots + a_2\, x^2 + a_1 x + a_0$$

avec $n \in N$ et $a_0, a_1, \ldots, a_n \in F_2[x]$.

MOTS-CLES : corps fini , Polynômes irréductibles , Algorithme de Berlekamp.

3.7 CONCLUSION

L'expréssion de ""Polynômes irréductibles sur corps finis"" se manifeste au 17 siècle , avec Newton et Leibniz qui donnent la façon pour établir les coefficients irréductiblés sur Q.

Le concepet de corps fini devient avec Discson au 1915 et ses résultat avec Euler ,Fermat , Lagrange et Gauss sur un corps F_p et p premier.

La construction d'un corps fini et l'extension d'un tel corps à été faite par ""Galois " en 1930 , l'algorithme de Berlekamp a vu le jour 1967.

Qu'est ce que veut dire l'irréductibilité d'un polynôme sur F_2

$$P(x) = a_n\, x^n + a_{n-1}x^{n-1} + \ldots + a_2\, x^2 + a_1 x + a_0$$

L'agorithme de Berlekamp est une méthode de factorisation des polynômes à coefficients dans un corps fini , qui repose sur des calculs de PGCD de polynômes et des opérations matricielles: Il a été découvert par Elwyn Berlekamp en 1967 , et est resté l'algorithme le plus performant concernant ce problème jusqu'en 1981.

3.8 BIBLIOGRAPHIE :

[1] ***A . BODIN*** *"Des Coures De GOUTING CHEN et Marc Bourdon" exo7.emath.fr/ficpdf/fic00007.pdf*

[2] ***A . BONNEGAZE*** *"Mathématique, Algèbre application" institut de mathématique de luniny , 2013.*

[3] ***A BUAF-R.BOYER*** *"Expose de matière factorisation dans $Z[X]$ " , sujet proposé par F.Loeser , 20 juin 2007.*

[4] ***A. CHERCHEM*** *" Cours de corps finis"1^{ere} anneé Master ACC , Université de Sciences et de la Technologie Houari Boumedienne , 2012/2013.*

[5] ***M. EISERMANN*** *"Introduction a la Cryptologie" Université Josèphe Fourier , 2008/2009.*

[6] ***L. LADJLAT*** *"Cours de corps fini et codes lineaires" 2^{eme} Master MA&D , Université de M'sila , 2013/2014.*

[7] ***C.MIHOUBI*** *"Etude Sur l'irréductible D'un Polynôme Sur Un Corps Finis " Mémoire pour l'obtenir Diplôme de Magister de TRONCOMMUN , Université de M'sila , 2001.*

[8] ***O.MOUSSI.*** *"Codes Cyclique Optimaux De Rendement 1/2 Sur F_2 " Mémoire pour l'obtenir Diplôme De Master Université De M'sila 2012/2013.*

[9] ***L.PIERRE*** *"Polynôme irréductible " Corps de rupture .Exemples et application , 2010.*

[10] ***G .Renault*** *"Corps Finis " généraux /Polyny .UPMC/UNRIALE , 2013.*

[11] ***M.PIERRE*** *"Déterminants, ranges, systèmes Linéaires" Département de Mathématique Faculité de Sciences , liège , 21 Février 2013.*

[12] ***J. STREN*** *"Licence D'information Algorithmique et Programmation " Coures avance 2010/2011.*

[13] ***R. ROBERT*** *"Introduction à L'étude Des Corps Finis " Résume.robert.rolland.acrypta.com/telechargements/algebre/**corpsfinis.pdf**.*

*[14] **M. ROMAGNY** "factorisation des polynomes sur les corps finis" .*
*perso.univ-rennes1.fr/matthieu.romagny/agreg/theme/Berlekamp.**pdf**.*
*[15] **M. VIENNEY**" Corps Finis ".*
*WWW.umpa.ens-lyon.fr/~mvienney/agreg/**corps_finis.pdf***
*[16] **Corps Finis** WWW.H.K.fr/ Publication / Objectifs. Agrégation.*