N° d'ordre : 18/2004 –M/MT

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Université des sciences et de la technologie Houari Boumedienne

Faculté de Mathématiques

Mémoire présenté

Pour l'obtention du diplôme de Magister

EN MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : MOUHOUB FERIEL

Thème

# THEORIE DES COURBES HYPERELLIPTIQUES

Soutenu le : 21 septembre 20004 , Devant le jury suivant :

| | | |
|---|---|---|
| M . ZITOUNI | Professeur (USTHB) | Président |
| K . BETINA | Professeur (USTHB) | Directeur de thèse |
| A . AROUCHE | Docteur d'état (USTHB) | Examinateur |
| A . IDRISS-BEY | Chargé de cours (USTHB) | Examinateur |

## *Remerciements*

*Je tiens à exprimer ma gratitude à monsieur* ***BETINA*** *mon encadreur pour m'avoir proposé ce travail,pour son soutien et ses conseils.*

*Je tiens à remercier également monsieur* ***ZITOUNI*** *qui me fait l'honneur de présider le jury .*

*Ainsi qu'à messieurs* ***IDRISS-BEY*** *et* ***AROUCHE*** *qui ont voulu faire partie du jury.*

## *Sommaire*

# *Introduction*

Les courbes hyperelliptiques sont une classe des courbes algébriques, Leurs utilisation à la cryptographie à clé publique a fait de leur étude une nécessité en algèbre et théorie des nombres .

Dans le premier chapitre de ce papier , nous traiterons les définitions de : courbes hyperelliptiques , point opposé , spécial , ordinaire , et leurs propriétés ; de plus nous étudierons les fonctions polynomiales, rationnelles ainsi que les propriétés des zéros et pôles de ces dernières .

Comme la notion des diviseurs et de la jacobienne d'une courbe apparaît nécessaire dans la théorie des courbes hyperelliptiques , le deuxième chapitre sera consacré à leur traitement .

Enfin dans le troisième chapitre , nous traiterons l'implémentation de ces courbes dans la cryptographie .

# CHAPITRE I : Définitions et propriétés de base

## I.1 /Courbes hypereliptiques :

Soit K un corps de caractéristique p, et $K^{alg}$ sa clôture algébrique .

**Définition 1 :**

une courbe hyperelliptique C sur K de genre g ($g \geq 1$) est l'ensemble des points $(u , v) \in (K^{alg})^2$ qui vérifient une équation de la forme :

$$C : v^2 + h(u)\, v = f(u) \quad \ldots\ldots\ldots\ldots(1)$$

Avec :

*$h(u) \in K[u]$ : polynôme de degré au plus g.

*$f(u) \in K[u]$ : polynôme de degré 2g+1.

* Il n'existe pas de solutions $(u ,v) \in K^{alg} \times K^{alg}$ qui vérifie simultanément l'équation (1) ainsi que les équations aux dérivées partielles : $2v + h(u) = 0$ ……..(2)

$$h'(u)\, v - f'(u) = 0 \quad \ldots\ldots.(3)$$

Un point singulier sur C est une solution $(u , v) \in K^{alg} \times K^{alg}$ qui satisfait les équations (1) , (2) et (3) .

Remarque :

la définition précédente indique ainsi qu'une courbe hyperelliptique n'a pas de points singuliers .

## I-2/ Propriétés des courbes hyperelliptiques :

**Lemme 2 :**

Soit C une courbe hyperelliptique sur K définie par l'équation (1)

← Si h(u) = 0 ,alors la caractéristique de K est différente de 2

↑ Si $p \neq 2$ , alors le changement de variables $(u , v) \rightarrow (u , v- (h(u) /2)$

transforme l'équation (1) en $v^2 = f(u)$ où $d^\circ f = 2g+1$ .

→Soit C une courbe d'équation (1) avec h(u) = 0 et $p \neq 2$ ; alors C est une courbe hyperelliptique si et seulement si $f(u)$ n'a pas de racine multiple .

Preuve :

Supposons que h(u) = 0 et p = 2 , donc les équations aux dérivées partielles (2) et (3) se réduisent à : $f'(u) = 0$ .

Soit $x \in K^{alg}$ une racine de l'équation $f'(u) = 0$ et $y \in K^{alg}$ une racine de l'équation $v^2 = f(x)$, ceci implique que le point (x , y) est un point singulier de la courbe C (contradiction) .

↑ Soit la courbe C d'équation : $v^2 + h(u)\, v = f(u) \in K[u, v]$.

Nous effectuons le changement de variables : $(u , v) \rightarrow (u , v- (h(u) /2)$

Nous obtenons l'équation suivante :

$$[v – (h(u) /2)]^2 + h(u) [v – (h(u) /2)] = f(u)$$

i.e.

$$v^2 - ¼\ h^2(u) = f\ (u)$$

Finalement , nous obtenons l'équation de la courbe hyperelliptique C :

$v^2 = f(u) + ¼\ h^2(u)$ , avec : $d°[f(u) + ¼\ h^2(u)] = 2g+1$.

$\rightarrow$ Supposons que C possède un point singulier (x ,y ) , ceci est équivalent à dire que le point (x , y) satisfait les équations :

$v^2 = f(u)$ , $2v = 0$ et $f'(u) = 0$ i.e. $2y = 0$ et $f'(x) = 0$ .

donc : $f(x) = 0$ et $f'(x) = 0$ d'où x est une racine multiple de $f$ □

**Définition 3 :**

Soit L une extension du corps K . L'ensemble des points L- rationnels sur C , noté C (L) , est l'ensemble de tous les points $P = (x , y) \in L \times L$ qui satisfont l'équation (1) de la courbe C union le point spécial à l'infini , noté $\infty$ .

$C(L) = \{ (x , y) \in L \times L ; y^2 + h(u)\, y - f(x) = 0 \} \cup \{\infty\}$ .

L'ensemble des points $C(K^{alg})$ est la courbe C .

Les points de C autres que $\infty$ sont les points finis de C.

**<u>I-3 /Point opposé , point spécial , point ordinaire :</u>**

**Définition 4 :**

Soit P = (x , y) un point fini sur la courbe C , l'opposé de P est le point :

$\overline{P} = ( x , - y - h(x) )$ . [l'opposé de $\infty$ est $\infty$ lui même : $\overline{\infty} = \infty$]

* Si le point P satisfait $\overline{P} = P$ , alors le point P est spécial .

*Autrement ( i.e. si $\overline{P} \neq P$ ) le point est ordinaire .

## I-4/ Fonctions polynomiales :

**Définition 5 :**

L'anneau des coordonnées de la courbe C sur le corps K , noté K[C] , est l'anneau quotient :

$$K[C] = K[ u , v] /( v^2 + h(u) v - f (u) )$$

où ( $v^2 + h(u) v - f (u)$ ) est l'idéal dans K[ u , v] engendré par le polynôme $v^2 + h(u) v - f (u)$ .

L'anneau des coordonnées de C sur $K^{alg}$ est défini par :

$$K^{alg} [C] = K^{alg} [ u , v] /( v^2 + h(u) v - f (u) ).$$

Un élément de $K^{alg}$ [C] est appelé fonction polynomiale sur C .

**Lemme 6 :**

Le polynôme $r( u , v) = v^2 + h(u) v - f (u)$ est irréductible sur $K^{alg}$ , et alors $K^{alg}$[C] est un domaine intégrale .

Preuve :

Supposons r(u , v) est réductible sur $K^{alg}$ :

r(u , v) = (v – a(u)) (v – b(u)) avec a(u) et b(u) $\in K^{alg}$ [u]

$$= v^2 – (a(u) + b(u)) v + a(u) b(u)$$

l'identification implique les égalités : a(u) + b(u) = - h(u)

$$a(u) \times b(u) = -f(u)$$

les égalités ci- dessus impliquent que

$\deg(a+b) = \deg(h) \leq g$

$\deg(a \times b) = \deg(f) = 2g+1$ (contradiction).

Remplaçons chaque occurrence de $v^2$ par $f(u) - h(u)\,v$ ,pour obtenir par la suite , pour chaque fonction polynomiale $G(u , v)$ de $K^{alg}[u , v]$ la représentation suivante : $G(u , v) = a(u) - b(u)\,v$ / $a(u) , b(u) \in K^{alg}[u]$

**Définition 7 :**

Soit $G(u , v) = a(u) - b(u)\,v$ une fonction polynomiale sur $K^{alg}$

*Le conjugué de $G(u , v)$ est défini par la fonction polynomiale :

$$\overline{G}(u , v) = a(u) + b(u)\,( h(u) + v)$$

*La norme de G est la fonction polynomiale définie par :

$$N(G) = G \times \overline{G}$$

**Lemme 8 :**

Soit G , H deux fonctions polynomiales dans $K^{alg}$ [C] :

← N(G) est un polynôme de l'anneau $K^{alg}$ [u] .

↑ La norme du polynôme conjugué $N(\overline{G})$ de G est égale à la norme N(G) du polynôme G : $N(\overline{G}) = N(G)$ .

→La norme $N(G \times H)$ du produit des deux polynômes G et H est égale au produit $N(G) \times N(H)$ des normes de G et H : $N(G \times H) = N(G) \times N(H)$.

Preuve :

notons les polynômes G et H par : $G = a - b\,v$ et $H = c - d\,v$

← Par définition la norme N(G) de G est égale au produit $G \times \overline{G}$ :

$$N(G) = G \times \overline{G}$$

$$= (a - b\,v) \times (a + b(h + v))$$

$$= a^2 + a\,b\,h - b^2\,v\,h - b^2 v^2$$

L'équation de la courbe hyperelliptique C implique :

$$N(G) = a^2 + a\,b\,h - b^2\,v\,h - b^2(-hv + f)$$

$$= a^2 + a\,b\,h - b^2 f$$

les fonctions a, b, h et $f$ appartiennent à l'anneau $K^{alg}[u]$, ceci implique que la norme N(G) de G est un élément de l'anneau $K^{alg}[u]$ .

↑ Par définition le conjugué $\overline{G}$ de G est égal à :

$$\overline{G} = a + b(h + v)$$

$$= a + b\,h - (-b)\,v$$

donc le conjugué $\overline{\overline{G}}$ de G est égale à :

$$\overline{\overline{G}} = a + b\,h + (-b)\,(h + v)$$

$$= a - b\,v$$

$$= G$$

Le résultat ci-dessus implique :

$$N(\overline{G}) = \overline{G} \times \overline{\overline{G}} = \overline{G} \times G = N(G) .$$

$\rightarrow$Calculons le produit $G \times H$ :

$G \times H = (a - bv)(c - d v)$

$= (ac + bdf) - (ad + bc + bdh) v$

Il reste à montrer que $\overline{GH} = \overline{G} \times \overline{H}$ ; en effet :

$\overline{GH} = (ac + bdf) + (ad + bc + bdh)(h + v)$

$= ac + bc(h + v) + ad(h + v) + bd(h^2 + f + hv)$ ♦

l'équation $f = v^2 + h v$ et ♦impliquent :

$\overline{GH} = (a + b(h + v)) \times (c + d(h + v))$

$= \overline{G} \times \overline{H}$

Alors : $N(G \times H) = G H \overline{GH}$

$= G \overline{G} H \overline{H} = N(G) N(H)$ □

**Définition 9 :**

Soit $G(u , v) = a(u) - b(u) v$ une fonction polynomiale non nulle dans $K^{alg}[C]$ , le degré de G est défini par :

$$\deg(G) = \max [2\deg(a) , 2g+1 + 2\deg(b)].$$

**Lemme 10 :**

Soit G et H deux fonctions polynomiales de $K^{alg}[C]$

$\leftarrow$ Le degré de G est égal au degré de la norme de G :

$\deg(G) = \deg(N(G))$

↑le degré du produit G×H est égal à la somme des degré de G et H :

$\deg(G\times H) = \deg(G) + \deg(H)$

→ Le degré de G est égal au degré de son polynôme conjugué $\overline{G}$ :

$\deg(G) = \deg(\overline{G})$

Preuve :
notons que : $G(u , v) = a(u) - b(u)\, v$

$$N(G) = a^2 + abh - b^2 f$$

et $d_1 = \deg(a)$ , $d_2 = \deg(b)$

←Considérons les deux cas suivants :

1er cas : $2d_1 > 2g + 1 + 2d_2$

cela implique : $2d_1 \geq 2g + 2 + 2d_2$ , d'où $d_1 \geq g + 1 + d_2$

et par suite : $\deg(a^2) = 2d_1 \geq g + 1 + d_2 + d_1$

or $g + 1 + d_2 + d_1 > d_1 + d_2 + g$

donc $\deg(a^2) > \deg(abh)$ …….(1)

2em cas : $2d_1 < 2g + 1 + 2d_2$

cela implique $2d_1 \leq 2g + 2d_2 \Rightarrow d_1 < g + d_2$ ♦

L'inégalité $\deg(h) \leq g$ implique : $\deg(abh) \leq d_1 + d_2 + g$ ♦♦

♦et♦♦impliquent : $\deg(abh) \leq 2g + 2d_2$

$$< 2g + 2d_2 + 1$$

ie : $\deg(abh) < \deg(b^2 f)$ ……..(2)

Les inégalités (1) et (2) impliquent :

$\deg(N(G)) = \max(\deg(a^2), \deg(b^2 f))$

$= \max(2d_1, 2g + 1 + 2d_2)$

$= \deg(G)$ .

↑ Le résultat précédent implique l'égalité : $G \times H = N(G \times H)$

donc : $\deg(G \times H) = \deg(N(G \times H))$

$= \deg(N(G)) + \deg(N(H))$

$= \deg(G) + \deg(H)$

$\rightarrow \deg(G) = \deg(N(G))$

$= \deg(N(\overline{G}))$ car $N(G) = N(\overline{G})$

$= \deg(\overline{G})$ car $\deg(N(G)) = \deg(G)$ .□

**I-5 /Fonctions rationnelles :**

**Définition 10 :**

*Le corps des fonctions K(C ) de C sur K est le corps des fractions de K[C] . Par ailleurs le corps des fonctions $K^{alg}$ (C ) de C sur $K^{alg}$ est le corps des fractions de $K^{alg}$ [C] .

Les éléments de $K^{alg}$ (C ) sont appelés fonctions rationnelles sur C.

*Soit R une fonction rationnelle de $K^{alg}$ (C ) , et P un point fini de la courbe C ; R est dite définie en P s'il existe des fonctions polynomiales G et H de $K^{alg}$ [C] tels que : $R = G/H$ et $H(P) \neq 0$

Les fonctions polynomiales de $K^{alg}$ [C] ont des valeurs en tout point fini de C , donc une fonction rationnelle sur C peut ne pas avoir de valeurs en tout point fini et peut avoir une valeur en ∞ .

*Si R est définie en P ,la valeur de R en P est définie par :

R(P) = G(P)/H(P) .

**Définition 11 :** (valeur d'une fonction rationnelle au point ∞)

Soit R = G/H une fonction rationnelle de $K^{alg}$(C) :

← Si deg(G) < deg (H) , alors R(∞) = 0 .

↑ Si deg (G) > deg (H) , alors R est non définie , et on écrit R(P) = ∞

→ Si deg (G) = deg (H) ,alors R(∞) est définie comme le rapport des coefficients principaux .

**I-6/ Zéros et Pôles :**

**Définition 12 :**

Soit R une fonction rationnelle non nulle et P un point fini de la courbe hyperelliptique C :

*R possède un zéro en P si R(P) = 0 .

*R possède un pôle en P si R est non définie en P (i.e. R(P) = ∞ ) .

**Lemme 13 :**

Soit G une fonction polynomiale et P un point de C : si la valeur G(P) est nulle (G(P) = 0) ,alors la valeur du conjugué $\overline{G}$ de G en $\overline{P}$ est

nulle :($G(P) = 0 \Rightarrow \overline{G}(\overline{P}) = 0$)

Preuve :

notons $G(u , v) = a(u) – b(u)\, v$ et $P = (x , y)$

Les définitions de l'opposé $\overline{P}$ de P et du conjugué $\overline{G}$ de G nous permettent de calculer la valeur $\overline{G}(\overline{P})$ :

$\overline{G}(\overline{P}) = a(x) + b(x) (h(x) – y – h(x) )$

$= G (P) = 0$ □

**Lemme 14 :**

Soit $P= (x , y)$ un point de C et $G(u , v) = a(u) – b(u)\, v$ une fonction polynomiale non nulle de C :

Supposons que G admet un zéro en P ,et que x n'est pas une racine commune de a(u) et b(u) ,alors :

$\overline{G}(P) = 0$ si et seulement si P est un point spécial .

Preuve :

Condition suffisante : supposons que P est un point spécial

i.e. $\overline{P} = P$

L'hypothèse $G(P) = 0$ implique $\overline{G}(\overline{P}) = 0$ (lemme 13)

Donc : $\overline{G}(P) = 0$ ( car $\overline{P} = P$) .

Condition nécessaire :

Supposons que P est un point ordinaire i.e. $y \neq -y - h(x)$

$\overline{G}(P) = 0$ implique $a(x) + b(x)\,(h(x) + y) = 0$…..(1)

$G(P) = 0$ implique $a(x) - b(x)\,y = 0$ ……(2)

Nous soustrayons (1) de (2) , nous obtenons :

$-b(x)\,(h(x) + y) - b(x)\,y = 0 \Rightarrow -h(x)\,b(x) = 0$

or $h(x) \neq 0$ donc $b(x) = 0$ . ……(3)

(2) et (3) impliquent $a(x) = 0$

i.e. x est une racine commune de a(u) et b(u) ( contradiction).

**Lemme 15 :**

Soit P =(x , y) un point ordinaire de C et G = a – bv une fonction polynomiale non nulle .Si G(P) = 0 et x n'est pas racine commune de a(u) et b(u) alors G peut s'écrire sous la forme :

$G = (u - x)^s S$ , où s est la plus grande puissance de (u – x) qui divise N(G),et S est une fonction rationnelle telle que $S(P) \neq 0, \infty$

Preuve :

écrivons la fonction G sous la forme :

$G = G \times (\overline{G}/\overline{G}) = N(G)/\overline{G} = (a^2 + abh - b^2 f) / (a + b(h + v))$

Soit $N(G) = (u - x)^s \times d(u)$ où s est la plus grande puissance de (u – x) qui divise N(G), et $d(u) \in K^{alg}[u]^*$ telle que $d(x) \neq 0$ .

Le lemme 14 implique $\overline{G}(P) \neq 0$, alors $G(u , v) = (u - x)^s \times d(u) / \overline{G}$ ,

si on pose S = d(u) / $\overline{G}$ alors : S(P) $\neq 0$ (car d(x) $\neq 0$ )

et S(P) $\neq \infty$ ( car $\overline{G}$(P) $\neq 0$) .

**Lemme 16 :**

Soit P =(x , y) un point spécial de C ;alors (u – x) peut s'écrire sous la forme u – x =$(v - y)^2$ S(u , v) où S(u,v)$\in K^{alg}$ (C ) ; S(P) $\neq 0,\infty$ .

Preuve :

posons H(u , v) = $(v - y)^2$ et S(u , v) = (u – x) /H(u , v) ,

donc (u – x) = H × S ; il s'agit donc de montrer que S(u , v) $\neq 0 , \infty$ .

P est un point non singulier donc ses coordonnés vérifient :

$\leftarrow$ h'(x) y - $f$'(x) $\neq 0$

$\uparrow$ $f$'(x) = $y^2$ + h(x) y

l'hypothèse P un point spécial implique l'égalité y = - y – h(x),donc

$f$(x) = $y^2$+ (-2y) y = - $y^2$ ,

alors H(u , v) = $(v – y)^2$ = $v^2$ - 2v + $y^2$ ,

or $v^2$= $f$(u) –h(u) v donc H(u , v) = $f$(u) – h(u) v – 2yv + $y^2$ ♦

d'où 1 / S(u,v) = ($f$(u) + $y^2$ / (u-x)) – v(h(u) + 2y /(u-x)) ♦♦

Soit s(u) = H(u , v) ; la formule ♦implique s(x) = 0

D'autre part la dérivée s'(u) de s est égale à s'(u) = $f$'(u)-h'(u) y

La formule $\leftarrow$ implique s'(x) $\neq 0$ ; ainsi (u –x) divise s(u) et $(u -x)^2$ ne divise pas s(u), par suite le membre de droite de ♦♦est une fonction

polynomiale , de plus il n'admet pas de zéro en P ,

par conséquent $S(P) \neq 0 , \infty$. □

**Théorème 17 :** (existence de l'uniformisante)

Soit P un point de la courbe C , alors il existe une fonction rationnelle U avec U(P) = 0 tel que pour toute fonction G de $K^{alg}$ (C) non nulle , il existe un entier rationnel d et une fonction rationnelle S ,définie et non nulle en P, vérifiant $G = U^d \times S$ . De plus l'entier d ne dépend pas du choix de la fonction U .

**Définition 18 :**

La fonction U est l'uniformisante en P .

Preuve :

Soit G(u , v) une fonction rationnelle non nulle de C sur $K^{alg}$

*Si P est un point fini ,on suppose que G(P) = 0

*Si P= $\infty$ , on suppose que G(P) = $\infty$ .

Nous démontrons le théorème en trouvant une uniformisante pour chacun des cas suivants : $\leftarrow$ P= $\infty$ ,$\uparrow$ P point ordinaire ,$\rightarrow$ P point spécial .

$\leftarrow$Nous démontrons que l'uniformisante pour le point P =$\infty$ est $U= u^g / v$ ; pour cela , nous écrivons G sous la forme :

$$G = (u^g /v)^d \times (v/u^g)^d \times G \; ; \; d = - \deg(G) .$$

Notons $S(u , v) =(v / u^g)^d \times G$ ,

$\deg(v) - \deg(u^g) = 2g + 1 - 2g = 1$et $d = \deg(G)$

entraînent que $\deg ( u^{-gd} \times G ) = \deg(v^{-d})$ ; alors : $S(\infty) \neq 0 , \infty$ .

↑ Nous démontrons que l'uniformisante pour le point ordinaire $P = (x,y)$

est $U = u - x$ ; remarquons d'abord que $U(P) = x - x = 0$ .

$$G(u,v) = a(u) - b(u)v$$

Soit $(u - x)^r$ la plus grande puissance de $(u - x)$ qui divise $a(u)$ et $b(u)$ au

même temps , et nous écrivons $G(u ,v) = (u - x)^r ( a_0(u) - b_0(u) v)$ ;

Avec : $a(u) = (u - x)^r a_0(u)$

$b(u) = (u - x)^r b_0(u)$

$a_0(u)$ et $b_0(u)$ n'ont pas x comme racine commune ,alors d'après le lemme 15,

$a_0(u) - b_0(u) v = (u - x)^s \times S$ où : $(u - x)^s$ est la plus grande puissance de

$(u - x)$ qui divise $N(a_0(u) - b_0(u) v)$ et $S \in K^{alg} (C)$ / $S(P) \neq 0 , \infty$ .

Alors $G = (u - x)^{s+r} \times S$ / $S(P) \neq 0, \infty$ et $r+s = d \in Z$ .

→ Démontrons que l'uniformisante pour le point spécial $P= (x,y)$ est

$U = v - y$ ; remarquons d'abord que $U(P) = y - y = 0$ .

En remplaçant les puissances de u supérieures à 2g avec l'équation de la

courbe C , nous pouvons écrire :

$G(u,v) = u^{2g}b_{2g}(v)+(u-x)^{2g-1}b_{2g-1}(v)+\ldots+u\, b_1(v)+b_0(v)$,où chaque

$b_i(v) \in K^{alg}[v]$

Remplaçons toute occurrence de u par $(u - x )+x$ :

$G(u,v) = (u-x)^{2g}\overline{b}_{2g}(v) + (u-x)^{2g-1}\overline{b}_{2g-1}(v)+\ldots+(u-x)\,\overline{b}_1(v) + \overline{b}_0(v)$

$= (u-x)B(u,v) + \overline{b}_0(v)$ ; où $\overline{b}_i(v) \in K^{alg}[v]$ ,et $B(u,v) \in K^{alg}[C]$ .

$G(P) = 0$ entraîne $\overline{b}_0(y) = 0$ , donc nous pouvons écrire

$\overline{b}_0(v) = (v-y)\,c(v)$ / $c \in K^{alg}[v]$ .

D'après la preuve du lemme 16, nous pouvons écrire $u - x = (v-y)^2 / A(u,v)$

où $A(u,v) \in K^{alg}[C]$ et $A(P) \neq 0,\infty$ ,(en posant $A(u,v) = 1 / S(u,v)$).

Donc $G(u,v) = ((v-y)^2 / A(u,v)) \times B(u,v) + (v-y)c(v)$

$= [(v-y)/A(u,v)] \times [(v-y)B(u,v) + A(u,v)\,c(v)]$

$= [(v-y)/A(u,v)] \times G_1(u,v)$

Si $G_1(P) \neq 0$, alors on prend $S = G_1/ A$ et on a $S(P) \neq 0 , \infty$ .

Si $G_1(P) = 0$, alors $c(y) = 0$ (car $A(x,y) \neq 0$) et on peut écrire alors que

$c(v) = (v-y)\,c_1(v)$ pour $c_1 \in K^{alg}[v]$ ; alors on a :

$G(u,v) = [(v-y)^2/ A(u,v)] \times B(u,v) + (v-y)^2\, c_1(v)$

$= [(v-y)^2/ A(u,v)] \times [B(u,v) + A(u,v)\, c_1(v)]$

$= [(v-y)^2/A(u,v)] \times G_2(u,v)$

Si $G_2(P) \neq 0$ , on prend $S = G_2 / A$, sinon le processus peut être répété .

Pour voir que le processus se termine, on suppose qu'on a k facteurs de $(v-y)$ ; il y a deux cas à considérer :

1er cas : $k = 2l$

nous écrivons $G = [(v-y)^{2l} / A^l(u, v)] \times D(u, v)$ où $D \in K^{alg}[C]$,

ce qui implique $A^l G = (v-y)^{2l} \times D$ ; or $(u-x)^l = (v-y)^{2l} \times A^l$ ,

donc : $A^l G(u, v) = (u-x)^l \times A^l(u, v) \times D(u, v)$ ,d'où $G = (u-x)^l \times D$

Prenons les normes : $N(G) = (u-x)^{2l} \times N(D)$ , alors : $k \leq \deg(N(G))$.

2^em cas : $k = 2l + 1$

écrivons $G = [(v-y)^{2l+1} / A^{l+1}(u, v)] \times D(u, v)$ où $D \in K^{alg}[C]$

ce qui implique : $A^{l+1} G = (v-y)^{2l+1} \times D$

$$= (u-x)^l \times A^l \times (v-y) \times D$$

d'où $A \times G = (u-x)^l \times (v-y) \times D$ .

Prenons les normes : $N(A \times G) = (u-x)^{2l} \times N(v-y) \times N(D)$ ,

Alors : $2l < \deg(N(AG))$ , d'où : $k \leq \deg(N(AG))$ .

Conclusion : Dans les deux cas , k est borné par $\deg(N(AG))$ , donc le processus doit s'arrêter au bout d'un nombre fini d'étapes .

L'entier d est indépendant du choix de U , en effet :

soit $U_1$ une autre uniformisante de P ; dés que $U(P) = U_1(P) = 0$,

nous pouvons écrire $U = U_1^a \times A$ et $U_1 = U^b \times B$ ,où $a \geq 1$ , $b \geq 1$ et

$A, B \in K^{alg}(C)$ avec $A(P) \neq 0, \infty$ et $B(P) \neq 0, \infty$ .

Ainsi : $U = (U^b \times B)^a \times A = U^{a\,b} \times B^a \times A$ .

Divisons les deux membres par U , nous obtenons :

$U^{a\,b-1} \times B^a \times A = 1$ ,donc : $U^{a\,b-1} \times B^a \times A\,(P) = 1$ , ce qui implique :

a b –1 = 0 d'où : a = b = 1 .

Ainsi $G = U^d \times S = U^d_1 \times (A^d \times S)$ avec : $A^d S(P) \neq 0 , \infty$ □

**Définition 19 :** (ordre d'une fonction polynomiale en un point)

Soit G une fonction polynomiale de la courbe C sur $K^{alg}$ et P un point de C.

Soit $U \in K^{alg}(C)$ l'uniformisante en P et $G = U^d S$ où $S \in K^{alg}(C)$ , $S(P) \neq 0,\infty$.

L'ordre de G en P est l'entier $ord_P(G) = d$ .

**Lemme 20 :**

Soit $G_1$ et $G_2$ deux fonctions polynomiales non nulles de C sur $K^{alg}$ et soit $ord_P(G_1) = r_1$ , $ord_P(G_2) = r_2$ :

← l'ordre du produit $G_1 \times G_2$ est égal à la somme des ordres de $G_1$ et $G_2$ :

$ord_P (G_1 \times G_2) = ord_P(G_1) + ord_P(G_2)$

↑Supposons que $G_1 \neq G_2$ :

Si $r_1 \neq r_2$ , alors : $ord_P(G_1 + G_2) = \min( r_1 , r_2)$ .

Si $r_1 = r_2$ , alors : $ord_P(G_1 + G_2) \geq \min( r_1 , r_2)$ .

Preuve :

Soit U l'uniformisante en P , nous pouvons écrire :

$G_1 = U^r_1 \times S_1$ , $G_2 = U^r_2 \times S_2$ ; où $S_1, S_2 \in K(C) / S_1(P) \neq 0,\infty$ et $S_2(P) \neq 0,\infty$ .

Supposons que $r_1 \geq r_2$ :

$\leftarrow G_1 \times G_2 = U^{r1+r2} \times S_1\, S_2$ avec $S_1\, S_2\,(P) \neq 0, \infty$ ,donc : $ord_P(G_1 \times G_2) = r_1 + r_2$

$\uparrow G_1 + G_2 = U^{r\,1} S + U^{r2} S$

$= U^{r2} ( U^{r1\,-r2} S_1 + S_2 )$

Si $r_1 > r_2$ : $U^{r\,1-r2}\ S_1(P) = 0$ , et $S_2(P) \neq 0, \infty$ ; d'où :

$ord_P(G_1+G_2) = r_2 = \min(r_1, r_2)$ .

Si $r_1 = r_2$ : $G_1 + G_2 = U^r S_1 + U^r S_2$

$= U^r (S_1 + S_2)$ , avec : $(S_1 + S_2)(P) \neq \infty\ 0$ ;

d'où : $ord_P(G_1 + G_2) \geq r$ .

**Lemme 21 :**

Soit G une fonction polynomiale non nulle de C sur $K^{alg}$ et P un point de C ; alors : $ord_P(G) = ord_{\overline{P}}(\overline{G})$ .

**Théorème 22 :**

Soit G une fonction polynomiale de C sur $K^{alg}$ ,G possède un nombre fini de zéros et pôles , de plus $\sum_{P \in C} ord_P(G) = 0$ .

Preuve :

Soit $n = deg_u(G)$ ,cela implique $deg_u(N(G)) = n$,

écrivons la norme N(G)) sous la forme

$N(G) = G \times \overline{G} = (u - x_1)(u - x_2) \ldots (u - x_n)$

où les $x_i \in K$ ne sont pas nécessairement distincts .

Si $x_i$ est la $i^{eme}$ coordonnée du point ordinaire $P=(x_i , y_i)$ de C ,alors

$ord_P(u - x_i) = 1$ , $ord_{\overline{P}}(u - x_i) = 1$ et $(u - x_i)$ n'a pas d'autres zéros .

Si $x_i$ est la $i^{eme}$ coordonnée du point spécial $P = (x_i , y_i)$de C , alors

$ord_P (u - x_i) = 2$ et $(u - x_i)$ n'a pas d'autres zéros.

Alors l'équation $N(G) = G \times \overline{G} = 0$ possède 2n solutions , ce qui implique que l'équation $G = 0$ possède n solutions i.e. un nombre fini de zéros .

De plus G est une fonction polynomiale non nulle, donc $G \neq \infty$ sauf si $P = \infty$ et $ord_\infty(G) = -n$ …….……(1)

Le lemme 21 entraîne l'égalité $\sum ord(N(G)) = 2n$, d'où

$\sum_{P \in C} ord(G) = \sum_{\overline{P} \in C} ord(\overline{G})$ , et alors $\sum ord(G) = n$ ……..(2)

(1) et (2) impliquent que $\sum_{P \in C} ord(G) = 0$ . □

**Définition 23 :** (ordre d'une fonction rationnelle en un point )

Soit $R = G / H$ une fonction rationnelle de C sur $K^{alg}$ et P un point de C ; l'ordre de R en P est défini par : $ord(R) = ord(G) - ord(H)$ ;

Remarques :

*l'ordre de R ne dépend pas du choix de G et H .

*Si $ord_P(R) = r > 0$, on dit que R possède un zéro en P d'ordre r sur C.

*Si $ord_P(R) = r < 0$, on dit que R possède un pole en P d'ordre r sur C.

*Le lemme 20 et le théorème 22 sont vrais aussi pour les fonctions rationnelles non nulles .

Le logiciel MAGMA contient une implémentation des courbes hyperelliptiques :

## Exemple :

```
> p:=103;
> K:=GF(p);
> P<x>:=PolynomialRing(GF(p));
> C:=HyperellipticCurve(x^5+8*x+1);
> #C;
96
> time;
Time: 0.000
> Points(C);
{@ (1 : 0 : 0), (0 : 1 : 1), (0 : 102 : 1), (2 : 7 : 1), (2 : 96 : 1), (5 : 30 :1), (5 : 73 : 1), (6 :
93 : 1), (6 : 10 : 1), (8 : 64 : 1), (8 : 39 : 1), (9 : 0 : 1), (10 : 58 : 1), (10 : 45 : 1), (12 : 9 :
1), (12 : 94 : 1), (13 : 17 : 1),(13 : 86 : 1), (17 : 97 : 1), (17 : 6 : 1), (19 : 82 : 1), (19 : 21 :
1), (23 :26 : 1), (23 : 77 : 1), (24 : 14 : 1), (24 : 89 : 1), (27 : 83 : 1), (27 : 20 : 1), (28 : 23
: 1), (28 : 80 : 1), (34 : 50 : 1), (34 : 53 : 1), (37 : 15 : 1),(37 : 88 : 1), (39 : 23 : 1), (39 :
80 : 1), (42 : 15 : 1), (42 : 88 : 1), (43 : 9 : 1), (43 : 94 : 1), (45 : 81 : 1), (45 : 22 : 1), (46
: 61 : 1), (46 : 42 :1), (50 : 7 : 1), (50 : 96 : 1), (52 : 72 : 1), (52 : 31 : 1), (53 : 46 : 1), (53
: 57 : 1), (55 : 97 : 1), (55 : 6 : 1), (56 : 17 : 1), (56 : 86 : 1), (57 :68 : 1), (57 : 35 : 1), (58
: 41 : 1), (58 : 62 : 1), (63 : 18 : 1), (63 : 85 :1), (64 : 83 : 1), (64 : 20 : 1), (65 : 36 : 1),
(65 : 67 : 1), (68 : 92 : 1),(68 : 11 : 1), (70 : 92 : 1), (70 : 11 : 1), (73 : 97 : 1), (73 : 6 : 1),
(75 :83 : 1), (75 : 20 : 1), (76 : 23 : 1), (76 : 80 : 1), (78 : 92 : 1), (78 : 11 : 1), (81 : 2 : 1),
(81 : 101 : 1), (84 : 30 : 1), (84 : 73 : 1), (85 : 66 : 1),(85 : 37 : 1), (88 : 50 : 1), (88 : 53 :
1), (89 : 72 : 1), (89 : 31 : 1), (94 : 38 : 1), (94 : 65 : 1), (95 : 52 : 1), (95 : 51 : 1), (96 :
66 : 1), (96 : 37 : 1), (98 : 82 : 1), (98 : 21 : 1), (101 : 46 : 1), (101 : 57 : 1) @}
> time;
Time: 0.000
> FunctionField(C);
Algebraic function field defined over GF(103) by
$.1^5 + 8*$.1 + 102*$.2^2 + 1
```

# CHPITRE II : Diviseurs et Jacobienne d'une courbe hyperelliptique

Contrairement aux courbes elliptiques , il n'y a pas de loi de groupe définissable directement sur l'ensemble des points de la courbe hyperelliptique C ; c'est pourquoi on étudie la jacobienne de C qui, elle, peut être munie d'une loi d'addition .

Un élément de la jacobienne est «un diviseur» ; pour cela ,nous allons étudier quelques notions élémentaires sur les diviseurs .

## II-1/ Diviseurs sur une courbe hyperelliptique :

**Définition 1 :**

Soit la courbe hyperelliptique C sur le corps K :

*Un diviseur D sur C est une somme formelle de points appartenant à C .

Ainsi , un diviseur D s'écrit :

$$D = \sum_{P \in C} m_P \, P ,$$

où les $m_P$ sont des entiers rationnelles presque tous nuls .

*Le degré d'un diviseur D ,noté deg(D) , est la somme de ses coefficients : $\deg(D) = \sum_{P \in C} m_P$ .

*Un diviseur $D = \sum_{P \in C} m_P P$ est effectif (positif) si chaque $n_P$ est positif .

On écrit : $\sum_{P \in C} m_P P > \sum_{P \in C} n_P P$ si chaque $m_P \geq n_P$ .

*L'ordre d'un diviseur D en un point P est le nombre $m_P$ , on écrit :

$ord_P(D) = m_P$ .

**Définition 2 :**

Soit C une courbe hyperelliptique :

*L'ensemble de tous les diviseurs ,noté *D* ,forme un groupe abélien sous la loi d'addition formelle suivante :$\sum_{P\in C} m_P P + \sum_{P\in C} n_P P = \sum_{P\in C}(m_P+n_P)P$.

*L'ensemble de tous les diviseurs de degré 0 , noté $D^0$, est un sous groupe du groupe *D* des diviseurs de C .

**Définition 3 :** (diviseur d'une fonction rationnelle )

Soit $R \in K^{alg}(C)^*$ une fonction rationnelle ; Le diviseur de R est :

$div(R) = \sum_{P\in C} ord_P(R)\ P$ .

Notons que si R = G/H , alors : div(R) = div(G) –div(H) .

**Lemme 4 :**

Le diviseur div(R) d'une fonction rationnelle R est une somme formelle finie et est de degré 0 .

Preuve :

Soit $div(R) = \sum_{P\in C} ord_P(R)\ P$ le diviseur d'une fonction rationnelle R

La définition du degré d'un diviseur implique :$deg(div(R)) = \sum_{P\in C} ord(R)$

Le théorème I-22 entraîne que $deg(div(R)) = \sum_{P\in C} ord(R) = 0$ .

Exemples :

← P = (x , y) point ordinaire de la courbe C , alors :

$\text{div}(u - x) = P + \overline{P} - 2\infty$ ; en effet :

*Au point $P = (x , y)$ ordinaire , on associe l'uniformisante : $U = u - x$

donc : $u - x = (u - x)^1 \text{ id}$ avec : $\text{id}(P) \neq 0 , \infty$ .

d'où : $\text{ord}_P(u - x) = \text{ord}_{\overline{P}}(u - x) = 1$ ……..(1)

*Au point $Q = (a , b) \neq P , \overline{P}$ , on associe l'uniformisante : $U = u - a$

donc : $u - x = (u - a)^0 \times (u - x)$ avec : $(u - x)(Q) = a - x \neq 0 , \infty$ .

d'où : $\text{ord}_Q (u - x) = 0$ ……(2)

* Au point $P = \infty$ , on associe l'uniformisante : $U = u^g / v$

$\text{ord}_\infty (u - x) = -\deg (u - x) = -2$ ……(3)

Alors : $\text{div}(u - x) = \text{ord}_P(u - x)\, P + \text{ord}_P(u - x)\, P + \text{ord}_\infty(u - x)\, \infty$

$= P + \overline{P} - 2\infty$ .

↑ $P = (x , y)$ point spécial de la courbe C ($\overline{P} = P$ ) , alors :

$\text{div}(u - x) = 2P - 2\infty$ ; en effet :

*Au point spécial $P = (x , y)$ , on associe l'uniformisante : $U = v - y$

donc : $u - x = (v - y)^2 \times S$ avec : $S(P) \neq 0 , \infty$ (d'après le lemme I-16 )

d'où : $\text{ord}_P (u - x ) = 2$ .

*Au point $P = \infty$ , on associe l'uniformisante : $U = u^g / v$

donc : $(u - x) = (u^g / v)^d \times (v / u^g)^d (u - x)$

$= (v / u^g)^d \times (u^g / v)^d \times (u - x)$

$$= (v / u^{g})^{d} \times S$$

Pour que S soit finie , non nulle en P , il suffit d'avoir :

$\deg [u^{g\times d} \times (u - x)] = \deg v^{d}$ , d'où : $d = 2$ i.e. : $\mathrm{ord}_{\infty}(u - x) = -2$

Alors : $\mathrm{div}(u - x) = \mathrm{ord}_{P}(u - x)\, P + \mathrm{ord}_{\infty}(u - x)\, \infty$

$$= 2P - 2\infty .$$

**Lemme 5:**

Soit $R_1$, $R_2$ deux fonctions rationnelles de la courbe C ;alors Le diviseur du produit $R_1 \times R_2$ est égal a la somme des diviseurs de $R_1$ et $R_2$ $[\mathrm{div}(R_1 \times R_2) = \mathrm{div}(R_1) + \mathrm{div}(R_2)]$ .

Preuve :

La définition du diviseur d'une fonction rationnelle implique :

$\mathrm{div}(R_1 \times R_2) = \sum_{P\in C} \mathrm{ord}_{P}(R_1 \times R_2)\, P$

Le lemme I-20 implique :

$\mathrm{div}(R_1 \times R_2) = \sum_{P\in C} (\mathrm{ord}_{P}(R_1) + \mathrm{ord}(R_2))\, P$

$$= \sum_{P\in C} \mathrm{ord}_{P}(R_1)\, P + \sum \mathrm{ord}_{P}(R_2)$$

$$= \mathrm{div}(R_1) + \mathrm{div}(R_2) .$$

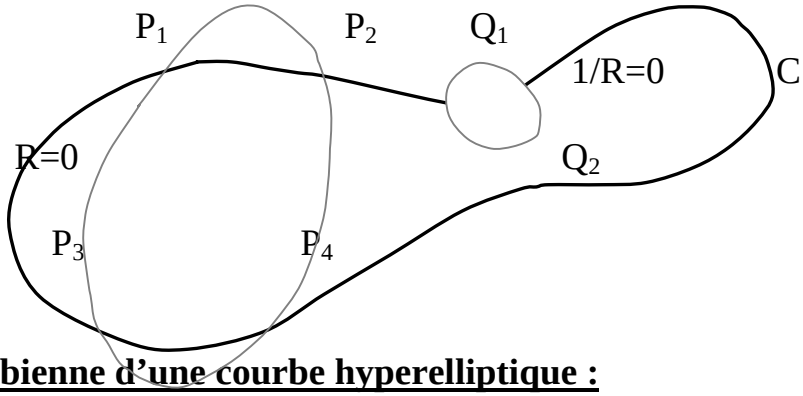
Remarque :

Soit R une fonction . On découpe souvent div(R) en la différence de 2 diviseurs effectifs :

$$\mathrm{div}(R) = \mathrm{div}_0(R) - \mathrm{div}_{\infty}(R) ,$$

où $div_0(R)$ est l'intersection de la courbe C avec la courbe R = 0 , et $div_\infty(R)$ est l'intersection avec 1/ R = 0 .

Sur le dessin ci-dessous on a : $div(R) = P_1+P_2+P_3 -(2Q_1+2Q_2)$ .




## II-2/ Jacobienne d'une courbe hyperelliptique :

**Définition 6 :**

*Un diviseur D du groupe $D^0$ des diviseurs de degré 0 est principal s'il est le diviseur d'une fonction rationnelle R , et on écrit : D = div(R) .

*L'ensemble de tous les diviseurs principaux, noté *P*, est un sous groupe du groupe $D^0$ .

**Proposition 7 :**

Soit D , D' deux diviseurs de degré 0 ,

←La relation ~ est une relation d'équivalence .

↑L'équivalence (D ~ 0) implique D est le diviseur d'une fonction rationnelle .

→ Si D ~ D' et $D_1$~ $D_1$' , alors : D + $D_1$ ~ D' + $D_1$' .

**Définition 8 :**

Soit C une courbe hyperelliptique définie sur un corp K .

*La jacobienne de C est le groupe des diviseurs de degré 0 quotienté par les diviseurs principaux : $J = D^0 / P$ .

*Deux diviseurs D , D' de degré 0 sont linéairement équivalents si leur différence est un diviseur principal : D' = D + div(R) pour une certaine fonction rationnelle R , et on écrit : D'~ D .

**Définition 9:**

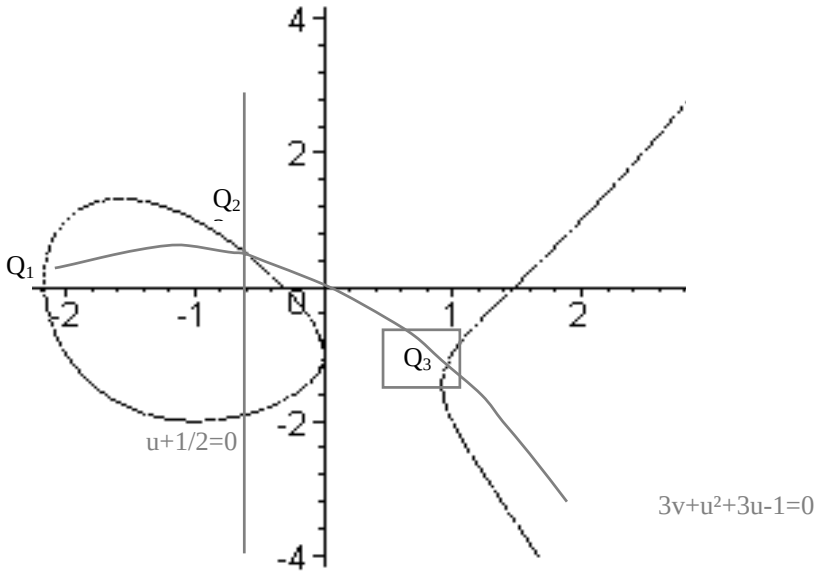
Un diviseur $D = \sum m_P P$ défini sur le corps K est dit premier si

*D est effectif .

*Si D' est effectif , défini sur K et $D' \leq D$ , alors D' est nul ou égal à D .

Exemple :
Considérons la courbe hyperelliptique C d'équation :

$v^2+(u+2)\,v = u^3 + u^2 - 3u - 1$ sur Q ; il s'agit d'une courbe elliptique ; son allure lorsqu'on la trace sur R est




C

On rajoute le point à l'infini qui complète notre courbe C .

Soient $P_1$et $P_2$ les deux points de C de coordonnées

$P_1$= (-½ , (-3+√19)⁄4) et $P_2$ = (-½ , (-3-√19)⁄4) ,

ces deux points sont conjugués sur Q et le diviseur D = $P_1$+ $P_2$ est un diviseur premier de degré 2 défini sur Q .

Soit la fonction rationnelle R sur C définie par R =(3v + $u^2$ +3u –1) /u +½.

La courbe correspondante à l'annulation du numérateur coupe C en les trois points $Q_1$=(-2 , 1) , $Q_2$ =(-1 , 1) , $Q_3$ =(1 , -1) , et celle correspondant au dénominateur coure C en $P_1$ et $P_2$ . Si l'on tient compte des intersections à l'infini on obtient ainsi

$$div(R) = Q_1 + Q_2 + Q_3 - P_1 - P_2 - \infty$$

Ainsi par exemple les deux diviseurs de degré 0 suivants sont linéairement équivalents :

$$P_1 + P_2 - Q_1 - Q_2 \sim Q_3 - \infty .$$

**Définition 10 :**

Soit P =(x , y) un point de la courbe hyperelliptique C , et soit σ un automorphisme du corps $K^{alg}$ dans le corps K ; on définit

*Le point $P^\sigma$ de la courbe C par $P^\sigma = (x^\sigma , y^\sigma)$ , ainsi que le diviseur $D^\sigma$ de C par : $D^\sigma = \sum m_P P^\sigma$ .

*Un diviseur $D = \sum_{P \in C} m_P P$ est«bien défini »sur K si $D^\sigma$ = D pour tout

automorphisme $\sigma$ de $K^{alg}$ dans K .

*L'ensemble des diviseurs principaux bien définis sur K forment un sous groupe du groupe *P* des diviseurs principaux , son image *J*(K) dans *J* est un sous groupe de *J* [ J(K) est l'ensemble de toutes les classes des diviseurs de *J* qui possèdent un représentant bien défini sur K] .

**II-3/ Loi de groupe sur la jacobienne :**

Soit P =(x , y) un point de la courbe C ,et $\overline{P}$ son opposé , l'exemple du chapitre II montre que le diviseur de la fonction (u –x) est :

div(u –x) = P +$\overline{P}$ -2$\infty$ , donc : P +$\overline{P}$ -2$\infty$ ~ 0(mod *P*) ou –$\overline{P}$ ~ P –2 $\infty$ ; ce qui entraîne que chaque élément D de la jacobienne J peut s'écrire sous la forme : D = $\sum P_i$ –r $\infty$ avec la condition suivante : si $P_i = (x_i , y_i)$ est un point de C qui apparaît dans D alors : $\overline{P}_i$ n'apparaît pas autant qu'un des $P_j$ ($j \neq i$) .

On appelle un tel diviseur « diviseur semi-réduit » .

**II-3-1/ Diviseurs semi –réduits :**

**Définition 11 :**

Soit $D = \sum_{P \in C} m_P P$ un diviseur de C , le support de D est l'ensemble fini de points P pour lesquels le coefficients $m_P$ est non nul :

$$supp(D) = \{P \in C / m_P \neq 0\} .$$

**Définition 12 :**

Un diviseur semi –réduit est un diviseur de la forme :

$D = \sum_{Pi \in C} m_i P_i - (\sum m_i)\infty$ où : $m_i \geq 0$ pour tout indice i et les $P_i$ sont des points finis tels que si $P_i \in supp(D)$ , alors $\overline{P}_i \notin supp(D)$

et si $\overline{P}_i = P_i$ , alors : $m_i = 1$ .

**Lemme 13 :**

Chaque diviseur de degré 0 est équivalent à un diviseur semi-réduit .

Preuve :

Soit $D = \sum_{P \in C} m_P P$ un diviseur de degré 0 ;

Soit $(C_1, C_2)$ une partition de l'ensemble des points ordinaires de la courbe C telle que :

← Un point P appartient à $C_1$ si et seulement si l'opposé $\overline{P}$ de P appartient à $C_2$ .

↑ Si un point P est dans $C_1$ , alors $m_P \geq m_{\overline{P}}$ .

Soit $C_0$ l'ensemble des points spéciaux de C , alors on peut écrire

$D = \sum_{P \in C1} m_P P + \sum_{P \in C2} m_P P + \sum_{P \in C0} m_P P - m \infty$ .

Considérons le diviseur suivant :

$D_1 = D - \sum_{P \in C2} m_P \, div(u - x) - \sum_{P \in C0} [m_P/2] \, div(u - x)$ ,

alors $D_1 \sim D$ .

De plus , $D_1=[\sum_{P\in C1}m_PP+\sum_{P\in C2}m_PP+\sum_{P\in C0}m_PP-m\infty]-\sum_{P\in C2}m_P\mathrm{div}(u-x)-\sum_{P\in C0}[m_P/2]\,\mathrm{div}(u-x)$

$=[\sum_{C1}m_PP+\sum_{C2}m_PP+\sum_{C0}m_PP-m\infty]-\sum_{C2}m_P(P+P-2\infty)-\sum_{C0}[m_P/2](2P-2\infty)$

$=\sum_{C0}(m_P-2[m_P/2])P+\sum_{C1}(m_P-m_P)P-m_1\infty$ pour un certain entier rationnel $m_1$ , donc $D_1$ est un diviseur semi-réduit .

Représentation des diviseurs semi-réduit (due à Mumford) :

**Lemme 14 :**

Soit P =(x , y) un point ordinaire de C , et R une fonction rationnelle non nulle qui ne possède pas de pole en P ; alors : pour un certain $k \geq 0$ , il existe des éléments uniques $c_0$ , $c_1$ ,…,$c_k$ de K et une fonction rationnelle $R_k$ de $K^{alg}(C)$ tels que $R = \sum_{i=0}^{k}c_i(u-x)^i + (u-x)^{k+1}R_k$ où $R_k$ n'a pas de pôle en P .

Preuve :

Il y a un unique élément $c_0$ de $K^{alg}$ qui vérifie $c_0 = R(x , y)$ et tel que : P est un zéro de $R - c_0$ .

P est un point ordinaire donc l'uniformisante en P est $U = u - x$ , et on peut écrire $R - c_0 = (u-x)\,R_1$, pour une fonction unique $R_1$ de $K^{alg}(C)$ avec $\mathrm{ord}_P(R_1) \geq 0$ , donc $R = c_0\,(u-x)^0 + (u-x)R_1$ …….(1)

De même $R_1 = c_1(u-x)^0 + (u-x)\,R_2$ ……(2)

avec $c_1 \in K$ et $ord_P R_2 \geq 0$ .

(1) et (2) impliquent $R = c_0(u-x)^0 + c_1(u-x) + (u-x)^2 R_2$ .

et on continue le processus jusqu'à avoir :

$R = \sum_{i=0}^{k} c_i (u-x)^i + (u-x)^{k+1} R_k$ .

**Lemme 15 :**

Soit P = (x , y) un point ordinaire de la courbe C, alors pour chaque $k \geq 1$,

il existe un unique polynôme $b_k(u)$ de $K^{alg}[u]$ tel que :

$\leftarrow \deg_u b_k \leq k$ , $\uparrow b_k(x) = y$ , $\rightarrow b_k^2(u) + b_k(u)\, h(u) \equiv f(u) \pmod{(u-x)^k}$ .

Preuve :

$\leftarrow$Soit $v = \sum_0^{k-1} c_i(u-x)^i + (u-x)^k R_{k-1}$ où les $c_i$ sont des éléments de $K^{alg}$ et

$R_{k-1}$ est une fonction de $K^{alg}(C)$ .

On définit le polynôme : $b_k(u) = \sum_0^{k-1} c_i (u-x)^i$ ; $\deg_u(b_k) \leq k$ .

$\uparrow$ Il existe un élément $c_0$ de K qui vérifie : $v(P) = c_0$ i.e. $v(x , y) = c_0$

d'où : $y = c_0$ , alors : $b_k(x) = \sum_0^{k-1} c_i(u-x)^i = c_0 = y$ .

$\rightarrow$ Finalement , soit C : $v^2+h(u)v = f(u)$ l'équation de la courbe C .

En réduisant les deux membres de l'équation modulo $(u-x)^k$ , on obtient :

$b_k^2(u)+((u-x)^k R_{k-1})^2+2\times b_k^2(u)\,(u-x)^k R_{k-1}+h(u)\, b_k(u)+h(u)(u-x)^k R_{k-1}=f(u)$.

d'où $b_k^2(u)+h(u)\, b_k(u) \equiv f(u) \pmod{(u-x)^k}$ .

**Définition 16 :**

Soit $D_1 = \sum_{P \in C} m_P P$ et $D_2 = \sum_{P \in C} n_P P$ deux diviseurs de C ; le plus grand

diviseur commun de $D_1$ et $D_2$ est définie par :

$Pgcd(D_1,D_2) = \sum_{P\in C} \min(m_P,n_P)P - (\min(m_P,n_P))\infty$ .

**Théorème 17 :**

Soit $D = \sum_{Pi\in C} m_i P_i - (\sum m_i)\infty$ un diviseur semi-réduit de C, avec

$P_i = (x_i,y_i)$, et soit dans K[u] les polynômes suivants :

*$a(u) = \Pi (u - x_i)^{mi}$

*b(u) l'unique polynôme de K[u] qui satisfait les trois propriétés

suivantes :

$\leftarrow \deg_u(b) < \deg_u(a)$

$\uparrow b(x_i) = y_i$ , pour tout i qui vérifie $m_i \neq 0$.

$\rightarrow$ a(u) divise $(b(u)^2 + b(u)\, h(u) - f(u))$.

Alors D = pgcd(diva(u) , div(b(u) –v)).

Notation : Un diviseur semi-réduit D dans sa représentation de Mumford

est noté D = div(a , b) .

**Définition 18 :**

Le degré du polynôme a est appelé le poids du diviseur, et le diviseur est

dit premier si le polynôme a est irréductible .

Remarque :

*Le diviseur nul , noté $\theta$ , est représenté par $\theta$ = div(1 , 0)

*Un diviseur de degré 1 i.e. avec un seul point $P = (x_P , y_P)$ est représenté

par $\mathrm{div}(u - x_P, y_P)$ .

## II-3-2/ Diviseurs réduits :

**Définition 19 :**

Un diviseur réduit sur un courbe hyperelliptique C est un diviseur semi-réduit $D = \sum_{Pi \in C} m_i P_i - (\sum m_i) \infty$ qui vérifie $\sum m_i \leq g$ ,où g est le genre de la courbe C .

**Définition 20 :**

Soit $D = \sum_{P \in C} m_P P$ un diviseur de C ; la norme de D est définie par :

$$|D| = \sum |m_P| \quad .$$

**Lemme 21 :**

Soit R une fonction rationnelle sur C , si R ne possède pas de pôles finis, alors R est une fonction polynomiale .

**Théorème 22 :**

Pour tout diviseur D du groupe $D^0$ des diviseurs de degré 0, il existe un unique diviseur réduit $D_1$ équivalent au diviseur D .

Cantor a trouvé un algorithme pour la loi de groupe utilisant une représentation des diviseurs due à Mumford ; or il a assumé que la fonction h(u) est nulle (h(u) = 0) et que la caractéristique du corps K est différente de 2 .

## II-3-3/ Algorithme de Cantor :

Le problème est le suivant : étant donnés deux diviseurs réduits dans la représentation de Mumford , trouver le diviseur réduit représentant leur somme dans la jacobienne (toujours sous forme de Mumford) .

**Lemme 23 :**

Soit C une courbe hyperelliptique de genre g , et soit

D =div(a , b) un diviseur réduit (ou semi-réduit) , alors son opposé dans *J* est donné sous forme de Mumford par –D =div(a , -b –h(u) mod(a)) .

L'algorithme d'addition dans la jacobienne se décompose en deux parties : la composition calcule un diviseur semi-réduit représentant la somme de deux diviseurs , la réduction transforme un diviseur semi-réduit en un diviseur réduit .

1/La composition :

Entrée : Deux diviseurs semi-réduits $D_1$ =div($a_1$,$b_1$) et $D_2$ =div($a_2$ , $b_2$) .

Sortie : Un diviseur semi-réduit $D_3$ tel que $D_3 \sim D_1+D_2$ dans *J* .

← Par deux calculs de pgcd étendus , construire $s_1$, $s_2$, $s_3$ tels que :

$$d = pgcd\ (a_1\ ,\ a_2\ ,\ b_1+b_2+h)$$

$$= s_1a_1+ s_2a_2+s_3(b_1+ b_2+ h)\ .$$

↑ Poser $a_3 = a_1a_2 / d^2$ ;

→ Poser $b_3 = (s_1a_1b_2+ s_2a_2b_1+s_3(b_1\ b_2+ h) / d \bmod(a_3)$ .

↓ Retourner $D_3 = div(a_3 , b_3)$ .

2/ La réduction :

Entrée : Un diviseur semi-réduit $D = div(a , b)$ .

Sortie : Un diviseur réduit $D' \sim D$ .

← Tant que $deg(a(u)) > g$ , faire

↑ $a' = (f - hb - b^2) / a$ ;

→ $b' = -h - b \bmod(a)$ ;

↓ Retourner $D' = div(a' , b')$ .

Remarque :

Dans la preuve de l'exactitude de l'algorithme , Cantor a commit des erreurs lorsqu'il a déclaré que la condition $a / b^2 - f$ est équivalente à la condition $b - y_i$ est divisible par $(u - x_i)^{m_i}$ pour tout i(où $P_i=(x_i , y_i)$ .
Neal Koblitz a présenté un algorithme efficace pour la loi de groupe , qui est une généralisation de l'algorithme de Cantor, mais il n'a pas démontré son exactitude .

**II-3-4 /Algorithme d'addition de deux diviseurs :**

1ere étape de l'algorithme : (la composition)

En composant deux éléments $D_1 = div(a_1 , b_1)$ , $D_2 = div(a_2 , b_2)$ de la jacobienne J de C , nous obtenons une représentation (en diviseur semi-réduit sur K) de la somme $D_1 + D_2$ [D semi- réduit / $D \sim D_1 + D_2$] .

1/ On utilise l'algorithme d'Euclide pour calculer :

$$d_1 = \text{pgcd}(a_1 , a_2)$$

ainsi que les polynômes $e_1$ , $e_2$ dans l'anneau K[u] qui vérifient :

$$d_1 = e_1 a_1 + e_2 a_2 .$$

2/On utilise le même algorithme pour calculer : $d = \text{pgcd}(d_1 , b_1+b_2+h)$

ainsi que les polynômes $c_1$ , $c_2$ de l'anneau K[u] qui vérifient :

$d = c_1 d_1 + c_2(b_1+b_2+h)$ .

3/On pose : $s_1 = c_1 e_1$ , $s_2 = c_1 e_2$ et $s_3 = c_2$ , donc :

$d = c_1(e_1 a_1 + e_2 a_2) + c_2(b_1+b_2+h)$

$= s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h)$ ……..(3)

4/ Finalement , on calcule les polynômes :

$$a = a_1 a_2 / d^2 \text{ …….(4)}$$

et $b = [(s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)) / d \,] \bmod a$ …..(5)

Alors le diviseur D = div(a , b) est un diviseur semi-réduit qui représente la somme $D_1+D_2$ dans J : $D \sim D_1+D_2$ .

Après avoir trouvé la représentation de la somme $D_1+D_2$ en diviseur semi-réduit , nous passons à la $2^{eme}$ étape pour la réduire .

$2^{em}$ étape de l'algorithme : (la réduction)

Nous décrivons l'algorithme de réduction du diviseur semi réduit D de la première étape représenté par D = div(a , b) .

1/Si le degré du polynôme a est inférieur ou égal au genre g ,D sera réduit.

Si deg(a) est supérieur ou égal à g , nous calculons les polynômes a' et b' tels que :

$a' = (f - b\,h - b^2) / a$

$b' = (-h - b) \bmod a'$ et deg b' <deg a .

2/ Si deg(a') est supérieur à g , on recommence le procédé précédent en remplaçant les polynômes a et b par les polynômes a' et b' obtenus dans l'étape précédente .

La jacobienne d'une courbe hyperelliptique est l'ensemble des diviseurs réduits , l'algorithme précédent défini une opération d'addition sur les diviseurs réduits qui fait de J un groupe , l'unique diviseur de degré 0, $\theta$=div(1,0), est l'élément neutre pour cette loi d'addition .

Analogie :

L'addition des diviseurs telle qu'elle est présenté ci-dessus est analogue à la sommation dans un groupe plus connu , c'est le groupe Z/pZ

Exemple :

Considérons le corps fini $F_2{}^5 = F_2[x] / (x^5+x^2+1)$ , et $\propto$ une racine primitive du polynôme $x^5+x^2+1$ dans le corps $F_2{}^5$ .

Considérons aussi la courbe hyperelliptique C : $v^2+(u^2+u)\,v = u^5+u^3+1$ de

genre 2 définie sur le corps $F_2{}^5$ .

Les points : $Q_1$= (0 , 1) , $Q_2$= (1 , 1) sont spéciaux .

Le point P =($\propto^{30}$ , 0) est ordinaire , son opposé $\overline{P}$ est égal à $\overline{P}$=($\propto^{30}$,$\propto^{16}$) .

Composition de deux diviseurs réduits :

Soit $D_1$= P +$Q_1$ –2 $\infty$ , $D_2$ = P +$Q_2$ –2$\infty$ deux diviseurs réduits :

I/ le théorème II-17 implique :

$D_1$ = div ($a_1$ , $b_1$) avec $a_1$=u(u + $\propto^{30}$) et $b_1$= $\propto$u +1 .

$D_2$ = div ($a_2$ , $b_2$) avec $a_2$=(u +1)(u + $\propto^{30}$) et $b_2$= $\propto^{23}$u +$\propto^{12}$ .

II / La composition :

1/ l'algorithme d'Euclide donne $d_1$= pgcd($a_1$, $a_2$) = u +$\propto^{30}$ ; $d_1$=$a_1$ +$a_2$ .

2/ le même algorithme donne aussi d = pgcd($d_1$ , $b_1$+$b_2$ +h) = u +$\propto^{30}$ ;

d = 1× $d_1$ + 0×( $b_1$+$b_2$ +h) .

3/ $s_1$ = 1 , $s_2$ = 1 et $s_3$ = 0 , d'où d = $a_1$ +$a_2$ = $d_1$ .

4/ on calcule les polynômes a et b tels que :

a = $a_1a_2$ / $d^2$ = u(u +1) = $u^2$ + u

b = [($s_1a_1b_2$ + $s_2a_2b_1$ + $s_3$($b_1b_2$ +*f*)) / d ] mod a

= $a_1b_2$ + $a_2b_1$ / $a_1$ + $a_2$ mod a

≡ 1 mod a .

Conclusion :

Le diviseur semi réduit D = div(a , b) représente la somme $D_1$+$D_2$ .

Ecrivons D sous la forme d'une somme $\sum_{P\in C} m_P P$ :

$div(a) = 2Q_1 + 2Q_2 - 4\infty$ .

$div(b-v) = Q_1+Q_2+ \sum_{i=1}^{3} P_i - 5\infty$ .

Alors $D = pgcd\ (div(a)\ ,\ div(b-v))$

$= Q_1+Q_2 - 2\infty$.

**II-4/ Doublement d'un diviseur :**

Doubler un diviseur (ou calculer 2D , D = div (a , b) ) est plus facile que

l'addition générale, les étapes 1← ,2 ↑, 3→ , et 4↓ de la composition peuvent

être simplifier comme suit :

← $d = pgcd\ (a, 2b + h)$ ;

↑ $a' = a^2 / d^2$ ;

$b' = [s_1\ a\ b + s_3\ (b^2 + f)\ ] / d \mod (a')$ ;

→ Retourner D' = div(a',b') semi-réduit avec D'~ 2 D .

Si deg (a') > g , nous calculons :

↓ $a'' = f - b'h - b'^2 / a'^2$ ;

$b'' = (-h - b') \mod (a'')$ ;

°Retourner D'' = div(a'', b'') diviseur réduit avec D''~ D~ 2 D .

## II-5/ Multiplication scalaire :

**Définition 23 :**

Soit l un entier , la multiplication par le scalair l est notée par

$$[l]\,D = D + D + \ldots + D \text{ (l fois)}$$

**Définition 24 :**

*****On dit que D est un diviseur de l-torsion si $[l]\,D = \theta$ .

*L'ensemble de tous les diviseurs de l-torsion , y compris ceux qui sont définis sur des extensions du corps de base K , noté $J[l]$ , est un sous groupe du groupe $J$ .

Remarque :

L'intérêt de doubler un diviseur est de calculer efficacement la multiplication scalaire $[l]D$ , qui serait utile en cryptographie .

Exemple :

```
> p:=100000007;
> P<x>:=PolynomialRing(GF(p));
> C:=HyperellipticCurve(x^5+456*x^4+98*x^3+76*x^2+54*x+32);
> J:=Jacobian(C);
> #J;
10001648178050390
> time;
Time: 0.000
> FactoredOrder(J);
[ <2, 1, 5000824089025195>, <5, 1, 2000329635610078>, <17, 1,
588332245767670>,

<58833224576767, 1, 170> ]
> D:=Random(J);
> D;
(x^2 + 37402108*x + 2928982, 19398429*x + 36900359, 2)
> Order(D);
5000824089025195
```

Nous crayons une nouvelle courbe hyperelliptique de genre 3 sur le même corps de base GF(p).

```
> f:=x^7+123456*x^6+123*x^5+456*x^4+98*x^3+67*x^2+54*x+32;
> J:=Jacobian(HyperellipticCurve(f));
> time Order(J);
1001155288112766456
Time: 48.229
> D1:=Random(J);
> D1;
(x^3 + 566870*x^2 + 467841*x + 535878, 90251*x^2 + 854670*x + 738820, 3)
> D2:=Random(J);
> D2;
(x^3 + 774343*x^2 + 502784*x + 633680, 295604*x^2 + 281326*x + 942207, 3)
> D1 eq D2;
false
> D1+D2;
(x^3 + 199061*x^2 + 276057*x + 932406, 790013*x^2 + 280051*x + 815478, 3)
> time;
Time: 0.000
```

# CHAPITRE III : Introduction à la cryptographie à l'aide des courbes hyperelliptiques

L'étude algorithmique des courbes hyperelliptique est la suite naturelle de celle des courbes elliptiques qui est maintenant bien avancée . La plupart des algorithmes connus pour les courbes elliptiques ainsi que leurs applications à la cryptographie peuvent être étendus plus au moins facilement aux jacobiennes des courbes hyperelliptiques .

## III-1/ Chiffrement à clé publique :

En 1976, W.F.Diffie et M.Hellman proposent une nouvelle façon de chiffrer. Commençons par expliquer leur procédé :

*A et B choisissent un groupe abélien fini G , et un élément $\propto$ de G .

*A choisit un entier aléatoire a et transmet $\propto^a$ à B .

*B choisit un entier aléatoire b et transmet $\propto^b$ à A .

A et B peuvent donc calculer $\propto^{ab}$ qui est leur clé secrète partagée, Diffie et Hellman proposent le groupe $(F_q)^*$ multiplicatif du corps fini $F_q$ de caractéristique le nombre premier p .

Si quelqu'un a espionné leur échange , il connaît G , $\propto$, $\propto^a$,$\propto^b$ .

Pour pouvoir calculer $\propto^{ab}$ il faut pouvoir calculer a ou b, c'est ce qu'on

appelle «résoudre le problème du logarithme discret sur le groupe fini G», problème réputé difficile de théorie des nombre .

## III-2/ Exemples de Cryptosystème :

1/Cryptosystéme RSA :

Le destinataire Bob choisit deux entiers N et E tels que $N = p \times q$ , p et q étant deux entiers premiers grands ,E est compris entre 0 et $\varphi(N)$ qui est le cardinal du groupe multiplicatif $(Z/NZ)^*$ .

*Bob calcule l'entier d , $d \in [0 , \varphi(N)]$, tel que : $Ed \equiv 1 \bmod \varphi(N)$ , il diffuse les entiers N et E mais garde secret p, q et d .

Alice veut envoyer un message secret à Bob , elle convertit le message en un élément m du groupe $(Z/NZ)^*$.

*Pour le chiffrer , elle calcule $c \equiv m^E \pmod N$ qu'elle transmet à Bob .

*Bob reçoit c et calcule $c^d \pmod N$, il obtient: $c^d \equiv (m^E)^d \pmod N \equiv m \pmod N$ .

La sécurité du RSA repose sur la difficulté à factoriser le nombre N, c'est à dire le décomposer en produits de nombres premiers . Si l'opération est relativement simple avec de petits nombres (233929 par exemple se décompose en 449×521) , elle est particulièrement ardue avec des nombres de 100 à 200 chiffres comme ceux couramment utilisés . Dans le système RSA, la clé secrète est fabriqué à partir de deux grands nombres

premiers, alors que la clé publique ne révèle que leur produit .

Pour casser le RSA , une des méthodes élégante de factorisation est la factorisation par courbe elliptique du à Lenstra 1985 , qui est basée sur celle de Pollard .

2/ Cryptosystéme d'El Gamel :

*Bob le destinataire choisit un grand nombre premier p ainsi qu'un générateur g du groupe multiplicatif $(F_p)^*$ ; Il choisit un entier $b \in [1,p-2]$ et calcule $B = g^b$ , il publie les entiers p, g et B et garde secret b .

*Pour chiffrer un message m du groupe $(F_p)^*$ , Alice choisit un entier k et calcule $K = g^k$ ainsi que $c = m \times B^k \pmod p$ , elle envoi le couple (K,c) à Bob ( il est important que k soit choisit grand au hasard) .

*Bob peut retrouver le message en calculant $Ck^{-b} \pmod p$ ; en effet :

$$cK^{-b} \equiv m \times B^k \times (g^k)^{-b} \pmod p$$

$$\equiv m \times (g^b)^k \times (g^k)^{-b} \pmod p$$

$$\equiv m \pmod p .$$

La sécurité de ce système est liée au problème du logarithme discret .

3/Cryptosystéme utilisant les courbes elliptiques :

Le problème du logarithme discret a son homologue naturel dans le cas des courbes elliptiques .

Soit E une courbe elliptique sur un corps fini $F_p^m$, et soit P un point

d'ordre h sur E ; le problème du logarithme discret sur E est celui de trouver, étant donné un point A du sous groupe engendré par P, l'entier a tel que aP = A.

On utilise dans ce cryptosystéme la méthode suivante :

*Le destinataire Bob choisit un entier b ($b \in [0, h-1]$ ) et diffuse la valeur du produit B = bP .

*L'expéditeur Alice peut alors chiffrer un message $M = (x_M , y_M)$ de la manière suivante : elle choisit un entier secret $k \in [0 , h-1]$ et calcule $K = kp$ , $kB = (x_{kB} , y_{kB})$ , elle transmet à Bob les données (K , c) où $c = (x_M x_{kB} , y_M y_k)$ .

A la réception , Bob peut trouver M en calculant $bK = (x_{bK} , y_{bK})$ et $M = (x_c x^{-1}_{bK} , y_c y^{-1}_{bK})$ .

**III-3/Cryptosystéme utilisant les courbes hyperelliptiques :**

Le cryptosystéme sur les courbes elliptiques se généralise aux courbes hyperelliptiques en remplaçant les points de la courbe elliptique par les diviseurs de la jacobienne de la courbe hyperelliptique .

**III-3-1 /Cardinal de la jacobienne d'une courbes hyperelliptique :**

La connaissance du cardinal exact d'un groupe est nécessaire si l'on veut construire un Cryptosystème . En effet afin de garantir une bonne sécurité, le cardinal de la jacobienne , noté $\#J(K)$, devrait être divisible par un

nombre premier d'au moins 45 chiffres décimaux .

**Définition 1 :**

Soit C une courbes hyperelliptique définie sur le corps fini $F_q$ ($q = p^n$ , p étant un nombre premier), et soit $F_q^r$ une extension de degré r du corps $F_q$ , et $M_r$ le nombre de points $F_q^r$ – rationnels de C .

La fonction zeta de C est définie par : $Z_C(t) = \exp(\sum_{r\geq 1} M_r t^r /r)$ .

**Théorème 2 :**

Soit C une courbe hyperelliptique de genre g définie sur le corps $F_q$ , et soit $Z_C(t)$ la fonction zeta de C ; alors

$\leftarrow Z_C(t)$ est une fonction rationnelle de la forme :

$$Z_C(t) = P(t) / (1 - t) (1 - qt)$$

où P(t) est un polynôme de degré 2g , de plus P(t) s'écrit sous la forme :

$P(t) = 1+a_1t+\ldots+a_{g-1}t^{g-1}+a_gt^g+qa_{g-1}t^{g+1}+q^2a_{g-2}t^{g+2}+\ldots+q^{g-1}a_1t^{2g-1}+q^gt^{2g}$ .

$\uparrow$P(t) peut se factoriser en $P(t) = \prod(1-\alpha_i t) (1-\overline{\alpha_i} t)$ où chaque $\alpha_i$ est le nombre complexe de valeur absolue $\sqrt{q}$ ,et $\overline{\alpha_i}$ est le conjugué de $\alpha_i$ .

$\rightarrow$ Le cardinal de la jacobienne sur $F_q^r$ , noté $N_r$ , satisfait l'égalité :

$$N_r = \prod|1-\alpha_i^r|^2$$

Pour calculer $N_r$ ,il suffit de déterminer les coefficients $a_1,\ldots ,a_g$ de P(t) ; ensuite factoriser P(t) pour obtenir les $\alpha_i$ , et enfin calculer $N_r$ à partir de l'expression $N_r=\prod|1-\alpha_i^r|^2$ .

La formule ← définissant la fonction $Z_C(t)$ entraîne la formule :

$$P(t) = (1 - t)(1 - qt)Z_C(t) .$$

Prenons les logarithmes des deux membres , et dérivant par rapport à t pour obtenir

$$P'(t)/P(t) = \sum_{r\geq 0} (M_{r+1} - 1 - q^{r+1}) t^r .$$

En identifiant les coefficients de $t^0, t^1, \ldots, t^{g-1}$ des deux membres de l'égalité précédente , nous obtenons les premières g valeurs $M_1, M_2, \ldots, M_g$ qui suffisent pour déterminer les coefficients $a_1, \ldots, a_g$ , et donc $N_r$ pour tout r .

Cas particulier : (g = 2)

Pour calculer le cardinal de la jacobienne d'une courbe hyperelliptique de genre 2 , nous suivons les étapes suivantes :

1/ On calcule $M_1$ et $M_2$ .

2/Les coefficients de $Z_C(t)$ sont donné par : $a_1 = M_1 - 1 - q$

et $a_2 = (M_2 - 1 - q^2 + a_1^2)/2$

3/On résoud l'équation quadratique $x^2 + a_1 x + (a_2 - 2q) = 0$, pour obtenir deux solutions $\gamma_1$ et $\gamma_2$ .

4/On résoud $x^2 - \gamma_1 x + q = 0$ pour obtenir une solution $\alpha_1$ , et résoudre $x^2 - \gamma_2 x + q = 0$ pour obtenir une solution $\alpha_2$ .

5/ On calcule $N_r = |1 - \alpha_1^r|^2 . |1 - \alpha_2^r|^2$ .

**Corollaire 3:**

Soit C une courbe hyperelliptique de genre g définie sur un corps fini $F_q$,

Alors

*Le nombre de points sur la courbe est borné par

$$| \#(C) - (q+1)| \leq 2g\sqrt{q} .$$

*Le cardinal de sa jacobienne est quand à lui borné par

$$(\sqrt{q} - 1)^{2g} \leq \#J(F_q) \leq (\sqrt{q} + 1)^{2g} .$$

*Soit $F_q^r$ une extension du corps $F_q$ , alors

$$(q^{r/2} - 1)^{2g} \leq \#J(F_q^r) \leq (q^{r/2} + 1)^{2g} .$$

Ainsi , $\#J(F_q^r) \approx q^{rg}$ .

**III-3-2/ Endomorphisme de Frobenius :**

Soit C une courbe hyperelliptique définie sur $F_q$ et $(F_q)^{alg}$ une clôture algébrique de $F_q$ .

**Définition 4 :**

L'endomorphisme de Frobenius , noté $\phi$, est l'automorphisme du corps $(F_q)^{alg}$ laissant fixe $F_q$ , défini par $\phi(x) = x^q$ .

Cette application se prolonge aux points P =(x , y) de la courbe C , par transformation des coordonnées x et y de P , elle se prolonge aussi aux diviseurs par action sur ses points .

Remarque :

Un diviseur est bien défini sur $F_q$ si et seulement s'il est invariant sous l'action de Frobenius .

**Proposition 5 :**

L'endomorphisme de Frobenius $\phi$ possède un polynôme caractéristique de degré 2g avec des coefficients entiers .

En genre 2 , le polynôme caractéristique est de la forme :

$$\chi(t) = t^4 - s_1 t^3 + s_2 t^2 - s_1 q t + q^2 ,$$

avec $\chi(\phi)$ est l'application identité sur tout le groupe *J* : pour tout diviseur D de *J* : $\phi(D)^4 - [s_1]\,\phi(D)^3 + [s_2]\,\phi(D)^2 - [s_1 q]\,\phi(D) + [q^2].D = \theta$ ,

où $|s_1| \leq 4\sqrt{q}$ et $|s_2| \leq 6q$ .

Relations entre l'endomorphisme de Frobenius et le cardinal de C ainsi que sa jacobienne *J* :

L'endomorphisme de Frobenius est relié au nombre de points de la courbe C et le nombre des diviseurs dans la jacobienne *J* sur le corps fini $F_q$ , en effet : connaître le polynôme $\chi$ est équivalent à connaître le cardinal de C sur les extension $F_q^i$ de $F_q$ pour $1 \leq i \leq g$ .

**Théorème 6 :**

Soit C une courbe hyperelliptique de genre 2 sur le corps $F_q$ .

Les cardinaux de la courbe C sur $F_q$ , $F_q^2$ sont

$$\#C(F_q) = q - s_1 \quad \text{et} \quad \#C(F_q^2) = q^2 - s_1^2 + 2s_2 .$$

Le cardinal de la jacobienne est borné par

$$q^2 - 4q^{3/2} + 6q - 4q^{1/2} \leq \#J(F_q) \leq q^2 + 4q^{3/2} + 6q + 4q^{1/2} + 1 .$$

La sécurité de ce système repose sur la difficulté du problème du logarithme discret .

**III-3-2/ Problème du logarithme discret hyperelliptique :**

**Définition 7 :**

Le problème du logarithme discret hyperelliptique pris sur une courbe hyperelliptique de genre g donné est le suivant :

Etant donné un élément $D_1$ de la jacobienne , d'ordre n, et un élément $D_2$ du sous groupe engendré par $D_1$ , le problème est de fournir un nombre $\lambda$ modulo n tel que : $D_2 = \lambda D_1$ .

Réduction de Pohling-Hellman :

Pohling et Hellman ont ramené le problème du log discret dans un groupe cyclique G d'ordre quelconque à des problème de log discret dans des sous groupes d'ordre premier divisant l'ordre du groupe initial .

Une conséquence de cette réduction est que si l'ordre du groupe ne contient pas de grand facteur premier , alors le calcul du log discret est facile .

Remarque :

Il existe d'autres méthodes pour résoudre ce problème difficile de la théorie des nombres , telles que la méthode en racines carré , méthode de

Rho due à Pollard …

Quand le groupe G est jacobienne d'une courbe hyperelliptique , il existe toujours des attaques d'un cryptosystéme sur les courbes hyperelliptiques qui reviennent à la résolution du probléme du log discret .

Attaque de Frey et Rück :

Les courbes elliptiques supersingulières sont plus faciles que les courbes elliptiques quelconques , à cause d'une attaque dite réduction MOV, du nom de ses auteurs Menzes , Okamoto , Vanstone . Cette attaque a été généralisée à des courbes de genre supérieure par Frey et Rück en 1994 . Cet algorithme réduit le problème du log discret dans la jacobienne $J(F_q)$ à un problème de log discret dans le groupe multiplicatif d'une extension $F_q^r$ de $F_q$ de degré r qui est le plus grand facteur de $\#J(F_q)$ .

La réduction de Frey et Rück est basée sur le couplage de Tate qui consiste à évaluer une fonction rationnelle R en un diviseur de $J$ .

Remarque :

Il existe d'autres méthodes pour résoudre ce problème telles que l'attaque par descente de Weil , l'attaque par calculs d'indices …

Exemple :

```
> p:=100000007;
> P<x>:=PolynomialRing(GF(p));
> C:=HyperellipticCurve(x^5+456*x^4+98*x^3+76*x^2+54*x+32);
> J:=Jacobian(C);
> #J;
10001648178050390
> time;
Time: 0.000
> FactoredOrder(J);
[ <2, 1, 5000824089025195>, <5, 1, 2000329635610078>, <17, 1,
588332245767670>,

<58833224576767, 1, 170> ]
> D:=Random(J);
> D;
(x^2 + 78461722*x + 3242251, 68440275*x + 12788255, 2)
> Order(D);
1000164817805039
> K:=GF(p);
> Frobenius(D,K);
(x^2 + 78461722*x + 3242251, 68440275*x + 12788255, 2)



> p:=NextPrime(6452);
> p;
6469
> K:=GF(p);
> P<x>:=PolynomialRing(GF(p));
> C:=HyperellipticCurve(x^5+125*x+542);
> J:=Jacobian(C);
> D:=Random(J);
> Order(D);
20917918
> Frobenius(D,K);
(x^2 + 3296*x + 5423, 3027*x + 2457, 2)
> ZetaFunction(C);
(41847961*$.1^4 - 19407*$.1^3 + 7284*$.1^2 - 3*$.1 + 1)/(6469*$.1^2 - 6470*$.1 +

   1)
> time;
Time: 0.000
```

## Quelques notations et abréviations utilisées :

$K^{alg}$ : Clôture algébrique du corps K .
g : Le genre d'une courbe hyperelliptique C .
K[C] : L'ensemble des polynômes à une indéterminée u sur le corps K .
K[u,v] : L'ensemble des polynômes à deux indéterminées u etv sur le corps K .
L : Extension du corps K .
C(L) : L'ensemble des points P de L×L satisfaisant l'équation de C.
$C(K^{alg})$ : La courbe C .
$\overline{P}$ : Le point opposé de P .
$K^{alg}[C]$ : L'ensemble des fonctions polynomiales sur C .
G : Fonction polynomiale sur C.
$\overline{G}$ : Le conjugué de la fonction G .
N(G) : La norme de la fonction G .
$deg_P(G)$ : Le degré de la fonction G en P .
ord(G) : L'ordre de la fonction G .
$K^{alg}(C)$ : L'ensemble des fonctions rationnelles de C .
R : Fonctions rationnelle .
U : L'uniformisante d'une fonction rationnelle en un point P .
*D* : L'ensemble des diviseurs d'une courbe hyperelliptique .
$D^0$ : L'ensemble des diviseurs de degré 0 d'une courbe hyperelliptique.
*P* : L'ensemble des diviseurs principaux d'une courbe hyperelliptique.
supp(D) : Support d'un diviseur D .
div(a,b) : Représentation de Mumford d'un diviseur D .
| D | : La norme d'un diviseur D .
*J* : Jacobienne d'une courbe hyperelliptique .
# $J(F_q)$ ,($q = p^n$ , p premier) : Cardinal de la Jacobienne d'une courbe hyperelliptique définie sur $F_q$ .
$Z_C(t)$ : La fonction zeta d'une courbe hyperelliptique .
$\phi$ : L'endomorphisme de Frabenius du corps $(F_q)^{alg}$ .
$\chi$ : Le polynôme caractéristique de l'endomorphisme de Frobenius .

# Références

[Can 87] D.Cantor , computing in the jacobian of a hyperelliptic curve, math of comp . vol 48 , N° 177, January 1987 , 95-101 .

[DH 76] W.Diffie and Hellman, New direction in cryptography , IEEE Transactions on information theory – vol .IT-22,N° 6 , Nov 1976 , 644-654.

[ElG 85] T- ElGamel , A public key cryptosystem and a signature scheme based on discret logarithm , IEEE Transactions on information theory – vol .IT-31,N° 4 , Nov 1985 , 469-472.

[Ful 69] W. Fulton , Algeraic curves , Benjamin , New York , 1969 .

[Gau 00a] P . Gaudry , An algorithm for solving the discret logarithm problem over hyperelliptic curve , Advances in Cryptology – EUROCRYP 2000 , Springer-Verlag , LNCS 1807, 19 –34 .
**http://www.lix.polytechnique.fr/Labo/publis/euro2K.ps.gz**.

[Gau 00b] P . Gaudry , Algorithmique des courbes hyperelliptiques et applications à la cryptologie PhD .Thesis , 2000 .
**http://www.lix.polytechnique.fr/Labo/Pierrick . Gaudry /publis/thesis . Final .ps.gz .**

[GH 00] P . Gaudry and R. Harly, Counting points on hyperelliptic curves over finite fields, ANTSIV 2000,Springer-Verlag ,LNCS1838,313-332 , 2000©Springer-Verlag .
**http://www.lix.polytechnique.fr/Labo/publis/ant IV.ps.gz**.

[MWZ 96] A. Menzes , Y. Wu ,et R. Zucchecoto , An elementary introduction to hyperelliptic curves, Technical report CORR 96-19 , Departement of
C &O, University of Waterloo , Ontario , Canada , November 1996 .

[PH 78] S. Pohling and M.Hellman , An improved algorithm for computing logarithms over GF(p) and its cryptographic significance , IEEE Transactions on information theory – vol .IT-24(1978) , 106-110 .

[PWGP 03 ]J. Pelzl , T.Wollinger , J. Guajardo , and C. Paar, Hyperelliptic Curve Cryptosystems : Closing the Performance Gap to Elliptic Curve . (2003) .
**http://Venona.antioffline .com/2003 / 026.pdfz**.