N° : 04 / PGS-2004/ MT

République Algérienne Démocratique et Populaire

Université des Sciences et de la Technologie Houari Boumediene

Faculté des mathématiques

Mémoire de Post-Graduation Spécialisée en Mathématiques

Spécialité : Cryptologie

Présenté par :

Monsieur : AOUINA Mohamed

Sujet :

Corps Finis et Applications

Soutenu le 25 / 03 / 2004

Devant le jury composé de :

M^{r} : HACHAICHI Mohamed .S, Maître de conférences, USTHB	**Président**
M^{r} : ZITOUNI Mohamed, Professeur, USTHB	**Directeur de Mémoire**
M^{r} : BENTINA Kamel, Professeur, USTHB	**Examinateur**
M^{r} : HAMITI Hassan, D.G.S.C.T	**Examinateur**

Sommaire

I Introduction

La théorie des corps finis est un domaine de la Théorie des Nombres, c'est pour cela que les ouvrages de Théorie des Nombres contiennent un chapitre sur les corps finis.

Les corps finis sont utilisés dans plusieurs domaines comme le codage, la cryptographie, les Courbes Elliptiques supersingulières.

Un corps fini a une structure de corps , une structure d'espace vectoriel ,une structure de groupe cyclique

indiquons quelques détails sur ces structures.

II. Structures algébriques

1. Structure de corps

Dans la théorie des corps, un corps infini, K, contient un sous corps isomorphe au corps Q 'des nombres rationnels' Comme Q est de caractéristique nulle, il en est de même des corps de nombres.

Il en résulte qu'un corps fini est de caractéristique égale à un nombre premier p non nul.

Proposition 1

Tout corps fini IF est de caractéristique un nombre premier p positif . Le nombre de ses éléments est égal à une puissance p^n de la caractéristique p.

□

L'anneau Z/pZ des classes résiduelles modulo un nombre premier p est un corps $IF_P = Z/pZ$ .Ce corps ne contient pas de sous corps propre ; par définition IF_P est un corps primitif.

Proposition2

Tout les corps finis IF_q à $q = p^n$ éléments sont isomorphes au corps fini $Z/p^n Z$.

□

Exemple

Le corps fini IF_{19}^5 contient 19^5 éléments

En cryptographie, les spécialistes manipulent les corps finis tels que IF_2^{1500} à 2^{1500} éléments.

Dans la théorie des corps de nombres algébriques, de degré fini tout corps $K=Q(\theta)$ admet un élément primitif θ . Ce nombre θ est une racine d'un polynôme irréductible minimal , de degré égal au degré $[K:Q]$ du corps K.

C'est un polynôme $f_\theta(x)$ dans l'anneau $Z[x]$, le corps K est le corps de décomposition de $f_\theta(x)$ s'il contient toutes les racines de ce polynôme.

Les corps finis obéissent à cette règle

Proposition3

Tout corps fini IF_q à $q = p^n$ éléments pour $n \geq 1$, est le corps de décomposition du polynôme $f(x) = x^q - x$ avec $q = p^n$.

□

Exemple

Le polynôme $f(x) = x^{p^n} - x$ avec p=11 et n=20 est de degré 11^{20}. Il admet donc 11^{20} racines qui sont $x_0 = 0, x_1 = a , x_2 = a^2, \ldots\ldots, x_N = a^N$ où $N = 11^{20} - 1$

Proposition4

Les éléments non nuls de IF_P^n forment un groupe multiplicatif cyclique à $p^n - 1$ éléments

$$IF^*_m = \{g, g^2, g^3, g^4, g^5, \ldots\ldots g^{m-1} = 1\} \text{ , avec } m = p^n$$

□

Exemple : Le polynôme $f(x)= x^m-x$ avec $m =11^{20}$ ce polynôme se factorise sous la forme $f(x)= x(x^n-1)$ où $n=11^{20}-1$ l'équation $x^n-1=0$ admet comme racine g
est une racine primitive n^{emé} de 1, les autres racines n^{e} de 1 sont les puissances $g, g^2, g^3, g^4, ..., g^n=1$, qui forment un groupe cyclique .

Le polynôme $f(x) = x^{p^n} - x$ est de degré p^n sa dérivée est égale à $f'(x) = p^n x^{p^n-1} - 1$ cette dérivée est un polynôme premier à $f(x)$ il en résulte que toutes les racines de $f(x)$ sont simples.

II. 2- structure d'espace vectoriel

Chaque corps fini IF_P^n, pour $n \geq 1$, est une extension algébrique du corps primitif IF_P , de degré n = $[IF_P^n : IF_P]$
Il en résulte que IFp^n à une structure d'espace vectoriel, sur le corps IF_P de dimension n égale au degré $[IFp^n : IF_P]$ de l'extension de ce corps. Donc cet espace vectoriel, IF_P^n admet une base ω_1 , ω_2 ,……. ω_n de n éléments. Ainsi tout élément a de IF_P^n se met sous la forme unique :

$a = a_1\omega_1 + a_2\omega_2 + a_3\omega_3 + a_4\omega_4 + \ldots\ldots\ldots\ldots\ldots + a_n\omega_n$

à coefficients a_i dans le corps de base IF_P .

II 3. Inclusion de corps finis et automorphismes

Proposition5

Soit un corps fini IF_P^n , $n \rangle 1$. Alors tout sous corps de IF_P^n est un corps fini IF_P^d, pour tout diviseur d de n. Donc le corps IF_P^n est une extension normale et séparable du sous corps IF_P^d .

□

Corollaire

Soit deux corps finisIF_1 et IF_2 satisfaisant l'inclusion $IF_1 \subset IF_2$. Alors IF_1 et IF_2 ont même caractéristique p et si $IF_1 = IF_P^n$, alors $IF_2 = IF_P^d$ pour un diviseur d de n.

□

Exemple

Sous corps du corps fini IF_7^{12} .Ces sous corps sont associés aux diviseurs de 12 donc $d = 2,3,4,6$.

Nous obtenons deux tours d'extensions de corps

$IF_7 \subset IF_7^2 \subset IF_7^4 \subset IF_7^{12}$ et $IF_7 \subset IF_7^3 \subset IF_7^6 \subset IF_7^{12}$

II. 4. Endomorphisme de Frobenius

Le corps primitif IF_P admet un seul automorphisme

$$IF_P \longrightarrow IF_P$$

C'est l'application identique.

L'application f: $IF_P \longrightarrow IF_P$ de valeur $f(a) = a^d$

Implique $f(a+b) = (a+b)^d = a^d + \ldots\ldots\ldots + b^d \neq a^d + b^d = f(a)+f(b)$

Donc f n'est pas un automorphisme lorsque $d \neq p$. Pour, $n \geq 1$, le corps fini IF_P^n admet un groupe d'automorphisme non trivial.

Proposition6

Chaque corps fini IF_P^n , $n > 1$, admet un groupe d'automorphismes, cyclique d'ordre n, ce groupe est engendré par l'endomorphisme de Frobenius F_{rob} : $IFp^n \longrightarrow IFp^n$,de valeur $F_{rob}(a) = a^p$ pour tout élément a de IF_P^n

□

III .Anneaux des polynômes $A = IFp^n[x]$

Le corps fini IF_P^n étant de caractéristique p, il en est de même de la caractéristique de l'anneau A ; cela implique des coefficients $a_i \bmod p$

Mais les degrés des polynômes de l'anneau sont indépendants de p

Il y a des polynômes de tout degré dans l'anneau A.

Par définition, un polynôme $f(x)$ de l'anneau A est irréductible s'il est divisible que par lui-même et par un élément inversible de IF_P^n.

Un polynôme est décomposable s'il est produit de deux polynômes au moins, de degrés au moins un. Dans tout anneau, il y a des idéaux.

Un idéal engendré par un polynôme $f(x)$ de A est de la forme $f(x)A$

Proposition7

L'anneau quotient $A/f(x)A$ d'un anneau $A = IF_P^n[x]$ par un idéal $f(x)A$ engendré par un polynôme irréductible, est un corps.

□

Donc toute classe de l'anneau quotient $A/f(x)A$ est inversible.

Exemple

Soit le corps fini IF_5 et l'anneau de polynômes $A= IF_5[x]$, le polynôme $f(x)= x^3 +x +1$ est irréductible dans A. Alors l'anneau quotient $A/(x^3 +x +1) A$ contient les classes de polynômes $ax^2 +bx +c$, x^2, x et 1.

L'inverse de $cl\ x^2$ est $cl\ x$. Il y a plusieurs méthodes pour factoriser un polynôme $f(x)$ dans cet anneau de polynôme.

Exemple1

Factoriser le polynôme $f(x) = 2x^4 + x^3 + 2x^2 + 4x + 1$ dans l'anneau $A = IF_{25}[x]$

Nous cherchons les racines de $f(x)$ en calculant $f(a)$ pour $a=0,1,.....$

Nous obtenons $f(1) = 0 = f(-1) = f(-2)$

Cela implique que $f(x)$ est divisible par $x - 1$, $x + 1$ et $x + 2$

avec la division euclidienne des polynômes dans l'anneau $IF_{25}[x]$

Nous obtenons la factorisation en polynômes irréductibles

$f(x) = 2(x-1)(x+2)(x+1)^2$

Exemple2

Factoriser $f(x) = x^3 + 4x^2 + 5x + 4$

Les calculs donnent $f(a) \neq 0 \bmod 5$ pour $a=0,1,2,3$ et 4

Donc $f(x)$ n'est pas de facteur de degré 1

Supposons un facteur de degré 2

$$f(x) = (ax^2 + bx + c)(dx + e)$$

Dans ce polynôme, il y a un facteur de degré 1 or $f(x)$ n'admet pas de facteur de degré 1.

Donc $f(x)$ est irréductible dans l'anneau $IF_{25}[x]$

Il y a un autre critère d'irréductibilité d'un polynôme.

Proposition 8

Soit un polynôme $f(x)$ de degré k dans l'anneau $IF_P^n[x]$, $n \geq 1$.

Alors $f(x)$ est irréductible si et seulement les polynômes $f(x)$

et $g_j(x) = x^{p^j-1} - x$ sont premiers entre eux pour $j= 1,2,\ldots..[\frac{k}{2}]$

Où $[\frac{k}{2}]$ est la partie entière de $\frac{k}{2}$, pgcd ($f(x)$, $g_j(x)$) =1

□

Exemple1:

Soit le polynôme $f(x) = 3x^{10} + x^8 + 5x^7 + 4x^5 + 3x^4 + 6x^3 + 4x + 6$

de degré 10 dans l'anneau $IF_7[x]$

Appliquons l'algorithme de calcul de l'exemple précédent

On donne le polynôme $f(x) = 3x^{10} + x^8 + 5x^7 + 4x^5 + 3x^4 + 6x^3 + 4x + 6$

Etudier leurs décompositions

1- décomposition de $f(x)$

nous calculons les valeurs $f(d)$ pour $d=0,1,2,3,4,5$ et 6 pour les facteurs éventuels, de degré 1

$f(0)=6 \neq 0 \bmod 7 \ldots\ldots\ldots\ldots(1)$

$f(1)=4 \neq 0 \bmod 7 \ldots\ldots\ldots\ldots .(2)$

$f(2)=2 \neq 0 \bmod 7 \ldots\ldots\ldots\ldots(3)$ n'admet pas de facteur de degré1

$f(3) \neq 0 \bmod 7 \ldots\ldots\ldots\ldots\ldots(4)$

$f(4)=4 \bmod 7 \ldots\ldots\ldots\ldots\ldots\ldots(5)$

$f(5)=3 \bmod 7 \ldots\ldots\ldots\ldots\ldots(6)$

$f(6)=1 \bmod 7 \ldots\ldots\ldots\ldots\ldots(7)$

Ces valeurs impliquent que le polynôme $f(x)$ n'admet pas de facteur du $1^{\underline{er}}$ degré

Algorithme de factorisation du polynôme

$f(x) = 3x^{10} + x^8 + 5x^7 + 4x^5 + 3x^4 + 6x^3 + 4x + 6$ (1)

dans l'anneau $IF_7[x]$

recherche d'un facteur irréductible du 2e degré

$g(x) = x^2 + ax + b$ avec $g(x) \neq 0$ pour $d = \pm 1, \pm 2, \pm 3$

$b \neq 0$ (2)

Posons

$f(x) = 3g(x)[x^8 + \ldots\ldots] = 3g(x)\,h(x)$

avec $h(x) = x^8 + t_7x^7 + t_6x^6 + t_5x^5 + t_5x^5 + t_4x^4 + t_3x^3 + t_2x^2 + t_1x + t_0$ (3)

le calcul donne le produit $g(x)h(x)$

$g(x)h(x) = x^{10} + N_9x^9 + N_8x^8 + N_7x^7 + N_6x^6 + N_5x^5 + N_4x^4 + N_3x^3 + N_2x^2 + N_1x + N_0$

les coefficients $N_9 \ldots\ldots N_0$ sont

$N_9 = a + t_7 = 0$ (4)

$N_8 = t_6 + a\,t_7 + b = 5$

$N_7 = a\,t_6 + bt_7 = 4$

$N_6 = a\,t_5 + bt_6 = 0$

$N_5 = a\,t_4 + bt_5 = 6$

$N_4 = a\,t_3 + bt_4 = 1$

$N_3 = a\,t_2 + bt_3 = 2$

$N_2 = a\,t_1 + bt_2 = 0$

$N_1 = a\,t_0 + bt_1 = 6$

$N_0 = bt_0 = 2$

Les nombres a, b, t_i et N_i sont liés par les congruences

$3N_9 = 0,\ 3N_8 = 1,\ 3N_7 = 5,\ 3N_6 = 0,\ 3N_5 = 4$

$3N_4 = 3,\ 3N_3 = 6,\ 3N_2 = 0,\ 3N_1 = 4,\ 3N_0 = 6$ (5)

La congruence $3\times5 \equiv 1 \bmod 7$ et *(5)* impliquent les congruences *mod 7*

$N_9 = 0$, $N_8 = 5$, $N_7 = 4$, $N_6 = 0$, $N_5 = 6$, $N_4 = 1$

$N_3=2$, $N_2=0$, $N_1=6$ et $N_0=2$ (6)

Les relations (1), (2), (3) et (4) impliquent les nombres $N_9, \ldots\ldots N_0$

$N_9 = a + t_7$, $N_8 = t_6 + a\ t_7 + b$, $N_7 = a\ t_6 + bt_7$, $N_6 = a\ t_5 + bt_6$,

$N_5 = a\ t_4 + bt_5$, $N_4 = a\ t_3 + bt_4$, $N_3 = a\ t_2 + bt_3$, $N_2 = a\ t_1 + bt_2$,

$N_1 = a\ t_0 + bt_1$, $N_0 = bt_0$ (7)

(6), (7) impliquent la congruence $bt_0 = 2$ *(8)*

Elle admet les solutions

b	1	2	3	4	5	6
t_0	2	1	3	4	6	5

(9)

1) Cherchons une factorisation $f(x) = 3g(x).\ h(x)$ pour $b=1$, $t_0 = 2$ *(10)*

$N_9 = a + t_7$, $N_8 = t_6 + a\ t_7 + b$, $N_7 = a\ t_6 + bt_7$

impliquent les 3 équations

$t_7=-a$, $t_6= a^2+4$, $a(a^2+ 3) = 4$

Elles admettent une seule solution :

$a=1$, $t_6= 5$, $t_7=6$ *(11)*

la valeur $N_6 = a\ t_5 + t_6 = 0$ et (10) donnent la solution

$t_5=1$ *(12)*

L'équation $N_5 = a\ t_4 + t_5 = 6$ admet la solution

$t_4=5$ *(13)*

L'équation $N_4 = a\ t_3 + t_4 = 1$ admet la solution

$t_3=3$ *(14)*

L'équation $N_3 = a\ t_2 + t_3 = 1$ admet la solution

$t_2=1- t_3 =5$ *(15)*

L'équation $N_2 = a\ t_1 + t_2 = 0$ admet la solution

$t_1=-t_2 = 2$ *(16)*

L'équation $N_1 = 2a + t_1 = 6$ admet la solution

$$t_1 = 6 - 2a = 4 \qquad (17)$$

La relation $2 \neq 4$ impliquent une contradiction

Il en résulte que la solution $a = 1$, $b = 2$

Ne donne pas de factorisation de $f(x)$

2) Factorisation pour $b = 2$, $t_0 = 1$

$N_9 = a + t_7 = 0 \qquad (1)$

$N_8 = t_6 + a\, t_7 = 3 \qquad (2)$

$N_7 = a\, t_6 + 2t_7 = 4 \qquad (3)$

Ces 3 équations donnent :

$t_7 = -a \qquad (4)$

$t_6 = a^2 + 4 \qquad (5)$

$at_6 - 2a = 4 \qquad (6)$

Ces 2 équations (5) et (6) donnent

$a(a^2 + 1) = 4 \qquad (7)$

L'équation (7) une seule solution a= 5 (8)

(4) et (5) donnent les solutions $t_6 = 0$, $t_7 = 2$ (9)

L'équation $N_6 = a\, t_5 + bt_6 = 0$ admet la solution

$t_5 = 0$

L'équation $N_5 = a\, t_4 + bt_5 = 6$ admet la solution

$t_4 = 4$

L'équation $N_4 = a\, t_3 + bt_4 = 1$ admet la solution

$t_3 = 0$

L'équation $N_3 = a\, t_2 + bt_3 = 2$ admet la solution

$t_2 = 6$

L'équation $N_2 = a\, t_1 + bt_2 = 0$ admet la solution

$t_1 = 6$

L'équation $N_1 = a\, t_0 + bt_1 = 6$ admet la solution

$t_0 = 3$

Mais cette solution $t_0=3$ n'est pas compatible avec $t_0=1$

Donc pas de factorisation de $f(x)$

3) Factorisation pour $b=t_0=3$

$N_9 = a+ t_7 =0$, $N_8 = t_6 + a\, t_7 =2$ et $N_7 = a\, t_6 + 2t_7 = 4$

admettent la solution

$t_7 = -a$, $t_6 = 2 + a^2$ et $a(a^2 -1) = 4$

les équations admettent la solution

$a=4$, $t_6 =4$, $t_7 =3$

L'équation $N_6 = a\, t_5 + bt_6 = 0$ admet la solution

$t_5=4$

L'équation $N_5 = a\, t_4 + bt_5 = 6$ admet la solution

$t_4=2$

L'équation $N_4 = a\, t_3 + bt_4 = 1$ admet la solution

$t_3=4$

L'équation $N_3 = a\, t_2 + bt_3 = 2$ admet la solution

$t_2=1$

L'équation $N_2 = a\, t_1 + bt_2 = 0$ admet la solution

$t_1=1$

L'équation $N_1 = a\, t_0 + bt_1 = 6$ admet la solution

$t_0=6$

Mais cette solution est contraire à l'hypothèse $t_0=3$

Donc : pas de factorisation de $f(x)$

4) Factorisation pour $b=t_0=4$

$f(x)=x^2+ax+b$ avec a^2-4b non carré $mod7$ alors $f(x)$ se met sous la forme

$f(x)=3(x^2+ax+b)(x^8+t_7x^7+t_6x^6+t_4x^4+t_3x^3+t_2x^2+t_1x+t_0)$

où les coefficients $t_7\ldots\ldots\ldots t_0$ sont dans le corps IF_7 .

En effectuant le produit du 2e membre nous obtenons un système de congruences $mod7$

Coefficient de x^9 $0=3(a+t_7)$, cela implique $t_7=-a$ *(1)*

Coefficient de x^8 , $1=3(t_6+at_7+b)$ nous multiplions par l'inverse $3^{-1}=5$

Nous obtenons une 2e condition $5=t_6+at_7+b$ *(2)*

Coefficient de x^7 , $5=3(t_4+at_6+bt_7)$ nous multiplions par l'inverse $3^{-1}=5$
Nous obtenons une 3e condition $4=t_4+at_6+bt_7$ *(3)*

Mais on peut utiliser **maple** pour factoriser ce polynôme

```
> Factor(3*x^10 +x^8 +5*x^7 + 4*x^5 +3*x^4 +6*x^3 +4*x+6)
mod 7 ;
```

$3x^{10}+x^8+5x^7+4x^5+3x^4+6x^3+4x+6$

Donc : f est un polynôme irréductible

Exemple2:

Dans l'anneau $IF_{17}[x]$

On donne le polynôme $f(x) = x^6 - x^3 + 1$ étudier leurs décomposition

On commence pour calculer les valeurs f(d) pour $d = 0,1,2,.....16$

Mais : $f(d) \neq 0 \ mod 17$ avec $d=0,1,2,....,16$

Le polynôme $f(x)$ n'admet pas de facteurs linéaires.

Recherche d'un facteur quadratique irréductible.

$f(x)=(x^2 + ax + b)(x^4 + cx^3 + kx^2 + ex + m) \ mod 17$

Cette congruence implique les congruences suivantes :

$0 \equiv (c+a) mod\ 17 \ldots\ldots\ldots\ldots\ldots\ldots (1)$

$0 \equiv (k+ca+b)\ mod 17 \ldots\ldots\ldots\ldots\ldots (2)$

$-1 \equiv (e+ka+bc)\ mod 17 \ldots\ldots\ldots\ldots (3)$

$0 \equiv (m+ae+kb)\ mod 17 \ldots\ldots\ldots\ldots (4)$

$0 \equiv (am+eb)\ mod\ 17 \ldots\ldots\ldots\ldots\ldots (5)$

$1 \equiv bm\ mod\ 17 \ldots\ldots\ldots\ldots\ldots\ldots (6)$

Système de 6 équations à 6 inconnues

Ce système admet la solution $a=7$, $b=1$, $c=-7$, $k= 14$, $e=-7$, $m= 1$

Nous en déduisons la factorisation en polynômes irréductibles

$f(x)= (x^2 + 7x + 1)(x^4 - 7x^3 + 14x^2 - 7x + 1) mod 17$

III Générateurs du groupe IF^*_q avec $q= p^n$ et racines primitives n^{eme} del'unite

Le groupe multiplicatif cyclique IF^*p^n admet p^n-1 éléments et $\Phi(p^n-1)$ générateurs , où Φ désigne la fonction arithmétique d'Euler les ordres des éléments d'un groupe satisfont la

Théorème de Lagrange

Dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe

□

Définition1

Un générateur du groupe cyclique $(Z/p^nZ)^*$ *pour* $n\geq 1$ *est une racine primitive modulo* p^n *.Un générateur est donc un élément a du groupe solution de la congruence.*

$$a^{q-1} \equiv 1 \bmod q \quad avec \quad q= p^n$$

L'isomorphisme des corps finis IFp^n et Z/p^nZ implique l'isomorphisme des groupes abéliens finis $IF^*_{P^n} \longrightarrow (Z/p^nZ)^*$ avec $g \longrightarrow a$ générateurs respectifs de 2 groupes $q = p^n$

Cette propriété donne un moyen de calcul d'un générateur

Nous choisissons un élément g non nul dans le corps IF_q

$g, g^2, g^3, g^4, g^5, \ldots\ldots g^{(m-1)/2}$ avec $m = p^n$

Si $g^{(m-1)/2} = -1$ alors g est un générateur sinon g n'est pas un générateur

On commence pour calculer les puissances de g dès qu'on obtient une puissance $g^2 \equiv -1 \bmod q$, alors 2 cas possible lorsque $r = (q-1)/2$ alors g est un générateur . Lorsque $r < (q-1)/2$ alors g n'est pas un générateur.

Il faut tester un autre élément g. Jusqu'à l'obtention d'un générateur

Exemple1

Le groupe multiplicatif $(Z/109Z)^*$ est d'ordre 108, il admet $\Phi(108) = 36$ racines primitives modulo 109.

Appliquons l'algorithme de calcul en testant les éléments

Test de $g = 2$: nous calculons les puissances de 2 jusqu'à l'obtention de -1 ou 1. Nous obtenons $2^{18} \equiv -1 \bmod 109$, donc 2et d'ordre $36 < 108$

2 n'est pas une racine primitive mod 109

Les calculs des puissances de 3 donnent $3^{27} \equiv -1 \bmod 109$ donc 3 n'est pas un générateur.

Les calculs des puissances de 6 donnent $6^{54} \equiv -1 \bmod 109$ donc 6 est un générateur.

Exemple2

Le groupe $(Z/13Z)^*$ admet 12 éléments et $\Phi(12) = 4$ générateurs

On calcule les puissances jusqu'à l'ordre 6.

Nous trouvons $2^6 = -1$; donc $g_1 = 2$ est un générateur ; c'est aussi une racine primitive *mod 13.*

Le calcul des puissances des autres éléments donne

les trois autres générateurs : $g_2 = 6$, $g_3 = 7$ et $g_4 = 11$.

Exemple3

Générateur du groupe $(Z/23Z)^*$, ce groupe admet 22 éléments et $\Phi(22) =$ 10 éléments générateurs.

On calcule les puissances $a, a^2, \ldots\ldots a^{11}$

On peut faire les calculs

Il y a un autre critère pour déterminer les racines primitives d'un groupe fini IF^*_q avec $q = {}_P{}^n$

Proposition10

Soit le corps fini IF_q , $q = p^n$ $n \geq 1$ .Alors un élément g du groupe multiplicatif IF_q^* est une racine primitive si et seulement si chaque diviseur premier d de $q - 1$ satisfait les congruences : $g^{(q-1)/d} \not\equiv 1 mod q$

□

Exemple 1

Calcul des générateurs du groupe multiplicatif IF_{49}^*, ce groupe contient 48 éléments. Les générateurs de ce groupe sont au nombre de $\Phi(48) = \Phi(2^4).\ \Phi(3) = 16$ générateurs, Appliquons le test : $g^{(q-1)/d} \equiv 1 mod q$ à $q = 7^2$ les diviseurs premiers de 48 sont d= 2,3.appliquons l'algorithme de calcul des puissances $g^{48/d}$

Nous testons g=2

il faut calculer $g^{48/2} = g^{24}\ mod\ 49$ et $g^{48/3} = g^{16}\ mod 49$

nous obtenons $g^{48/2} = g^{24} = 11$ et $g^{48/3} = g^{16} = 15$ le critère 9 est satisfait

dans le corps fini IF_{49} , calcul de 2^{16} et 2^{24}

$2^4 = 16,\ (2^4)^2 = 2^8 = 16^2 = 11,\ \ 2^{16} = 121 = 24 \neq 1 mod 49$

$2^{24} = 2^{16}\ 2^8 = 11.24 = 264 = 19 mod 49$ donc $2^{24} \neq 1 mod 49$

Le critère s'applique à $g_1 = 2$ est une racine primitive de IF_{49}^*

Pour $g = 3$ on obtient $g^{16} = 16$ et $g^{24} = 18$ donc $g_2 = 3$ est une autre racine primitive.

Exemple (Application1)

Nous allons étudier plus détails la construction ou plutôt les constructions du corps IF_2^8 pour cela, nous allons tout d'abord commencer de factoriser le polynôme $x^n - x$ avec $n = 2^8$ ce calcul peut se faire

soit à la main (utilisant un méthode de classes cyclotomiques)

soit en utilisant un logiciel type **maple** .

J'ai utilisé logiciel maple pour factoriser ce polynôme $x^n - x$ avec $n = 2^8$

Donc

```
> Factor(x^256-x) mod 2;
```

$$(x^8+x^7+x^5+x^3+1)(x^8+x^6+x^5+x^2+1)(x^8+x^7+x^3+x^2+1)$$
$$(x^8+x^7+x^6+x^4+x^3+x^2+1)(x^8+x^6+x^5+x^4+1)(x^4+x^3+x^2+x+1)$$
$$(x^8+x^6+x^5+x^4+x^3+x+1)(x^2+x+1)(x^8+x^7+x^6+x^5+x^4+x^3+1)$$
$$(x^8+x^4+x^3+x^2+1)(x^8+x^7+x^6+x^5+x^4+x^2+1)(x^8+x^4+x^3+x+1)\,x$$
$$(x^8+x^6+x^5+x^4+x^2+x+1)(x^8+x^7+x^6+x^4+x^2+x+1)(x^8+x^7+x^2+x+1)$$
$$(x^8+x^7+x^5+x^4+x^3+x^2+1)(x^8+x^7+x^6+x^5+x^2+x+1)$$
$$(x^8+x^7+x^5+x^4+1)(x^8+x^6+x^5+x^3+1)(x^8+x^6+x^4+x^3+x^2+x+1)$$
$$(x^8+x^7+x^6+x+1)(x^4+x+1)(x^8+x^5+x^3+x+1)(x^4+x^3+1)$$
$$(x^8+x^5+x^4+x^3+x^2+x+1)(x+1)(x^8+x^5+x^4+x^3+1)$$
$$(x^8+x^7+x^4+x^3+x^2+x+1)(x^8+x^7+x^6+x^3+x^2+x+1)(x^8+x^6+x^3+x^2+1)$$
$$(x^8+x^7+x^3+x+1)(x^8+x^7+x^5+x+1)(x^8+x^6+x^5+x+1)$$
$$(x^8+x^5+x^3+x^2+1)(x^8+x^7+x^6+x^5+x^4+x+1)$$

>

Finalement nous obtenons que $x^8 + x^4 + x^3 + x + 1$ est un polynôme irréductible

```
> Irreduc(X^8+x^4+x^3+x+1) mod 7;
```

true

Soit α une racine de ce polynôme dans une extension de IF_2 .

Alors α est un élément primitif. Tous les polynômes degré inférieur à 8 forment une classe de polynômes modulo $(x^8 + x^4 + x^3 + x + 1)$ ils sont :

```
> G256 := GF(2,8,alpha^8+alpha^4+alpha^3+alpha+1):
a := G256[ConvertIn](alpha);
```

$a := \alpha$

```
> G256[`*`](a,a);
```

α^2

```
> G256[`^`](a,4);
```

α^4

```
> x := G256[`^`](a,8);
```

$x := 1 + \alpha + \alpha^3 + \alpha^4$

```
> G256[`^`](a,16);
```

$\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6$

```
> G256[`^`](a,254);
```

$1 + \alpha^2 + \alpha^3 + \alpha^7$

```
> G256[`^`](a,255);
```

1

Polynômes	Notation utilisant les valeurs des coefficients en x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	1
x	0	0	0	0	0	0	1	0
x^2	0	0	0	0	0	1	0	0
. .. x^4	0	0	0	1	0	0	0	0
.... x^8	0	0	0	1	1	0	1	1
... x^{16}	0	1	0	1	1	1	1	0
x^{254}	1	0	0	0	1	1	0	1
x^{255}	0	0	0	0	0	0	0	1

Cet ensemble contient 2^8 éléments c'est le IF_2^8

Pour définir le corps, il faut définir les opérations d'addition et de multiplication.

1. multiplication : nous utilisons la notation en puissance de x :
   $x^i x^j = x^{(i+j) \bmod (m-1)}$ avec $m = 2^8 = 256$
2. l'addition : nous utilisons la notation en polynôme de x.On fait la somme bit par bit modulo 2

Exemple2 : Nous allons étudier la deuxième application de la construction du corps IF_2^4 pour cela, nous factorisons le polynôme $x^n - x$ avec $n = 2^4$ ce calcul se fait
- soit à la main
- soit en utilisant un logiciel type **maple**

Nous obtenons que $x^4 + x + 1$ est un polynôme irréductible. Soit α une racine de ce polynôme dans une extension de IF_2.

Alors α est un élément primitif et nous avons la table suivante :

α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	1100
α^7	$\alpha^3 + \alpha^2 + 1$	1101
α^8	$\alpha^2 + 1$	0101
α^9	$\alpha^3 + \alpha$	1010
α^{10}	$\alpha^2 + \alpha + 1$	0111
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101
α^{14}	$\alpha^3 + 1$	1001
α^{15}	1	0001

Nous calculons alors que les facteurs irréductibles de $x^{16}-x$ sont :

x (racine 0)

$x-1$ (racine 1)

x^4+x+1(racine α , $\alpha^2,\alpha^4,\alpha^8$)

$x^4+x^3+x^2+x+1$ (racine $\alpha^3,\alpha^6,\alpha^{12},\alpha^9$)

x^2+x+1 (racine α^5,α^{10})

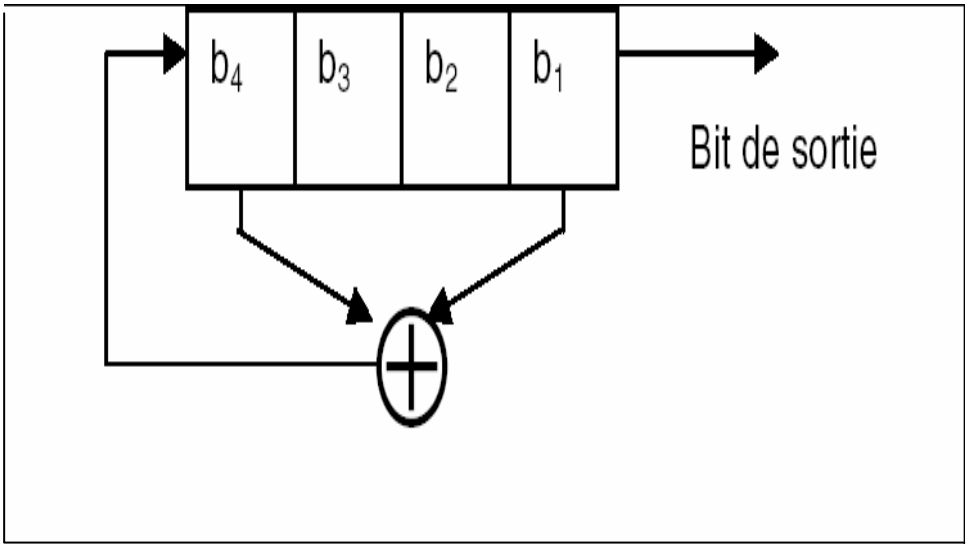
x^4+x^3+1 (racine α^{11} , $\alpha^7,\alpha^{14},\alpha^{13}$)

Donc :

$$x^{16}-x = x(x-1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$$

On peut utiliser **RDRL** pour trouver les polynômes

RDRL signifie Registre à Décalage à Rétroaction Linéaire. Les séquences de registre à décalage s'utilisent à la fois en cryptographie et en Théorie des codes. Il existe une théorie très riche à leur propos; les algorithmes de chiffrement en continu basés sur des registres à décalage ont été le cheval de bataille des cryptographes.



Bit de sortie

La figure ci-dessus représente un RDRL de 4 bits, dérivé au premier et au quatrième bit. Pour l'exemple qui suit, le registre est initialisé avec la valeur 1111. Le bit introduit par décalage dans le registre (à gauche) est déterminé à partir de l'état présent en fonction des connexions avec l'additionneur modulo-2 (Rétroaction). La séquence des états du circuit donne forcément lieu à un cycle; la sortie se répète donc après un certain temps. La longueur maximale de séquence qui peut être produite est égale à 2^{n-1} où n est le degré du registre à décalage. Dans ce cas, la séquence des états passe par tous les états non nuls possibles avant de se répéter. Mais Dans le cas de l'exemple illustré, la séquence d'états est :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1111	0111	1011	0101	1010	1101	0110	0011	1001	0100	0010	0001	1000	1100	1110

Le polynôme correspondant à l'exemple est $x^4 + x + 1$.

La première connexion du registre (à gauche) correspond au terme x^4, la dernière connexion (à droite) correspond au terme x. Le terme 1, toujours présent dans un polynôme n'est pas associé à une connexion .Une solution consiste à faire tourner 16 RDRL

Exemple3 Pour travailler dans IF_7^3, cherchons un polynôme irréductible du type x^3+a dans $Z/7Z$. Comme le degré est 3, x^3+a est irréductible seulement si il n'a pas de racine.

```
> for i from 0 to 6 do i^3 mod 7; od;
```

0

1

1

6

1

6

6

Donc x^3-2, x^3-3, x^3- 4, x^3-5 sont irréductibles. Prenons, par exemple x^3+3.

```
> Irreduc(X^3+3) mod 7;
```

true

Les éléments de IF_7^3, sont donc les $(a+bx+cx^2)$ *modulo* 7 et x^3+3.

Testons x : [0 1 0], est-il générateur ?

```
> Test_Poly_Générateur( 7, X^3+3, X );
      Facteurs de 342 : 2, 3, 19
        A^171 : 1
        A^114 : 2
        A^18 : 1
```

false

Prenons un élément au hasard (ou presque) : [3 3 6], est-il générateur ?

```
> Test_Poly_Générateur( 7, X^3+3, 3+3*X+6*X^2 );
      Facteurs de 342 : 2, 3, 19
        A^171 : 6
        A^114 : 2
        A^18 : 2*X^2+6
```

true

Generator $:= 3 + 3\,X + 6\,X^2$

```
> Generator:=3+3*X+6*X^2;
```

$$Generator := 3 + 3\,X + 6\,X^2$$

```
> Factor(x^343-x) mod 7 ;
```

$$(x^3+2x^2+x+4)\,(x^3+6x^2+x+5)\,(x^3+x^2+5x+1)\,(x^3+x^2+5x+3)$$
$$(x^3+x^2+5x+2)\,(x^3+4x^2+x+6)\,(x^3+3x^2+3x+5)\,(x^3+3x+2)$$
$$(x^3+5x+5)\,(x^3+6x+5)\,(x^3+4x^2+6x+5)\,(x^3+2x^2+6x+1)$$
$$(x^3+4x^2+3)\,(x^3+4x^2+1)\,(x^3+6x^2+4x+4)\,(x^3+4x^2+2x+2)\,(x^3+2)$$
$$(x^3+6x+2)\,(x^3+x+1)\,(x^3+6x^2+4)\,(x^3+x^2+1)\,(x+3)\,(x^3+6x^2+6)$$
$$(x^3+x+6)\,(x^3+2x+1)\,(x^3+2x^2+4x+2)\,(x^3+4x^2+3x+3)$$
$$(x^3+6x^2+3x+2)\,(x^3+3x^2+5x+2)\,(x^3+x^2+x+2)\,(x^3+6x^2+5x+3)$$
$$(x^3+6x^2+6x+2)\,(x^3+4x^2+4x+6)\,(x^3+6x^2+6x+4)\,(x^3+2x^2+x+6)$$
$$(x^3+x^2+x+5)\,(x^3+x^2+2x+6)\,(x^3+x^2+2x+4)\,(x^3+x^2+4x+3)\,x$$
$$(x^3+4x^2+5x+5)\,(x^3+4x^2+3x+1)\,(x^3+3x^2+x+4)\,(x^3+x^2+3x+5)$$
$$(x^3+5x^2+5x+6)\,(x^3+3x^2+3x+4)\,(x^3+5x^2+x+1)\,(x^3+3x+5)$$
$$(x^3+4x^2+5x+3)\,(x^3+5x^2+5x+2)\,(x^3+2x+6)\,(x^3+5)\,(x^3+3)$$
$$(x^3+3x^2+4)\,(x^3+4x^2+2x+5)\,(x^3+3x^2+2x+5)\,(x^3+2x^2+3x+5)$$
$$(x+6)\,(x^3+5x+2)\,(x^3+2x^2+6x+3)\,(x^3+3x^2+6)\,(x^3+3x^2+x+1)$$
$$(x^3+3x^2+6x+6)\,(x+1)\,(x^3+3x^2+4x+3)\,(x^3+4x^2+3x+4)$$
$$(x^3+2x^2+2x+3)\,(x^3+6x^2+5x+6)\,(x^3+3x^2+3x+3)\,(x^3+6x^2+3x+6)$$

$(x^3+x^2+5x+4)(x^3+5x^2+4x+2)(x^3+x^2+3x+1)(x^3+2x^2+6x+4)$
$(x^3+4x^2+x+3)(x^3+6x^2+x+2)(x^3+6x^2+2x+1)(x^3+6x^2+5x+5)$
$(x^3+3x^2+4x+1)(x^3+4x+6)(x^3+5x^2+2x+4)(x^3+5x^2+6x+5)$
$(x^3+2x^2+3x+3)(x^3+2x^2+4x+5)(x^3+2x^2+5x+5)(x^3+5x^2+6x+4)$
$(x^3+4x^2+4x+4)(x^3+5x^2+6x+6)(x^3+2x^2+2x+6)(x^3+5x^2+6)$
$(x+5)(x^3+3x^2+2x+2)(x+2)(x^3+5x^2+4)(x^3+x^2+3)(x+4)$
$(x^3+6x^2+4x+1)(x^3+x^2+6x+3)(x^3+4x+1)(x^3+2x^2+3)(x^3+2x^2+1)$
$(x^3+4x^2+6x+1)(x^3+3x^2+3x+6)(x^3+x^2+6x+5)(x^3+6x^2+2x+3)$
$(x^3+5x^2+x+3)(x^3+2x^2+5x+1)(x^3+6x^2+5x+4)(x^3+5x^2+4x+5)$
$(x^3+3x^2+5x+4)(x^3+2x^2+6x+2)(x^3+5x^2+3x+2)(x^3+5x^2+6x+3)$
$(x^3+5x^2+3x+4)(x^3+x^2+4x+6)(x^3+4x^2+3x+2)(x^3+3x^2+6x+2)$
$(x^3+4)(x^3+5x^2+2x+1)$

V .Fractions continues

V -1 Fractions continues simples

Les notions de fractions continues se trouvent dans plusieurs ouvrages de Théorie des Nombres. Cette notion continue provient de l'algorithme d'Euclide de la division de deux entiers u_0 et u_1 premiers entre eux, cet algorithme de division donne un nombre fini de relations

$u_0=u_1a_0+u_2$, $0 < u_2< u_1$ où a_0 est le quotient de la division et u_2 est le reste

$u_1=u_2\,a_1+u_3$, $0 < u_3< u_2$

$u_2=u_3a_2+u_4$, $0 < u_4< u_3$

……

$u_{n-1}=u_na_{n-1}+u_{n+1}$,avec $0< u_{n+1}< u_n$

Les divisions s'arrêtent lorsque le reste est nul.

$u_0= u_{n+1}a_n$

Ces $n+1$ relations se mettent sous la forme d'une fraction continue :

$$u_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + ... + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}...}}$$

L'entier a_0 est la partie entière $a_0 = [u_0/u_1]$ du nombre rationnel u_0/u_1 .

Définition :

Cette fraction à « étages » est une fraction continue simple. Le développement du nombre rationnel u_0/u_1 se met sous la forme symbolique :

$$\frac{u_0}{u_1} = \langle a_0, a_1, \ldots\ldots a_n \rangle + \frac{1}{\langle a_1, \ldots\ldots, a_n \rangle}$$

$$\frac{u_0}{u_1} = \langle a_0, a_1, \ldots \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots\ldots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

$$= < a_0, a_1, \ldots\ldots\ldots a_{n-1}, \frac{1}{\theta_n} >$$

Où $a_n = \frac{1}{\theta_n}$

Exemple :

Développer 9801/1820, 170/39 en fraction continue simple.

Nous effectuons les divisions euclidiennes successives suivons

L'algorithme précèdent:

de 9801 par 1820 .

Nous obtenons $9801 = 1820 \times 5 + 701$ donc $a_0 = 5$ …… (1)

$1820 = 701 \times 2 + 418$ donc $a_1 = 2$ ……(2)

$701 = 418 \times 1 + 283$ donc $a_2 = 1$

$418 = 283 \times 1 + 135$ donc $a_3 = 1$

$283 = 135 \times 2 + 13$ donc $a_4 = 2$

$135 = 13 \times 10 + 5$ donc $a_5 = 10$

$13 = 5 \times 2 + 3$ donc $a_6 = 2$

$5 = 3\times1 + 2$ donc $a_7 = 1$

$3 = 2\times1 + 1$ donc $a_8 = 1$

$1 = 1\times1$ donc $a_9 = 1$

Nous avons obtenu la fraction continue simple :

$$\frac{9801}{1820} = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}}}}}}$$

$$\frac{9801}{1820} = \langle 5, 2, 1, 1, 2, 10, 2, 1, 1, 1 \rangle$$

L'algorithme de la division euclidienne donne le développement en fraction continue du nombre rationnel 170/39 de façon suivante :

$$\frac{170}{39} = \langle 4, 2, 1, 3, 1, 2 \rangle$$

$$= 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}}}}$$

Proposition11

Toute fraction continue simple représente un nombre rationnel Réciproquement tout nombre rationnel peut être développé en fraction continue simple finie unique :

$$r = \frac{u_1}{u_2} = \langle a_0, a_1, \ldots . a_n \rangle = a_0 + \frac{1}{\langle a_1, \ldots \ldots . a_n \rangle}$$

□

V-2-Fractions continues infinies

Tout nombre rationnel donne une fraction continue simple finie. Il en résulte que les nombres irrationnels et les nombres réels donnent des fractions continues infinies.
Pour étudier ces fractions continues infinies nous associons à toute fraction continue $x = < a_0 , a_1,\ldots\ldots\ldots a_n\ldots\ldots >$ les 2 suites $\{h_n\}, \{k_n\}$ définies par récurrence :

$$h_{-2}=0 , h_{-1}=1 \text{ et } h_i=a_i h_{i-1}+h_{i-2} \text{ pour } i \geq 0 \quad (1)$$

$$k_{-2}=1 , k_{-1}=0 \text{ et } k_i=a_i k_{i-1}+k_{i-2} \text{ pour } i \geq 0 \quad (2)$$

Ces 2 récurrences (1) et (2) donnent une suite croissante $\{k_i\}$

$$1 = k_0<k_1 < k_2<\ldots\ldots\ldots< k_n < k_{n+1} <\ldots\ldots$$

Proposition12

Pour tout nombre réel x positif, les fractions continues $< a_0 , a_1,\ldots\ldots\ldots a_n , x >$ satisfait la relation :

$$< a_0 , a_1,\ldots\ldots\ldots a_{n-1}, x> = \frac{x\, h_{n-1}+h_{n-2}}{x\, k_{n-1}+ k_{n-2}}$$

□

Exemple :

Soit le nombre réel $x = \pi = 3{,}1415926535...$
Appliquons l'algorithme de la division euclidienne pour obtenir le développement en fraction continue :

$$\pi \approx 3 + \cfrac{1}{7 + \cfrac{1}{15{,}996\ldots}} = 3 + \cfrac{1}{7 + \cfrac{1}{15 + 0{,}996}}$$

$$= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + 0{,}00341\ldots}}}$$

Définition :

Dans la fraction continue $< a_0 , a_1, \ldots\ldots\ldots a_{n-1}, x> = \dfrac{x\, h_{n-1}+h_{n-2}}{x\, k_{n-1}+ k_{n-2}}$

le nombre rationnel $r_n=\frac{h_n}{k_n}$ *est le* n^{eme} *convergent des suites* $\{h_n\}, \{k_n\}$

Soit une $r_n = < a_0 , a_1, \ldots\ldots\ldots a_n>$, *alors pour tout entier* $n\geq 0$

$r_n= \frac{h_n}{k_n}$

Proposition13

Les suites $\{h_n\}$ et $\{k_n\}$ ci-dessus et les convergents $r_n= \frac{h_n}{k_n}$

satisfont les relations :

1. $h_ik_{i-1} - h_{i-1}k_i = (-1)^{i-1}$ et $r_i-r_{i-1} = \frac{(-1)^{i-1}}{k_ik_{i-1}}$ pour $i\geq 1$
2. $h_ik_{i-2} - h_{i-2}k_i= (-1)^i a_i$ et $r_i-r_{i-2} = \frac{(-1)^i a_i}{k_ik_{i-2}}$ pour $i\geq 1$
3. pgcd $(h_i, k_i)=1$ et la fraction $\frac{h_i}{k_i}$ est réduite

□

Les convergents r_n forment une suite adjacente comme le montre la.

Proposition14

Les convergents $r_n = \frac{h_n}{k_n}$ forment une suite « adjacente » :

Les convergents r_{2n} d'indices pairs forment une suite croissante, les r_{2n+1} d'indices impairs forment une suite décroissante, tout convergent r_{2n} est inférieur à un convergent r_{2p+1}.

$r_0 < r_2 < r_4 < \ldots\ldots\ldots\ldots < r_{2n} \ldots\ldots\ldots < r_{2i+1} < \ldots\ldots\ldots < r_7 < r_5 < r_3 < r_1$

□

Définition :

Une fraction continue infinie est périodique lorsqu'elle est de la forme :

$<a_0,a_1\ldots\ldots,a_t,a_{t+1}\ , \ldots a_{t+s},\ a_t,\ldots,a_{t+s},\ a_t,\ldots,a_{t+s},\ a_t,\ldots> = <a_0\ ,\ a_1,\ .,\overline{a_t,a_{t+1}\ ,\ \ldots a_{t+s}}>$

de période $\overline{a_t\ ,\ a_{t+1},\ldots a_{t+s}}$

où $<a_0\ ,a_1\ldots\ldots,a_t,\ a_1\ldots\ldots,a_t,\ldots\ldots> = <a_0\ ,\overline{a_1\ldots\ldots,a_t}>$

de période $\overline{a_1\ldots\ldots,a_t}$

Exemple : les fractions continues, infinies, périodiques

Evaluer $< 1,1,1,\ldots\ldots>$, $< 1,2,1,2\ldots\ldots >$

1. $\theta_1 = < 1,1,1,\ldots.> = < \overline{1}\ ,\ 1 >$, est une fraction continue,infinie de période $\overline{1}$

$$\theta_1 = 1 + \frac{1}{1 + \frac{1}{1\ \ldots\ldots\ + \frac{1}{1+\frac{1}{1}}}} = 1 + \frac{1}{\theta_1} \qquad (1)$$

la relation (1) implique l'équation quadratique $\theta_1^2 - \theta_1 - 1 = 0$

Cette équation admet 2 racines (seule la racine convient)

Donc : $\theta_1 = \frac{1+\sqrt{5}}{2}$

2. $\theta_2 = < 1,2,1,2\ldots\ldots > = < \overline{1,\ 2,1}\ >$ est une fraction continue périodiques, infinie , de période $\overline{2,1}$

$$\theta_2 = 1+\frac{1}{2+\frac{1}{\theta_2}} = 1+\frac{\theta_2}{2\theta_2+1} \quad (1)$$

Cette relation entraîne l'équation quadratique suivante

$$\theta_2 = \frac{3\theta_2+1}{2\theta_2+1} \quad (2)$$

Donc : $2\theta_2^2 - 2\theta_2 - 1 = 0$ (3)

(3) admet 2 solutions mais c'est la racine positive qui convient

$$\theta_2 = \frac{1+\sqrt{3}}{2}$$

V 3 Fractions continues périodiques

Dans les fractions continues, il y a 2 cas spécifiques :

Lorsque la partie $< a_0 , a_1,\ldots a_n>$ est périodique à partir de $a_1$et lorsque une partie $< a_0 , a_1,\ldots a_n>$ est périodique à partir d'un rang $r > 1$

Exemple1:

Soit la fraction continue périodique $\theta = < \overline{2, 3} >$

Alors θ satisfait la relation :

$$\theta = 2 + \frac{1}{3 + \frac{1}{\theta}}$$

Cette relation donne l'équation quadratique

$3\theta^2 - 6\theta - 2 = 0$ cette équation admet 2 solutions

la solution convenable est positive, donc

$$\theta = \frac{3 + \sqrt{15}}{3} \quad \text{où } a_0 = [\theta] = 2 \ ; \ a_1 = 3$$

Exemple2 :

Le symbole $< 7, \overline{2, 3} >$ désigne la fraction continue simple infinie périodique de période $\overline{2,3}$

Posons $\theta = < 7, \overline{2, 3} >$ (1)

Ce nombre θ satisfait la relation :

$$\theta = 7 + \frac{1}{\langle \overline{2,3} \rangle} \qquad (2)$$

la fraction $< \overline{2, 3} >$ périodique est égale à

$$< \overline{2, 3} > = \frac{3+\sqrt{15}}{3} \qquad (3)$$

(2) et (3) impliquent

$$\theta = 7 + \frac{3}{3+\sqrt{15}} = \frac{11+\sqrt{15}}{2}$$

Proposition16

Toute fraction continue simple périodique est un nombre irrationnel quadratique $a+b\sqrt{d}$

Réciproquement tout nombre irrationnel quadratique $\theta = a + b\sqrt{d}$ admet un développement en fraction continue simple périodique.

□

Définition :

Une fraction continue simple purement périodique est une fraction de période $<\overline{a_0, a_1, \ldots . a_n}>$

Proposition17

Le développement d'un nombre irrationnel quadratique est une fraction continue simple purement périodique si et seulement si $\theta > 1$ et son conjugué θ' satisfait l'inégalité $-1 < \theta' < 0$

□

Exemple

Le nombre irrationnel quadratique $\theta=3+\sqrt{10}$ satisfait la condition $\theta>1$. Son conjugué $\theta`=3-\sqrt{10}$ satisfait la condition $-1<\theta`<0$

La proposition 17 implique un développement de θ en fraction continue simple purement périodique.

$$\theta = < \overline{a_0, a_1, \ldots\ldots a_n} > \text{ avec } a_0 = a_1 = \ldots = a_n = 6$$

Donc $\theta = < \overline{6} >$

Proposition18

Tout nombre irrationnel quadratique $\sqrt{d}$ admet un développement en fraction continue simple périodique de période r de la forme :

$$\sqrt{d} = < a_0, a_1, \ldots\ldots a_{r-1}, 2a_0 >$$

□

Exemple : développer $\sqrt{85}$ en fraction continue

$\sqrt{85} = \langle a_0, a_1, \ldots. \rangle$. Appliquons l'algorithme de calcul

Partie entière $a_0 = [\sqrt{85}] = 9$

Calcul de a_1 avec $\sqrt{85} = 9 + (\sqrt{85} - 9) = 9 + \dfrac{1}{\dfrac{1}{\sqrt{85}-9}}$

et $\dfrac{1}{\sqrt{85}-9} = a_1 + \dfrac{1}{\theta_1}$

$$= \frac{\sqrt{85}+9}{(\sqrt{85}-9)(\sqrt{85}+9)} = \frac{\sqrt{85}+9}{4} = 4 + \frac{\sqrt{85}-7}{4} \text{ donc } a_1 = 4$$

Calcul de a_2 avec $\dfrac{4}{\sqrt{85}-7} = \dfrac{4(\sqrt{85}+7)}{36} = \dfrac{2(\sqrt{85}+7)}{18}$

$$= 1 + \frac{2(\sqrt{85}-2)}{18} \text{ donc } a_2 = 1$$

Calcul de a_3 avec $\frac{9}{\sqrt{85}-2} = \frac{\sqrt{85}+2}{9}$

Mais $\frac{\sqrt{85}+2}{9} = 1 + \frac{\sqrt{89}-7}{9}$ donc $a_3 = 1$

Calcul de a_4 avec $\frac{9}{\sqrt{85}-7} = \frac{\sqrt{85}+7}{4}$

Mais $= 4 + \frac{\sqrt{85}-9}{4}$ donc $a_4 = 4$

Calcul de a_5 avec $\frac{4}{\sqrt{85}-9} = \sqrt{85}+9$

$= 18 + \frac{1}{\frac{1}{\sqrt{85}-9}}$ donc $a_5 = 18$

Calcul de a_6 avec $\frac{1}{\sqrt{85}-9} = \frac{\sqrt{85}+9}{4}$

$= 4 + \frac{\sqrt{85}-7}{4}$ donc $a_6 = 4$

Calcul de a_7 avec $\frac{4}{\sqrt{85}-7} = \frac{\sqrt{85}+7}{9} = 1 + \frac{\sqrt{85}-2}{9}$

$= 1 + \frac{1}{\frac{9}{\sqrt{85}-2}}$ donc $a_7 = 1$

Calcul de a_8 avec $\frac{9}{\sqrt{85}-2} = 1 + \frac{\sqrt{85}-7}{9}$ donc $a_8 = 1$

Calcul de a_9 avec $\frac{9}{\sqrt{85}-7} = \frac{\sqrt{85}+7}{4}$

$$= 4 + \frac{1}{\frac{4}{\sqrt{85}-9}} \quad \text{donc } a_9 = 4$$

Calcul de a_{10} avec $\frac{4}{\sqrt{85}-9} = \sqrt{85}+9$

$$= 18 + (\sqrt{85}-9) \text{ donc } a_{10} = 18$$

Calcul de a_{11} avec $\frac{1}{\sqrt{85}-9} = \frac{\sqrt{85}+9}{4}$

$$= 4 + \frac{\sqrt{85}-7}{4}$$

$$= 4 + \frac{1}{\frac{4}{\sqrt{85}-7}} \quad \text{donc } a_{11} = 4$$

Calcul de a_{12} avec $\frac{4}{\sqrt{85}-7} = \frac{\sqrt{85}+7}{9}$

$$= 1 + \frac{\sqrt{85}-2}{9} \text{ donc } a_{12} = 1$$

Le nombre $\sqrt{85}$ admet un développement en fraction continue simple périodique de période $r = 5$ de la forme :

$$\sqrt{85} = \left\langle 9\ ,4\ ,\overline{1\ ,1\ ,4\ ,18\ ,4}\right\rangle$$

V -4 : Equation diophantienne de Pell. Fermat $x^2-dy^2 = N$ où $d \rangle 1$ et sans facteur carre

La résolution de ces équations utilisent le développement du nombre $\theta = \sqrt{d}$ irrationnel quadratique en fraction continue simple périodique.
Soit r la longueur de la période de la fraction continue

$$\sqrt{d} = < a_0, a_1, \ldots \overline{a_t, a_{t+1}, a_{t+2,\ldots\ldots} a_{t+r}} >$$

Soit les convergents $r_n = \frac{h_n}{k_n}$ associés.

Proposition19

Soit une équations diophantienne de Pell Fermat $x^2 - dy^2 = N$ où $N = \pm 1$ et d sans facteur carré la fraction continue $\sqrt{d}$ admet une période r. soit h_n et k_n les congruentes associées.

1) lorsque r est pair l'équation $x^2 - dy^2 = -1$ n'admet pas de solution.

L'équation $x^2 - dy^2 = +1$ admet une infinité de solutions positives de $x = h_{nr-1}$, $y = k_{nr-1}$ pour $n = 1,2,3\ldots.$

2) lorsque r est impair, l'équation $x^2 - dy^2 = -1$ admet infinité de solution

$x = h_{nr-1}$, $y = k_{nr-1}$ pour les entiers impairs n = 1,3,5……(1)

L'équation $x^2 - dy^2 = +1$ admet une infinité de solutions des formules (1) pour les entiers pairs n= 2 , 4 ,…

□

Corollaire :

Soit l'équation de Pell $x^2 - dy^2 = 1$ où d est un entier naturel sans facteur carré. Soit (x_1, y_1) la plus petite solution positive de cette équation. Alors les autres solutions (x_n , y_n) sont établies par la formule

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \text{ pour } n = 1,2,3,\ldots\ldots$$

□

Exemples

Les calculs effectifs concernant les développements en fraction continue

sont exécutés par des logiciels appropriés, que nous utiliserons ici .

1. Résoudre l'équation de Pell Fermat $x^2-34y^2 = 1$

Le développement en fraction continue de $\sqrt{34}$ est

$$\sqrt{34} = <5, \overline{1, 4, 1,10}>$$

Il y a une période unique ce résultat implique que la période est égale à $r = 4$. La proposition 19 et $r = 4$ pair, implique que l'équation $x^2 - 34y^2 = -1$ n'admet pas de solution

2. Résoudre l'équation de Pell Fermat

$x^2 - 31y^2 = 1$ (1)

Pour appliquer la proposition 19 qui donne les solutions, il faut développer $\sqrt{31}$ en fraction continue le logiciel ; donne la fraction continue

$$\sqrt{31} = \langle 5, \overline{1,1,3,5,3,1,1,10} \rangle \qquad (2)$$

donc la plus petite période est $m = 8$ le les solutions positives sont de la forme : $x_n = h_{nr-1}$, $y_n = k_{nr-1}$ (3)

pour les entiers naturels $n = 1,2,3,4,5,\ldots\ldots$

Les nombres h_t et k_t sont détermines par 2 suites récurrentes

Corollaire implique la relation

$$x_n + y_n \sqrt{31} = (x_1 + y_1 \sqrt{31})^n \qquad (4)$$

Où $x_1 = h_{r-1} = h_7$ et $y_1 = k_{r-1} = k_7$ (5)

Ces suites récurrentes sont, par définition

$h_{-2} = 0$, $h_{-1} = 1$ et $h_t = a_t h_{t-1} + h_{t-2}$ pour $t \geq 0$

$k_{-2} = 1$, $k_{-1} = 0$ et $k_t = a_t k_{t-1} + k_{t-2}$ (6)

Les nombres a_t sont déterminés par (2)

$a_1 = a_2 = 1$, $a_3 = 3$, $a_4 = 5$, $a_5 = 3$, $a_6 = 1 = a_7$, $a_8 = 10$

3. Résoudre l'équation diophantienne Pell Fermat

$$x^2-53y^2 = -1 \qquad (1)$$

« **Maple** » donne le développement de $\sqrt{53}$ en fraction continue

$$\sqrt{53} = \langle 7, \overline{3,1,1,3,14} \rangle \qquad (2)$$

Il en résulte que la période de cette fraction est égale à

$$m = 5 \qquad (3)$$

la proposition 19 implique une infinité de solutions

$$x_n + y_n \sqrt{53} = (x_1 + y_1 \sqrt{53})^n \qquad (4)$$

Où $x_1 = h_4$ et $y_1 = k_{m-1} = k_4$ et $n = 1,3,5,7,\ldots$ (5)

Le logiciel donne les valeurs $h_4 = 182$, $y_4 = 25$ (6)

Il en résulte les solutions

$$x_n + y_n \sqrt{53} = (182 + 25 \sqrt{53})^n \text{ pour } n = 1,3,5,7,\ldots (7)$$

Conclusion :

Dans ce mémoire, nous avons étudié les résultats fondamentaux concernant les corps finis: structure algébrique théorème de l'élément primitif. Nous nous intéressons ensuite aux polynômes irréductibles sur tels corps et décomposition de $x^m - x$ avec $m = q^n$ à l'aide d'un logiciel « **MAPLE** » puis les fractions continues de différents types en définitive l'équation de Pell Fermat avec des exemples résolus à l'aide d'un logiciel « MAPLE » . L'algorithme des fractions continues permet de calculer les meilleures approximations rationnelles d'un réel telles que le dénominateur ne soit pas trop grand .Si le réel est un rationnel, l'algorithme s'arrête et il a la même complexité que l'algorithme d'Euclide.

Références

[1].DICKSON : (introduction to the theory of numbres

Chicago universite 1929

[2].GROSSWALD Emil: topics from the theory of Numbers (New York), Macmillan(1966)

[3].I.NIVEN Irrational Numbers, Carus Monograph 11,

Newyork,John Wiley (1956).

[4].J.E. SHOCKLEY: Introduction to Number Theory ,Holt Rinehart and winston Inc 383 Madison Avenue , NY(1967).

[5].NIVEN et ZUCKERMAN (introduction to the theory of numbres third edition john wiley now york 1972

[6]. R.Crandall and C. Pomerance prime numbers a computational perspective springer (2002) New york .

[7]. S. Lang , Algebra , Addison –Wesley publishing company,Inc, Reading Massachusets (1965) New york .