N° d'ordre: 29/2008-M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIEN

Faculté des Mathématiques

THESE

Présentée par Mr KHELIFI Fouad Mohssen

Pour l'obtention de MAGISTER
En :MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

SUJET

Arithmétique des Courbes Elliptiques

E(t,m) : $y^2+2(t-1)xy=x^3-(t-1)^2x^2-3mx-m \in Q[x,y]$ $m \neq 0$, $\frac{1}{4}$

application en Cryptographie

Soutenue le: .....15/05/2008.....devant le jury composé de :

Mr AIDER Meziane	Professeur à l'U.S.T.H.B ,	Président
Mr ZITOUNI Mohamed	Professeur à l'U.S.T.H.B	Directeur de Thèse
Mr BENKAFADAR M/,	Professeur à l'Université de Constantine	Examinateur
Mr NOUALI Omar	Docteur d'état ,maître de recherche au CERIS	Examinateur
Mr HERNANE Mohand Ouamar	M de C, à l'U.S.T.H.B	Examinateur
Mr FERTASSI	Directeur Du centre de recherche CFN	Invité
Mr DJALEL	Directeur R , DRSM BLIDA	Invité

Remerciements

Je tiens tout d'abord à exprimer mes plus sincères remerciements et ma gratitude à mon Directeur de thèse Monsieur Mohamed ZITOUNI Professeur à l'USTHB de m'avoir proposé ce sujet et pour m'avoir guidé tout le long de la réalisation de cette thèse.

Je remercie spécialement Monsieur AIDER Meziane Professeur à l'USTHB pour l'honneur qu'il m'a fait en présidant mon jury de soutenance .

J'adresse également mes remerciements à Monsieur Le Professeur BENKAFADAR Mohamed de l'Université Mentouri de Constantine , à Monsieur NOUALI Ouamar Docteur d'état et Maître de recherche au CERIST ,et Monsieur HERNANE Mohand Ouamar Docteur d'état et Maître de Conférences à l'USTHB , pour avoir accepté d'examiner ce travail.

Je remercie chaleureusement Monsieur FERTASSI Directeur du Centre de recherche CFN et Monsieur DJALEL Directeur Régional à Blida d'avoir accepté mon invitation.

Son oublier mes Professeurs Monsieur HECHAICHI et Monsieur BENZAGHOU BEN ALI .

Dédicace

Je dédié cette thèse :

A ma petite fille AYA FATIMA ZOUHRA

A Celle qui m'a tant aidé et soutenu durant toute ma vie ma chère douce mère .

A mon père Laid qui a toujours était fièr de moi .

A ma femme Hanafi -M -.

A toute ma famille, la famille KHELIFI et la famille HANAFI.

Et à tous mes nombreux amis .

Table des matières

Introduction

La théorie des Courbes Elliptiques est liée à la Géométrie Algébrique, à la Théorie des Nombres, à l'Analyse Complexe selon Hartshorne [6] , Cassels [4] ; Shafarevich [21] , J-H-Silverman [23] .

Les Courbes Elliptiques sur les corps finis sont utilisées en Cryptographie, en Cryptologie, en codage pour trouver des clés inviolables de messages, des algorithmes de complexité, des certificats de sécurité .De nombreux exemples sont mis à la disposition des chercheurs sur les sites Internet.

Dans ma thèse de magister l'étude des Courbes Elliptiques est limitée aux structures algébriques de Variétés et de groupes. Elle est répartie sur cinq chapitres : I- Eléments de Géométrie Algébrique, II- Courbes Algébriques planes, III- Cubiques de Weierstrass Courbes Elliptiques, IV- Groupe de Mordell -Weil , et V- Courbes Elliptiques sur les corps finis .

Dans ce domaine des Courbes Elliptiques il y a encore les espaces homogènes , les groupes de Châtelet-Weil,de Schafarevich -Tate , de Selmer , les réseaux complexes , les formes modulaires et les Courbes Modulaires , les descentes , les rangs , les conducteurs , la fonction L(E;s) de Dirichlet-Hasse , la conjecture de Birch et Swinerton-Dyer que j'étudierai après le magister.

Chapitre I : Eléments de Géométrie Algébrique.

1-**Espaces affines $IA^n(K)$ sur un corps** [21] et , [6].

Soit un corps commutatif K algébriquement clos et un entier n / 1

Définition 1 : *un n- espace affine sur un corps K est l'ensemble des n-uples d'éléments a_i du corps* K *:/*A^n *(K)* $= \{a = (a_1, \ldots, a_n),\ a_i \in K\}$.

a est un point de cet espace ;les éléments a_i sont les coordonnées du point a.

L'espace affine /A^n(K) contient des points particuliers :les zéros des polynômes f de l'anneau K [$X_1, X_2 \ldots\ldots, X_n$] à n indéterminées

Définition 2*: un sous ensemble X de l'espace affine IA^n (K) est algébrique si ses points sont des zéros d'une famille de polynômes de l'anneau* K [$X_1, X_2 \ldots\ldots, X_n$] :

$$X = \{a \in IA^n(K),\ f_i(a) = 0;\ i = 1,..,t \ \ et\ f_i \in K[X_1 X_2 ....,X_n]\ \}$$

Exemple

Dans l'espace affine /A^2 (x) , le sous ensemble

X= $\{a \in IA^n(\mathrm{C}),\ f_i(a) = 0,\ f_1(x,y) = x^2 + y^2 - 4\}$ est un ensemble algébrique.

Alors $X = \{(t, \sqrt{(4 - t^2)}), t \in C\}$

Les propriétés des ensembles algébriques sont déterminées par la

Proposition 1:

Soit dans l'espace affine IA^n (K) les ensembles algébriques $\{X_i\}_i$. Alors :

1) *la réunion de ces ensembles est un ensemble algébrique.*

2) *l'intersection d'une famille finie d'ensembles algébriques est un ensemble algébrique.*

3) *l'ensemble vide et l'espace affine sont algébriques.*

Preuve

1) Soient deux ensembles algébriques

$X_1 = \{a \in IA^n(K),\ f_i(a) = 0 \ ,\ f_i \in K[x_1,.....,x_n]\}$ et

$X_2 = \{b \in IA^n(K), g_t(b) = 0, g_t \in K[x_1,.....,x_n]\}$.

Alors leur réunion $X_1 \cup X_2$ est l'ensemble des zéros des polynômes f_i et g_t ; cet ensemble est donc algébrique.

2)Soit une famille finie $\{X_1 ..... X_d\}$ d'ensembles algébriques; alors l'intersection $\bigvee_{1 \le i \le d} X_i$ est l'ensemble des zéros communs des polynômes associes aux ensembles $X_1 ..... X_d$.

3) Le polynôme constant $f=1+0x_1+0x_2+...+0x_n \in K[x_1,...,x_n]$, n'admet pas de zéros; donc il lui correspond l'ensemble vide ;le polynôme identiquement nul $f=0x_1+0x_2+...+0x_n$, admet tous les points de l'espace affine $IA^n(K)$ comme zéros ; donc l'espace affine $IA^n(K)$ est algébrique.

o

Ces propriétés des ensembles algébriques sont semblables aux propriétés des fermés d'une topologie.

Les ensembles algébriques d'un espace affine $IA^n(K)$ permettent de définir une topologie particulière :

Définition 3 :*la topologie de Zariski sur l'espace affine $IA^n(K)$ est constituée par les ensembles algébriques comme ensembles fermés et leurs complémentaires comme des ouverts. Cette topologie n'est pas de Hausdorff (Exemple 1-1-1 Hartshorne).*

Donc l'espace affine devient un espace topologique avec la topologie de Zariski.

Définition 4 **:***un sous ensemble X d'un espace topologique* IA^n *(K) est irréductible s'il n'est pas vide et s'il n'est pas la réunion* $X=X_1 \cup X_2$ *de deux sous ensembles fermés non vides disjoints; l'ensemble vide est un ensemble non irréductible***.**

Dans l'espace topologique IA^n (K) il y a des ensembles particuliers,

2-Varietes Algébriques affines

Définition 5 : 1) *une Variété Algébrique affine est un sous ensemble d'un espace topologique* IA^n (K), *fermé et irréductible.*

2) *une Variété Algébrique quasi affine d'un espace topologique* IA^n (K) *est un sous ensemble ouvert d'une Variété affine.*

3) *une sous Variété Algébrique affine est une partie irréductible et fermée X d'une Variété Algébrique affine de* IA^n (K) .

A une Variété Algébrique affine X est associé son idéal *;*

l'idéal d'une Variété Algébrique affine X d'une Variété est l'ensemble des polynômes f:

$$I(X)=\{ f\in [x_1,x_2,\ldots,x_n] , f(a)=0 \text{ pour tout } a \in X \}$$

Exemples

1)Soit un polynôme $f\in K[x,y]$, irréductible , de degré d ; alors f engendre un idéal premier dans l'anneau $K[x,y]$, l'équation $f(x,y)=0$ définit une Courbe algébrique affine de degré d.

2) un polynôme $f\in K[x,y,z]$ irréductible, de degré d définit une surface algébrique affine.

3)un polynôme $f \in K[x_1,x_2,.....,x_n]$, n >3 irréductible, définit une hypersurface algébrique affine .

En tant qu'espace topologique, une Variété Algébrique affine possède une dimension.

Définition 6 : *la dimension d'une Variété affine, ou quasi affine X est l'entier n maximal dans la chaîne* $X_1 \subset X_2 \subset X_3 \subset \ldots\ldots \subset X_n \subset \ldots\ldots \subset X$ *de sous ensembles fermés irréductibles* $X_1, X_2, \ldots\ldots, X_n$.

Exemples

1- $/A^n$ (K) pour n=1,2,3,.... est une Variété affine de dimension n;

2 - La dimension de l'espace $/A^2$ est égale à 2.

3)Variétés projectives Algébriques

On construit une Variété projective IP^n (K). à partir d'une Variété affine et d'une relation d'équivalence; Dans l'ensemble des (n+1)-uples ($x_1,x_2,\ldots,x_{n+1}$) d'éléments non tous nuls d'un corps K , nous considérons la relation R binaire définie par la formule :

a R b si et seulement si $a=\lambda b$ pour un certain élément non nul λ du corps K

$(x_1, x_2,..., x_{n+1}) R (\lambda x_1, \lambda x_2,..., \lambda x_{n+1})$ pour un élément $\lambda \in K^*$

Alors cette relation R satisfait les axiomes d'une relation d'équivalence : réflexive , symétrique et transitive; l'ensemble quotient implique la :

Définition 7 *: l'ensemble quotient de l'espace affine* $IA^{n+1}(K)$ - á0â *par cette relation R est l'espace algébrique projectif* $IP^2(K)$*:*

$$IP^2(K) = IA^{n+1}(K) - \{(0,0,\ldots,0\} / R.$$

Chaque classe d'équivalence est un ensemble de points de coordonnées $a=(a_1,a_2,\ldots,a_{n+1})$.

Il en résulte la structure des classes :

$$cl(a_1,a_2,\ldots,a_{n+1}) = \{(a_1,a_2,..,a_{n+1}),(\lambda a_1,\lambda a_2,..,\lambda a_{n+1}),(ta_1,ta_2,....,ta_{n+1}),...\}.$$

Exemples

1) L'espace projectif IP^1 (IR) :

$$cl(1,1) = \{(1,1),(-1,-1),(3,3),(6,6),...(x;x) \quad x \in I\mathrm{R}^*\}.$$

2) L'espace projectif IP^2 (IR) :

$$cl(0,1,0) = \{(0,1,0),(0,-1,0),(0,2,0),(0,-2,0),...\};$$

cette classe joue le rôle de point à l'infini pour les Cubiques planes. L'espace projectif peut donc être représenté par l'ensemble des droites passant par l'origine.

Les notions d'ensemble algébrique, de topologie de Zariski d'un espace affine se prolongent aux espaces projectifs.

Définition 8 : *un sous ensemble Y d'un espace projectif IP^n (K) est algébrique s'il est l'ensemble Z(T) des zéros d'une famille T de polynômes homogènes de l'anneau $K[x_1,x_2,...,x_{n+1}]$.*

Ces notions permettent de définir des Variétés projectives et des Variétés quasi projectives

Définition 9 :**1)** *une Variété Projective est un sous ensemble algébrique fermé d'un espace projectif IP^n (K) muni de la topologie de Zariski;*

2)*une Variété quasi projective est un sous ensemble ouvert d'une Variété Projective*.

Exemple

Le polynôme homogène Cubique:

$F(x,y,z)=y^2z+3xyz-x^3-4x^2z+5z^3 \in K[x,y,z]$ définit une Variété Projective de dimension un lorsque le polynôme f est irréductible ; la Variété est de dimension 0 lorsque le polynôme f est réductible.

La construction d'un espace projectif $IP^n(K)$ à partir d'un espace affine $IA^{n+1}(K)$ implique des formules de passage d'un espace à un autre .

(1) Déterminons les formules de passage de l'espace affine IA^2 au plan projectif IP^2.

Prenons une Cubique C d'équation affine :

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6; \qquad (1)$$

le changement de variables

$$x=\frac{X}{Z} \quad , \quad y=\frac{Y}{Z} \qquad (2)$$

transforme (1) en polynôme en $\frac{Y}{Z}$ et $\frac{X}{Z}$:

$$f\left(\frac{X}{Z},\frac{Y}{Z}\right)=\left(\frac{Y}{Z}\right)^2+a_1\left(\frac{XY}{Z^2}\right)+a_3\frac{Y}{Z}-\left(\frac{X}{Z}\right)^3-a_2\left(\frac{X}{Z}\right)^2-$$

$$-a_4\left(\frac{X}{Z}\right)-a_6 \qquad (3)$$

Multiplions (3) par Z^3;

$$Z^3 f(X,Y,Z)=g(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-$$

$$-a_2ZX^2-a_4XZ^2-a_6Z^3 \qquad (4)$$

Le polynôme g est homogène , de degré 3 , dans le plan projectif IP^2

(2) Formules de passage de $IP^2(K)$ à $IA^2(K)$

Prenons une Cubique C , d'équation homogène (4) , dans le plan IP^2

Le changement de variables

$$X = x \ , \ Y = y \ , \ Z = 1 \qquad (5)$$

transforme le polynôme homogène g en un polynôme affine f.

$$g(x, y, 1) = y^2 + a_1xy - a_3y - x^3 - a_2x^2 - a_4x - a_6 = f(x, y) \qquad (1)$$

Application à la famille de Cubiques de Weierstrass .

$$E\acute{Y}t, m\text{þ} \quad y^2 + 2(t-1)xy = x^3 - (t-1)^2x^2 - 3mx - m \quad \in Q[x, y],$$

Ces Cubiques sont dans le plan affine $IA^2(Q)$

Avec les formules de passage (2) j'obtiens un polynôme homogène dans le plan projectif IP^2

$$E\acute{Y}t, m\text{þ} \ : \ Y^2Z + 2(t-1)XYZ = X^3 - (t-1)^2X^2Z - 3mXZ^2 - mZ^3;$$

4-Variétés Algébrique Abéliennes ([7] 3-21 ,4-10-2,6-10-13)

Nous étudions de nouveaux types de Variétés Algébriques.

Définition 10: ***1)****une Variété Abélienne est une Variété de groupe complète projective .*

2)*Une Variété Algébrique est complète si elle est de type fini sur un corps algébriquement clos*

3)*une Variété de groupe est une Variété Algébrique X munie d'un morphisme u:* $X^2 \longrightarrow X$ *tel que l'application inverse* $u^{-1} : x \to x^{-1}$ *est un morphisme de cette Variété .*

Exemples

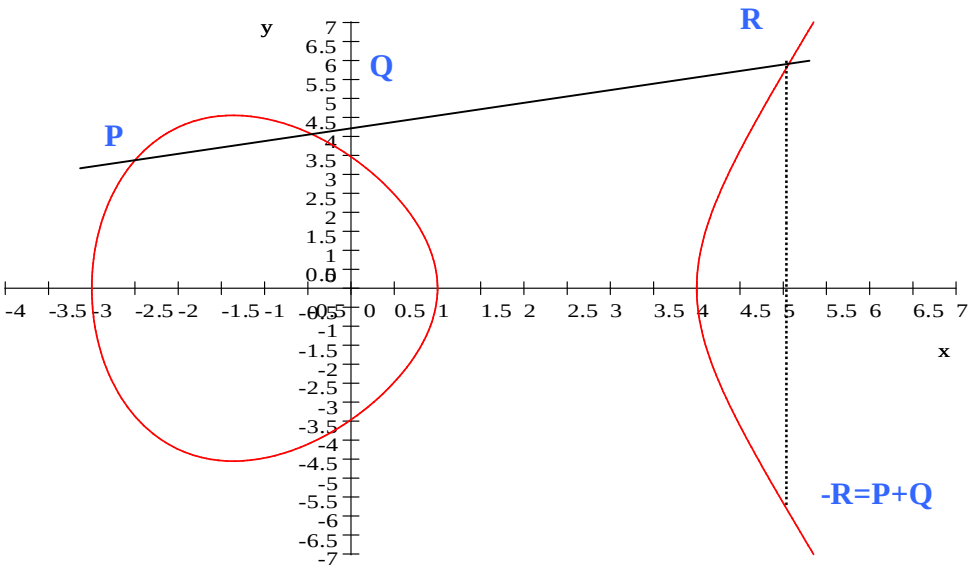
1) morphisme u de valeur u(a,b)=a+b pour un groupe additif ;

2) morphisme u de valeur u(a,b) = ab pour un groupe multiplicatif ;

3) Cubique de Weierstrass;

C: $y^2z + a_1xyz - a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \in IP^2[K]$

L'ensemble C(K) des points K-rationnels possède une structure de groupe abélien additif de type fini; il en résulte que C est une Variété Abélienne. Sur la figure suivante , la somme de deux points P+Q est le point -R symétrique de l'intersection R de la sécante PQ et de la Cubique C. *Le tracé de la Cubique d'équation* $y^2 = x^3 - 2x^2 - 11x + 12$ *avec le logiciel S-W-Place.*



O_E =(0,0)=(∞,∞) est le point à l'infini;c'est l'élément neutre de l'addition

(P,Q) ⟶ P+Q

Ce point est déterminé par la direction de l'axe Oy.

5-Diviseurs d'une Courbe Algébrique plane ([7] 6-11)

Il y a plusieurs manières de définir un diviseur en Géométrie Algébrique. Considérons une Courbe projective non singulière dans le plan projectif $IP^2[K]$. Chaque ligne L coupe C en un nombre fini de points ; le nombre de ces points comptés avec leurs multiplicités, est égal au degré de la Courbe C.

Définition 11 *:1)un diviseur d 'une Courbe projective lisse X est une somme formelle D =* $\sum_i n_i(P_i)$, *où les* n_i *sont des entiers rationnels et les* P_i *des points de X.*

2)*le degré de ce diviseur est l'entier rationnel degD =* $\sum_i n_i$.

Lorsque L varie ,nous obtenons une famille de diviseurs de C.

L'ensemble Div (C) des diviseurs de C peut être muni d'une loi de groupe abélien avec les opérations : D = $\sum_i n_i(P_i)$; et D' = $\sum_i n`_i(P_i)$

la somme D'+D= $\sum_i (n_i+n'_i)(P_i)$, le symétrique -D = $\sum_i(-n_i)(P_i)$ et le diviseur nul O= $\sum_i O(P_i)$

Il existe plusieurs types de diviseurs.

Définition 12 **1)** *un diviseur premier d'une Courbe projective C est de la forme D=(P) , pour tout point P de C*

2)*un diviseur de Weil est un élément du groupe abélien libre Div C engendré par les diviseurs premiers ,*

3) *un diviseur effectif sur C est de la forme D=* $\sum_i n_i (P_i)$ *pour* n_i μ 0;

4)*un diviseur principal est un diviseur (f) d'une fonction non nulle f*∈ *K* .*

Il existe une relation d'équivalence dans le groupe Div(X)

Définition **13** :*dans le groupe Div(X) des diviseurs d'une Variété X , deux diviseurs D et D' sont linéairement équivalents si leur différence est un diviseur principal : D-D'=(f)*

L'ensemble Prin(C) des diviseurs principaux d'une Courbe projective C forme un sous groupe du groupe abélien $Div(C)$

Le groupe quotient Div(C)/Prin(C) = cl (C) est le groupe des classes des diviseurs de C.

Proposition 2

Le degré d'un diviseur principal d'une Courbe Algébrique C non singulière est égal à 0.

Preuve :[7]. 6-10.

o

Exemple

Cubique de Weierstrass C non singulière , son point à l'infini O_E et une sécante L qui coupe C en trois points simples P_1 ,P_2 ,P_3.

Alors la somme des diviseurs des trois points est linéairement équivalente à trois fois le diviseur du point à l'infini O_E :$(P_1)+(P_2)+(P_3) \approx 3(O_E)$.

Chapitre II Courbes Algébriques Planes

Nous utilisons les références [2],[6],[20],[25],[29].

1- Degré d'une Courbe Algébrique plane.

Une Courbe Algébrique plane est l'ensemble des points P=(x,y) qui satisfont un polynôme $g(x,y) \in K[x,y]$; K étant un corps commutatif, algébriquement clos ou non

C: $g(x,y) = 0$, $g \in K[x,y]$ (1)

Tout polynôme g(x,y) de degré n µ 1 se met sous la forme

$g(x,y) = g_n + g_{n-1} + \ldots + g_1 + g_0$ (2)

les $g_d = g_d(x,y)$ sont des polynômes homogènes en x,y de degré d :

$$g_d(x,y) = a_1x^d + a_2x^{d-1}y + a_3x^{d-2}y^2 + \ldots\ldots + a_dxy^{d-1}x + a_{d+1}y^d \qquad (3).$$

L'invariant "degré" implique une classification des Courbes Algébriques C

Pour n=1 , les Courbes C sont des droites ;

Pour n=2 , les Courbes C sont des coniques; ce sont des intersections d'un cone par un plan (cercle , ellipse , parabole , hyperbole, un point, deux droites).

Pour n=3 ,les Courbes C sont des Cubiques .

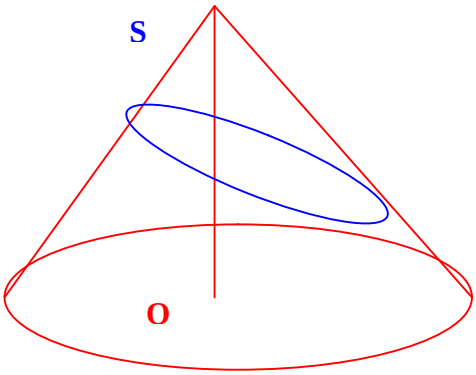
Pour n=4 , les Courbes C sont des quartiques.

Pour n=5 ,les Courbes C sont des quintiques ;etc .....

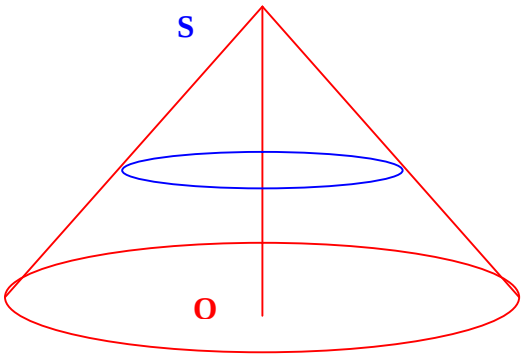
Tout polynôme $g(x,y) \in K[x,y]$ de degré $n > 1$ peut être irréductible ou dégénéré .

Ainsi , une Cubique C irréductible a une équation $g(x,y)=0$

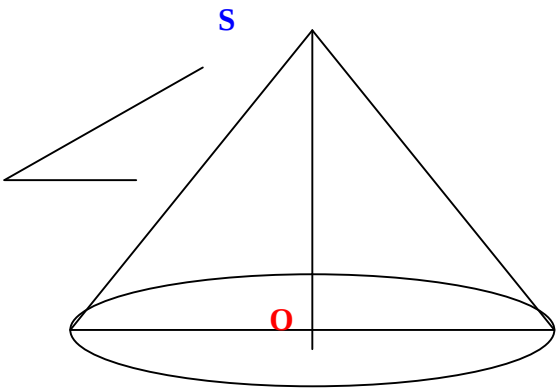
Une Cubique C non irréductible est dégénérée sous deux formes possibles : $C=DD_1D_2$ = produit de trois droites D_i ou C =DL produit d'une droite D et d'une conique L



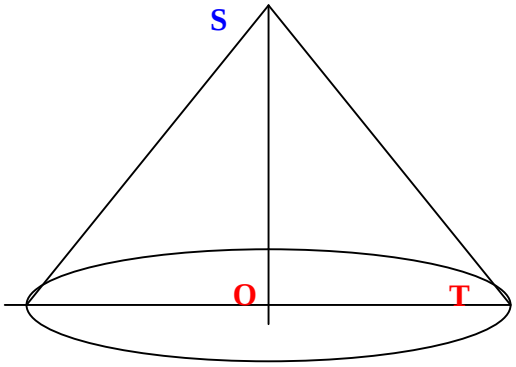
Ellipse:avec un plan sécant



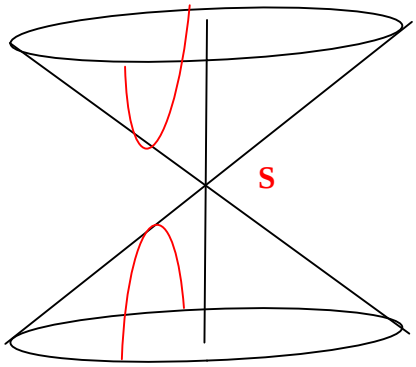
Cercle :avec un plan perpendiculaire à l'axe SO



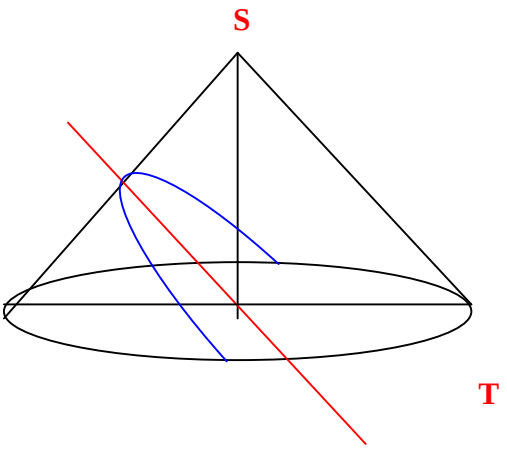
Un point avec plan passant par le sommet S



Deux droites avec plan passant par une arête ST



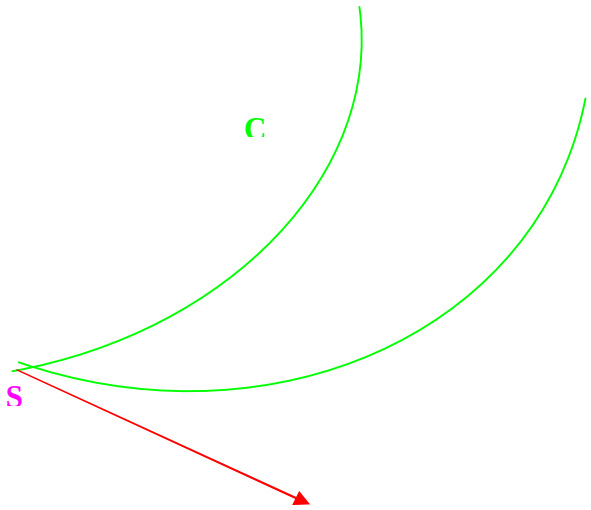
Hyperbole avec un plan coupant les deux parties du cone.

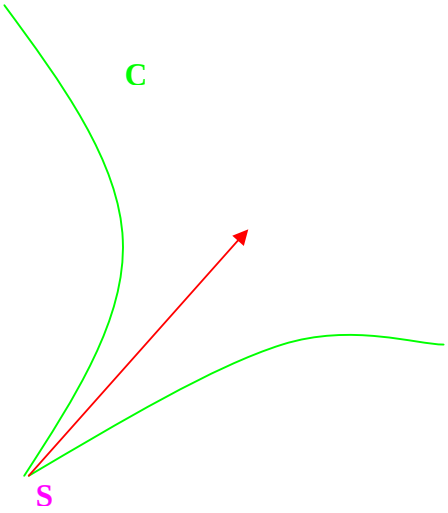


Parabole :avec un plan parallèle à une arête ST.

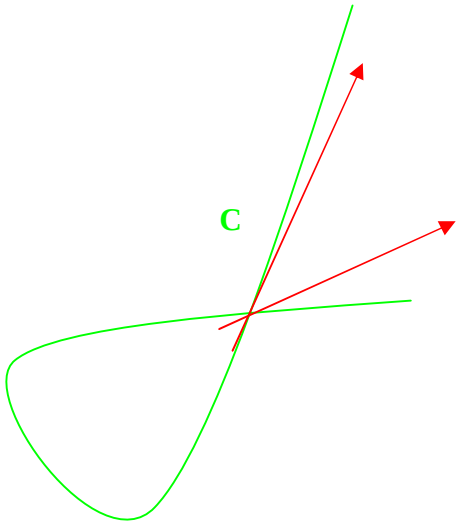
Figures 1-1

Point ordinaire et points singuliers.

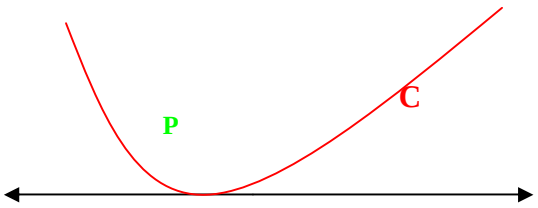




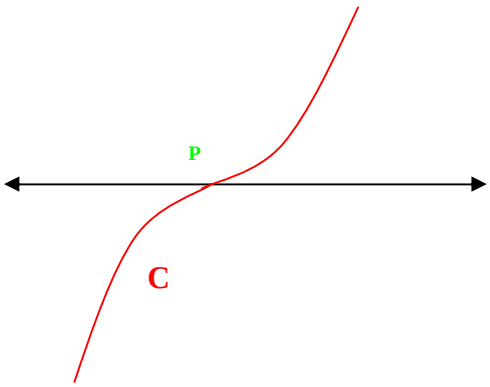
Point de rebroussement avec deux tangentes confondues.



Point singulier :
Un nœud S avec deux tangentes distinctes à C.



Point ordinaire la tangente ne traverse pas la Courbe C .



Point d'inflexion la tangente traverse la Courbe C .

Désormais nous ne considérons que des Courbes Algébriques planes de degré 3: les Cubiques planes

Une Cubique plane C peut admettre quatre types de points suivant la position de la tangente à C.

2-Points singuliers de Cubiques planes.

Définition 1 : 1) *un point P d'une Courbe C est ordinaire si C admet en ce point une tangente unique, qui ne traverse pas C dans un voisinage de P;*

2)*P est un point d'inflexion si C admet en P une tangente unique , qui traverse C dans un voisinage de P;*

Une Cubique C peut posséder des points singuliers ; points où la Courbe C admet deux tangentes

Définition 2 : **1)** *Un point singulier S d'une Cubique plane est un noeud si la Courbe C admet deux tangentes distinctes en S.*

2) *Un point singulier S d'une Cubique plane C est un point de rebroussement si la Courbe C admet deux tangentes confondues en ce point S*

Voir les figures 1-1

Le nombre s de points singuliers permet d'introduire l'invariant "genre" d'une Courbe algébrique plane .

3-Genres de *Courbes Algébriques*

Définition 3 *:Soit une Courbe Algébrique plane E de degré n qui possède S points singuliers; alors son genre est égal à l'entier rationnel positif ou nul:*

$g\,(C) = \frac{(n-1)(n-2)}{2} - S \geq 0$

([7]- 7-2- page . 54 ; [21]- IV - Curves)

Il en résulte que les genres des droites et des coniques sont nuls g (C) =0

Une Cubique admet S =0,1 point singulier,d'après la formule g(C) , il en résulte le genre d'une Cubique plane.

Proposition 1

1) *Une Cubique plane C singulière a un genre g(C)=0.*

2) *Une Cubique plane C non singulière a un genre g(C)=1.*

Preuve .

Pour S =1 , la formule du genre implique la valeur du genre

$g\,(C) = \frac{(3-1)(3-2)}{2} - 1 = 0$

Pour S =0 ; nous obtenons la valeur du genre

$g(C) = \frac{(3-1)(3-2)}{2} - 0 = 1$

o

Voici des petites valeurs de g calculées avec cette formule:

1)g = 0 pour les droites,les cercles , les coniques et les Cubiques singulières, les quartiques ayant 3 points singuliers ...

2)g =1 pour les Courbes Elliptiques, les quartiques ayant 2 points singuliers etc ...

3)g =2 pour les quartiques ayant 1 point singulier , les quintiques ayant 4 points singuliers , etc ...

4)Les Courbes hyperelliptiques sont les Courbes algébriques planes d'équation :

$y^2 = f(x) \in K[x]$, pour f(x) de degré n ³ 3.

Application à la famille de Cubiques E(t,m):

E(t,m): $y^2 + 2(t-1)xy = x^3 - (t-1)^2 x^2 - 3mx - m \quad \in Q[x, y]$

1)Cubique E(0,0) : $y^2 - 2xy = x^3 - x^2 \quad \in Q[x, y]$

$g(x, y) = y^2 - 2xy - x^3 + x^2$

Détermination des points singuliers avec les dérivées partielles

$g'_x = -2y - 3x^2 + 2x;$ $g'_y = 2y - 2x;$ $g'_x \neq g'_y.$

$g''_{x^2} = -6x + 2;$ $g''_{xy} = -2;$ $g''_{y^2} = 2,$ $g''_{xy} \neq g''_{y^2}.$

Le système admet le point S=(0,0) comme point singulier .

Donc la Cubique E(0,0) est singulière; la dérivée ý= $\frac{3x^2 - 2x + 2y}{2(y-x)}$

prend la valeur y'(0,0) = $\frac{0}{0}$ donc c'est un point de rebroussement .

Le tracé de la Courbe C : $y^2 - 2xy = x^3 - x^2$

L'intersection de C avec l'axe Ox:

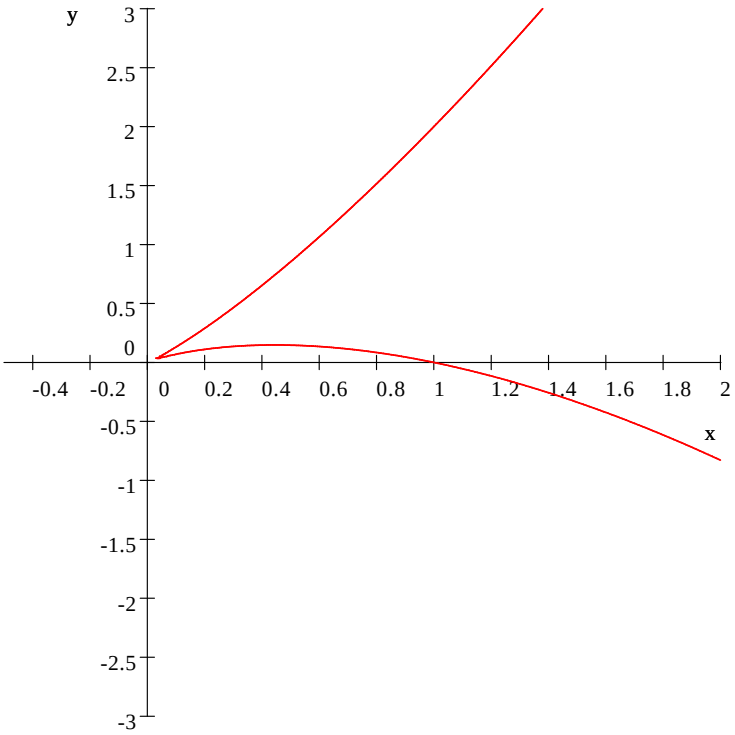
y =0; $x^3 - x^2 = x^2(x-1) = 0$; une racine double $x_1=x_2=0$ et une racine simple $x_3=1$ le point P_1 =(0,0) est double; le point P_2 =(1,0) est simple

L'intersection de C avec l'axe OY

$x=0;$ $y^2=0$; racine double $y_1=y_2=0$.

Quelques points de la Cubique E(0,0)

x	0	$\frac{1}{2}$		1		2	
y	$y_1=y_2=0$	0.85355	0.14645	2	0	$2-\sqrt{8}$	$2+\sqrt{8}$



2)Cubique E(1,1): $y^2 = x^3 - 3x - 1 \in Q[x,y]$ de la famille E(t,m)

Dérivées partielles: du polynôme $g(x,y)=x^3-3x-1-y^2$;

$g'_x = 3x^2-3=0$; $g'_y = -2y=0$

le système admet les solutions $x = \pm 1$, $y = 0$, les deux points singuliers sont (-1,0) et (+1,0) ne sont pas sur la Cubique E(1,1) , donc pas de point singulier. Le genre de cette Cubique est égal à 1.Donc E(1,1) est une Courbe Elliptique .

Quelques points de la Cubique E(1,1):

$x=0$; $y^2=-1$; pas de y réel, pas de point;

Les racines d'un polynôme cubique $u(x)=r_0x^3+r_1x^2+r_2x+r_3 \in Q(x)$ sont

déterminées par le :

Théorème : *soit un polynôme cubique u(x) ∈ Q(x) de discriminant dis(u).Alors :*

1)le polynôme u(x) admet trois racines réelles si est seulement si di(u)>0;

2)le polynôme u(x) admet une racine réelle et deux racines complexes conjugues si et seulement si di(u)<0;

o

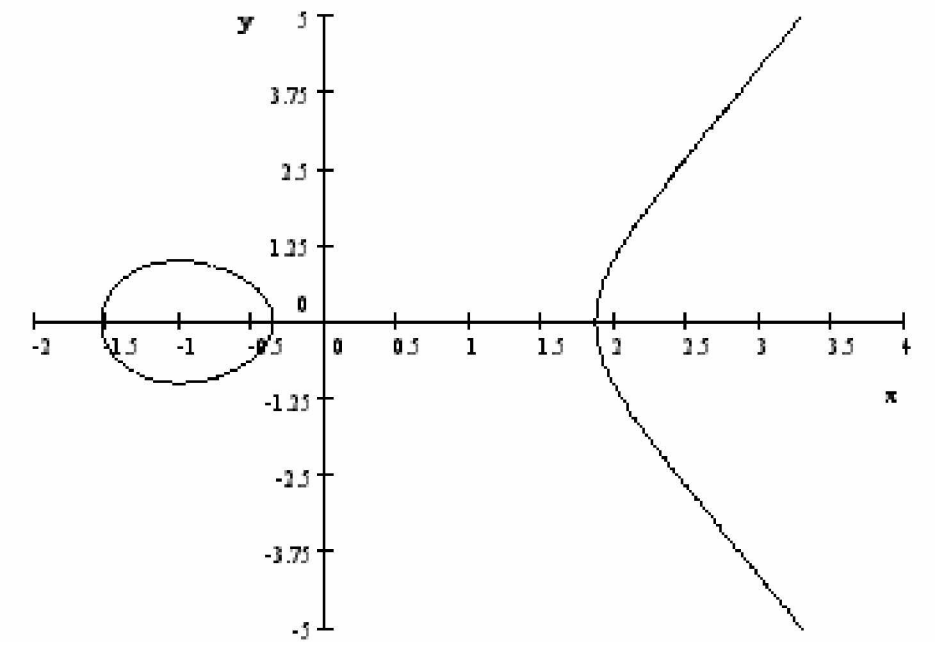
Nous obtenons trois racines réelles avec le logiciel S-W-Place

x_1=-0.34730, x_2=-1. 5321, x_3=1. 8794

y=0; x^3*-3x-1*=0; pas de *x* réel , pas de point sur la cubique ;

x =2; y^2*=1 ;* *y*= ±1; deux points simples (2,1) et (2,-1) .

Le tracé de la cubique E(1,1) avec le logiciel S-W-Place



3)Cubique E(3,-2) : $y^2+4xy=x^3-4x^2+6x+2$; de la famille E(t,m)

Dérivées partielles du polynôme g(x,y) = $y^2+4xy-x^3+4x^2-6x-2$:

$g'_x = 4y - 3x^2 + 8x - 6 = 0;$ $g'_y = 2y + 4x = 0$

le système n'a pas de solutions réelles donc pas de points singuliers sur la Cubique E(3,-2) ; son genre est égal à 1 .

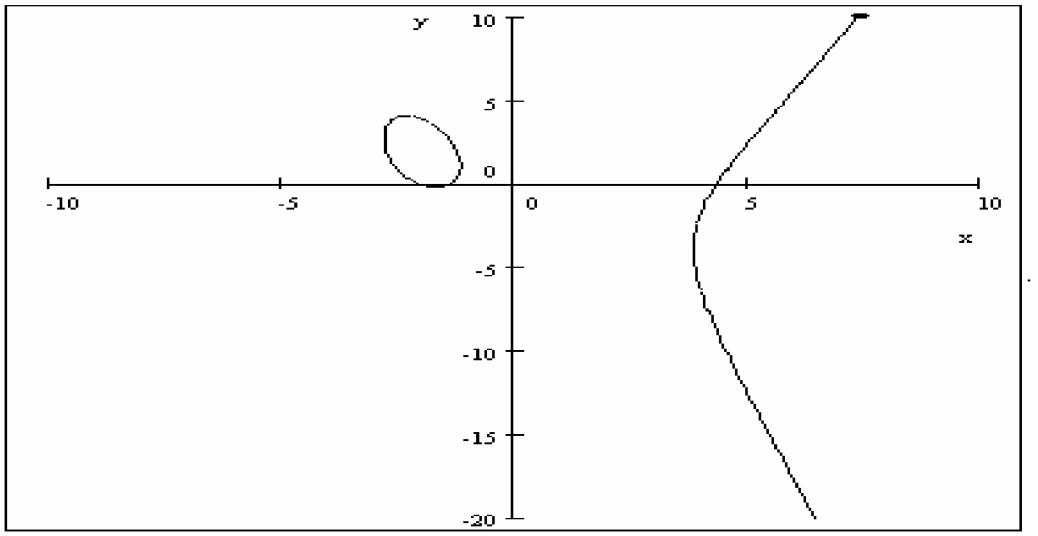
4) Cubique E(2,4): $y^2 + 2xy = x^3 - x^2 - 12x - 12 \quad \in Q[x, y]$

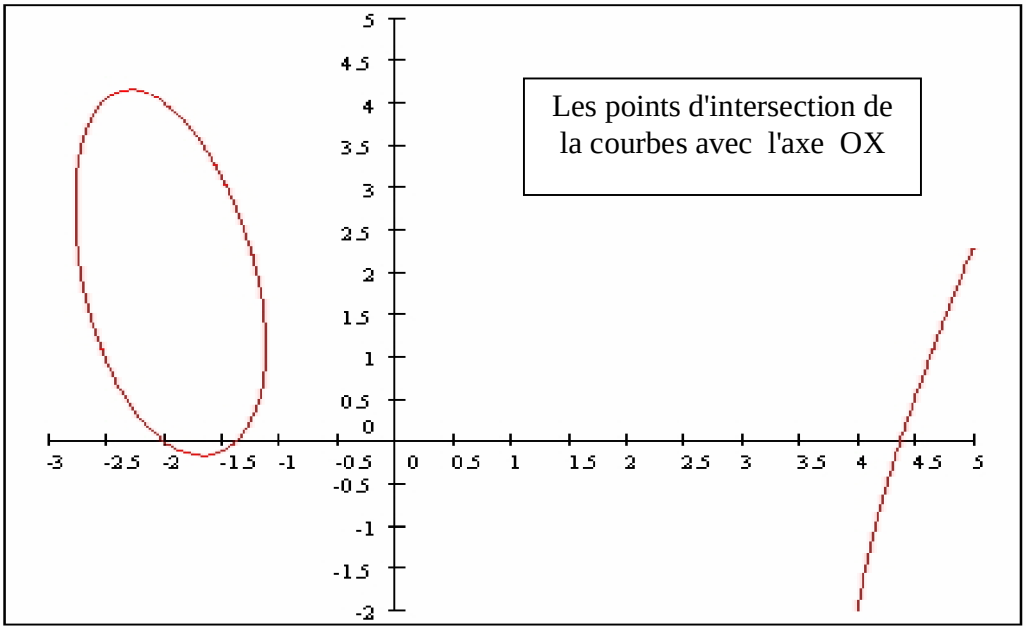
Dérivées partielles du polynôme $g(x,y)=y^2+2xy-x^3+x^2+12x+12$:

$g'_x = 2y - 3x^2 + 2x + 12 = 0; \qquad g'_y = 2y + 2x = 0$

le système n'a pas de solutions réelles donc pas de points singuliers sur la cubique E(2,4); son genre est égal à 1 ,c'est donc une Courbe Elliptique .

Le tracé de la cubique E(2,4) avec le logiciel S-W-Place





Chapitre III Cubiques de Weierstrass Courbes Elliptiques

1-Cubiques de Weierstrass

Une Cubique algébrique plane C a une équation de la forme

C: $d_1x^3 + d_2x^2y + d_3xy^2 + d_4y^3 + d_5x^2 + d_6xy + d_7y^2 + d_8x$

$+ d_9y + d_{10} \in K[x, y]$.

Cette Cubique dépend de 10 coefficients d_1 ,.....,$d_{10} \in K$.

Dans l'ensemble de ces Cubiques il y a des Cubiques avec cinq coefficients : les Cubiques de Weierstrass

Définition 1 : *une Cubique de Weierstrass est une Courbe Algébrique plane C de degré trois , d'équation de la forme:*

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y] \qquad (1)$$

Les cinq coefficients a_1, a_2, a_3, a_4, a_6 *sont des éléments d'un corps commutatif K global , local, ou fini.*

Les deux variables x,y sont des éléments d'une clôture algébrique du corps K.

Définition 2 :*l'équation (1) est l'équation de Weierstrass de la Cubique C.*

Ainsi , dans l'équation de Weierstrass de la famille $E_{t,m}$ les coefficients a_i sont égaux à :

$a_1 = 2(t-1)$, $a_2 = -(t-1)^2$, $a_3 = 0$,

$a_4 = -3m$ et $a_6 = -m$

Définition 3 :*Une Courbe Elliptique est une Cubique de Weierstrass non singulière irréductible d'équation de Weierstrass*

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ \in K[x; y]$$

2-**Changements de variables dans les équations.**

L'équation de Weierstrass :

$$E \quad : \quad y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6 \in K[x, y] \qquad (1)$$

se transforme par des changements de variables convenables .Il y a deux types de Cubiques de Weierstrass : celles qui sont singulières et celles qui ne sont pas singulières.

Lorsque le corps K est de caractéristique carac(K) ® 2, nous éliminons les monômes en xy et en y par le changement de variables linéaire:

$$(x, y) \rightarrow (X, \tfrac{1}{2}(Y - a_1X - a_3)); \qquad car(K) \neq 2 \qquad (2)$$

Nous obtenons l'équation d'une Cubique de Weierstrass :

$$E_1 \; : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6; \qquad (3)$$

Avec le calcul j'obtiens les valeurs des invariants b_{2j} :

$$b_2 = a_1^2 + 4a_2; \qquad b_4 = a_1a_3 + 2a_4; \qquad b_6 = a_3^2 + 4a_6; \qquad (4)$$

Ces 3 coefficients b_{2i} sont des polynômes "homogènes de degré 2*i* " dans l'anneau Z [a_1,a_2,a_3,a_4,a_6] .

Pour carac(K) ≠2 , 3, nous éliminons le monôme en X^2 et le coefficient 4 dans la formule (3) avec le changement de variables linéaire .

$$(X,Y) \longrightarrow \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right) \qquad (5)$$

Nous obtenons l'équation d'une Cubique de Weierstrass :

$$E_2 \quad : \quad y^2 = x^3 - 27c_4x - 54c_6; \qquad (6)$$

Ces deux invariants c_{2j} sont des polynômes homogènes de degré 2j dans l'anneau $Z[b_2, b_4, b_6]$:

$$c_4 = b_2^2 - 24b_4 \quad ; \qquad c_6 = 36b_2b_4 - b_2^3 - 216b_6; \qquad (7)$$

Il existe d'autres modèles de Cubiques de Weierstrass:

le modèle de Legendre: $E_3 : y^2 = x(x-1)(x-t)$ avec $t \neq 0$ et 1 (8)

le modèle de Deuring : $E_4 : y^2 + axy + y = x^3$; avec $a^3 \neq 3$; (9)

le modèle de Tate: $E_5 : y^2 + xy = x^3 + ax + b$; (10)

où a et b sont des séries de puissances formelles en $q = \exp(2\pi iz)$: z est un nombre du demi plan *IH* de Poincaré $IH = \{x + iy \in C ; y > 0\}$:

$$a = -5\sum_{m\geq 1} m^3 q^m (1-q^m)^{-1};$$
$$b = -\frac{1}{12}\sum_{m\geq 1} qm(7m^5 + 5m^3)(1-q^m)^{-1} \qquad (11)$$

la Cubique de Weierstrass:

$E: y^2 = x^3 + Ax + B.$ (12)

Cette Cubique devient une Courbe Elliptique lorsque $4A^3 + 27B^2 \neq 0$.

3-Les invariants des Cubiques de Weierstrass.

Les invariants des Cubiques de Weierstrass sont des fonctions des coefficients des équations, qui prennent des valeurs différentes et qui permettent de classifier les Cubiques de Weierstrass.

Toute Cubique de Weierstrass E possède plusieurs invariants: un discriminant, un invariant modulaire,un invariant différentiel,un conducteur, un régulateur , une série de Dirichlet -Hasse-Weil,etc...

Définition 4 *: le discriminant d'une Cubique de Weierstrass :*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y]$$

est le polynôme "homogène de degré 12" égal à :

$$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \in Z[b_2, b_4, b_6, b_8]$$

pour carac $(K) \neq 2, 3$ et $4b_8 = b_2b_6 - b_4^2$

Définition 5 :*l'invariant modulaire de la Cubique de Weierstrass E de discriminant Δ(E) et de coefficient usuel $c_4(E)$ est l'élément du corps K égal à :* $j(E) = \frac{c_4(E)^3}{\Delta(E)}$.

Définition 6 :*l'invariant différentiel de la Cubique de Weierstrass E est l'élément différentiel :* $g(E) = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$.

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = g(x, y) \in K[x, y]$;

différentielle dg(x,y) =$g'_x dx+g'_y dy=0$ du polynôme g(x,y) et les dérivées partielles :

$$g'_x = a_1y - 3x^2 - 2a_2x - a_4 \qquad et \qquad g'_y = 2y + a_1x + a_3$$

Exemples:

1) Cubique de Weierstrass: E : $y^2 = x^3 - 27c_4x - 54c_6$ 5 K ß x, y à

Les coefficients c_4 et c_6 de cette équation ne sont pas les invariant c_4(E) et c_6(E).

Avec le calcul je trouve les invariants : $b_2=0$; $b_4=-54c_4$; $b_6=-4\times54c_6$; $b_8=-(27c_4)^2$, $c_4(E) =16+81c_4$;

le discriminant est égal à : $\Delta(E) = 2^6 3^9 \left(c_4^3 - c_6^2\right)$

$$j(E) = \frac{12^3 c_4^3}{(c_4^3 - c_6^2)} \quad ; \qquad \omega(E) = \frac{dx}{2y} = \frac{dy}{3x^2 - 27c_4}.$$

2) Pour la Cubique E : $y^2 = x^3 + Ax + B$ 5 K ß x, y à ; car K ® 2, 3

Les invariants : $b_2 = 0$, $b_4 = 2A$, $b_6 = 4B$, $b_8 = -A^2$; $c_4 = -48A$

Le discriminant: $\Delta(E) = -16(4A^3 + 27B^2)$;

L'invariant modulaire: $j(E) = \frac{4(12A)^3}{4A^3 + 27B^2}$;

L'invariant différentiel: $\omega(E) = \frac{dx}{2y} = \frac{dy}{3x^2 + A}$.

3) La famille de Cubiques de Weierstrass

E(t,m): $y^2 + 2(t-1)xy = x^3 - (t-1)^2 x^2 - 3mx - m \quad \in Q[x, y]$

Les invariants: $b_2=0$; $b_4=-2\times 3m$; $b_6=-2^2m$; $b_8=9m^2$, $c_4=2^4 3^2 m$, $c_6=2^5 3^3 m$

Le discriminant : $\Delta(t,m) = 27.16m^2(4m-1)$.

L'invariant modulaire: $j(E(t,m))=\frac{c_4^{\,3}}{\Delta(t,m)} = \frac{(2^3.3^2 m)^3}{3^3.2^4.m^2(4m-1)} = \frac{2^5.3^3 m}{4m-1}$.

4)La Courbe de Fermat

Les deux théorème de Fermat

1)Le petit théorème de Fermat**:** *la congruence $a^p \equiv a \bmod p$ est satisfaite pour tout nombre premier p et pour tout entier a inférieur à p.*

2)Le grand théorème de Fermat ,qui n'a été démontré qu'en 1994 par Wiles, en utilisant la théorie des Courbes Elliptiques .

L'équation diophantienne $u^n+v^n=w^n$ n'a pas de solutions non triviales pour les entiers naturels $n\geq 3$: (u,v ,w)=(0,0,0), (1,0,1) ,(0,1,1)sont les seules solution.

Pour n=2, l'équation $u^2+v^2=w^2$ est l'équation de Pythagore ; elle admet une infinité de solutions :$u =t(a^2-b^2)$, $u=2tab$, $w=t(a^2+b^2)$ $t\in Z$, a et b premiers entre eux .

Pour n=3,l'équation $u^3+v^3=w^3$ est transformé par le changement de variables $x=\frac{3w}{u+v}$ et $y = \frac{9uv}{2(u+v)} + \frac{1}{2}$

En l'équation de Weierstrass : $E : y^2-y=x^3-7$

Avec le calcul nous obtenons les invariants

$c_4(E)=0$, $\Delta(E) = -3^9$, $N(E)=27$ et $\omega(E)=\frac{dx}{2y-1}=\frac{dy}{3x^2}$

5) Cubique de Legendre :

$y^2 = x(x-1)(x-t) = x^3 - (1+t)x^2 + tx$ Kß x, yà , $t \neq 0,1$; car(K) $\neq 2,3$

Avec le calcul j'obtiens les invariants: $b_2 = 4(1+t)$,

$b_4 = 2t, \quad b_6 = 0, \quad b_8 = -t^2, \quad c_4 = 16(t^2 - t + 1), \quad c_6 = -32(t-2)(2t-1)(t+1),$

Le discriminant: $\Delta(E) = 16\ t^2(1-t)^2,$

L'invariant modulaire : $j(E) = \frac{c_4^3(E)}{\Delta(E)} = \frac{(16(t^2 - t + 1))^3}{16t^2(1-t)^2}$

$= 256(t-1)^{-2}t^{-2}(t^2 - t + 1)^3,$

L ' invariant différentiel: ω (E) $\frac{dx}{2y} = \frac{dy}{3x^2 - 2(t+1)^2 x + t}.$

4-Classification des Cubiques de Weierstrass par leurs invariants

$\Delta(E),$ *et* $c_4(E)$

Pour une Cubique de Weierstrass E*:* $y^2 = f(x) \in K[x]$
les discriminants AÝEÞde E et dis(f) du polynôme f(x) sont liés , ß11à,ß12 ? 1à.

4-1*) Définition 7* *: le discriminant du polynôme* $f(x) = (x-\theta_1)....(x-\theta_n)$ *de degré n* x 1 *est la forme quadratique:*

dis(f)= $\prod_{i<j}(\theta_i - \theta_j)^2$

Lorsque le polynôme n'est pas unitaire, son discriminant peut être calculé avec la :

Proposition 1:

le discriminant d'un polynôme $f(x) = d_0 x^n + d_1 x^{n?1} + ... + d_n \in K[x,y]$ *de degré n* x 1 *est égal à :*

dis(f)= $d_0^{2n-2} \prod_{i<j}(\theta_i - \theta_j)^2$

o

Le discriminant peut être calculé avec la théorie du résultant de deux polynômes

4-2*) Définition 8* *: soient deux polynômes d'un anneau IR*[*x*]

$f(x) = d_0 x^n + d_1 x^{n?1} + ... + d_n$ *de degré n> 1 et*

$g(x)=s_0x^t+s_1x^{t?1}+.....+s_t$ *de degré* $t>1$

leur résultant est égal au déterminant d'ordre n+t.

$$\text{Res}(f,g)=\begin{vmatrix} d_0 & d_1 & .... & d_n & 0 & 0 & ... & 0 & 0 & 0 \\ 0 & d_0 & .... & . & d_n & 0 & ... & 0 & 0 & 0 \\ ... & ... & ... & .. & .. & & ... & .... & ..... & ..... \\ 0 & .. & .. & d_0 & d_1 & d_2 & .... & .. & .. & d_n \\ s_0 & s_1 & .. & ... & s_t & 0 & ..... & .... & 0 & 0 \\ 0 & s_0 & .... & .... & ... & s_t & 0 & ... & .. & 0 \\ 0 & ... & s_0 & 0 & ... & 0 & s_t & 0 & ... & 0 \\ .... & .. & .... & .. & ... & .... & .. & .. & ... & .... \\ 0 & .... & .... & ... & ... & .. & .. & .. & .... & 0 \\ 0 & 0 & ..... & 0 & s_0 & s_1 & .. & .. & .. & s_t \end{vmatrix}$$

Ces résultants possèdent plusieurs propriétés qui sont énoncées sans démonstrations (consulter ß11à,ß12,1àÞ

o

Proposition 2 :

Soient les deux polynômes f(x) de degré n et g(x) de degré t ci-dessus Alors leur résultant est égal à :

1) $Res(f,g) = d_0^t s_t^n \prod_{i=1}^{n}.\prod_{j=1}^{t}(\theta_i-\lambda_j)$, θ_i = *zéros de f ,* V_j = *zéros de g ,*

2) $Res(f,g)=d_0^t\prod_{i=1}^{n}.g(\theta_i)=(-1)^{nt}s_t^n\prod_{j=1}^{s}.f(\lambda_j)$

o

Corollaire .

Res (f,g)=0 est nul si et seulement si les polynômes f et g ont un zéro commun $\theta_i=\lambda_j$

o

Puisqu'un polynôme f(x) est différent de sa dérivée $f'(x)$; il existe un résultant Res(f,f'); ce résultant est lié au discriminant dis(f) de f.

Proposition 3 :

Soit un polynôme

$f(x)=d_0x^n+d_1x^{n-1}+.....+d_n=d_0(x-S_1)\ldots\ldots(x-S_n)$ *de degré n* $\neq 1$. *Alors le résultant Res(f,f') de f(x) et de sa dérivée est égal à :*

$Res(f,f')=d_0^{n-1}\prod_{i=1}^{n}.f'(\theta_i)=d_0(-1)^{\frac{n(n-1)}{2}}.dis(f)$, *avec dis(f)=discriminant du polynôme f(x)*

o

Exemples de discriminants dis(f) ,[13,1]

1)pour $f(x)=ax^2+bx+c$,alors dis(f)=b^2-4ac;

2)pour $f(x)=x^3+px+q$; alors dis(f)=$-(4p^3+27q^2)$

3) pour $f(x)=d_0x^3+d_1x^2+d_2x+d_3$,

alors dis(f) $=18d_0d_1d_2d_3+d_1^2d_2^2-27d_0^2d_3^2-4d_1^3d_3-4d_0d_2^3$;

4)pour $f(x)=\frac{x^n-1}{x-1}$, alors dis(f)=$(-1)^A n^{n-2}$ avec A= $\frac{(n-1)(n-2)}{2}$

5) pour $f(x)=x^n+d$, alors dis(f)= $(-1)^{\frac{n(n-1)}{2}}.n^n d^{n-1}$

4-3 Cubiques de Weierstrass singulières.

Soit une Cubique de Weierstrass :

E: $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\in K[x,y]$,

son discriminant $\Delta(E)$, son invariant c_4(E) et son point à l'infini $O_E=(\infty,\infty)=(0,1,0)$

Proposition 4:

Soient les hypothèses ci-dessus .

1)*le point* O_E *est un point non singulier de la Cubique E.*

2) *la Cubique est singulière si et seulement si* $\Delta(E)=0$.

La Cubique possède un noeud si $c_4(E)\neq 0$ *elle possède un point de rebroussement si* $c_4(E)=0$.

Preuve de "O_E est un point non singulier de la Cubique "

Prenons l'équation de Weierstrass.

$f(x,y,z)=y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$ 5 IP²ÝKÞ.

La valeur de f au point $O_E=(0,1,0)$ est égale à :

$f(O_E)=0$;

Donc le point O_E est sur la Cubique.

La dérivée partielle $f'_z=y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2$ prend la valeur: $f'_z(O_E)=1\neq 0$,

Donc ce point n'est pas singulier.

Preuve de " AÝEÞ = 0" implique "la Cubique est singulière ".

Prenons une Cubique de Weierstrass:

$E: y^2=x^3+Ax+B=f(x)$ 5 Kßxà,

D'après les propriétés des résultants , $Res(f,f')$ et le discriminant dis(f) sont liés par une relation $Res(f,f')=d_0.dis(f)$, d_0 =constante > 0

Les discriminants $\Delta(E)$ et dis(f) satisfont la relation $\Delta(E)=c.dis(f)$, c=constante positive ,

L'hypothèse $\Delta(E)=0$ implique $dis(f)=0$ et $Res(f,f')=0$.

Il en résulte que $f(x)$ admet une racine double ou triple ; le Cubique admet un point singulier .

Preuve de "$c_4(E)\neq 0$" implique " la Cubique admet un nœud ".

Prenons une Cubique de Weierstrass :

E: $y^2 = x^3 - 27c_4 x - 54 c_6 = f(x) \in K[x]$

Cette Cubique E est singulière : au point singulier S elle admet deux tangentes distinctes.

Les pentes de ces tangentes sont égales à la dérivée y' de y :

$$y' = \frac{3x^2 - 27c_4}{2y} = \frac{3}{2y}(x^2 - 9c_4).$$

Le polynôme $g(x)=x^2-9c_4=0$ admet deux zéros $x = \pm 3(c_4)^{1/2}$ si $c_4 \neq 0$.

Il en résulte deux tangentes distinctes en S ; donc le point est un nœud. Preuve de " $c_4 = 0$" implique" le point singulier est un point de rebroussement de E"

Prenons la Cubique de Weierstrass ci -dessus et la dérivée $y' = \frac{3}{2y}(x^2 - c_4)$.

L'hypothèse $c_4=0$ implique :$y' = \frac{3x^2}{2y}$; le polynôme $g(x)=x^2$ admet une racine double, donc la Cubique E admet deux tangentes confondues au point singulier .C'est donc un point de rebroussement .

o

Cette proposition implique que la Cubique de Weierstrass E de discriminant $\Delta(E) \neq 0$ n'est pas singulière : c'est donc une Courbe Elliptique.

4-4) Courbe Elliptique

Proposition 5 :

Soit une Cubique de Weierstrass E de discriminant $\Delta(E)$.

1)Cette Cubique est une Courbe Elliptique si et seulement si $\Delta(E) \neq 0$

2)Une Courbe Elliptique E coupe l'axe réel Ox en trois point simples si et seulement si AÝEÞ x 0 ,

3)Une Courbe Elliptique E coupe l'axe réel Ox en un seul point simple si et seulement si AÝEÞ Ö 0

Preuve de " $\Delta(E) \neq 0$" implique "E est une Courbe Elliptique"

Soit une Cubique de Weierstrass E de discriminant $\Delta(E)$.

D'après la proposition ci-dessus ," $\Delta(E) = 0$" si et seulement si " la Cubique E est singulière"

Il en résulte : $\Delta(E) \neq 0$" si et seulement si " la Cubique E n 'est pas singulière; donc E est une Courbe Elliptique .

Preuve de " AÝEÞ x 0 implique "E est une Courbe Elliptique qui coupe l'axe réel Ox en trois points distincts".

Prenons une Courbe Elliptique E d'équation

$y^2=f(x)=(x-e_1)(x-e_2)(x-e_3) \in K[x]$, (1)

Les discriminants $\Delta(E)$ de E et dis(f) de f(*x*) satisfont la relation $\Delta(E) =$ c.dis(f) , c =constante positive (2)

L'hypothèse $\Delta(E) \rangle 0$ implique dis(f) $\rangle$ 0.

"L'hypothèse dis(f) > 0 et f(*x*) =polynôme Cubique " impliquent que f(*x*) admet trois zéros réels e_1,e_2,e_3 simples (3)

(1) et (2) impliquent que la Courbe Elliptique E coupe l'axe réel Ox en trois points simples : P=(e_i ,0) , i=1,2,3 , (4)

Preuve de " AÝEÞ Ö 0" implique " la Courbe Elliptique E coupe l'axe réel O*x* en un seul point , qui est simple ".

L'hypothèse " $\Delta(E) < 0$" et la relation $\Delta(E) = c$ dis(f), c > 0 implique dis(f) $\neq 0$.

Il en résulte que le polynôme Cubique f(x) $\in \mathrm{R}[x]$ admet une racine réelle

et deux racines complexes conjuguées $r \pm is \in C$. Il en résulte le polynôme f(*x)=(x-e)(x-r-is)(x-r+is)* , avec deux nombres réels r et s .

Alors dis(f)= $\left[(e-r-is)(e-r+is)(2is)\right]^2 = \left[(e-r)^2 + s^2\right]\left[-4s^2\right] < 0$

Donc la Courbe Elliptique E coupe l'axe réel Ox en un seul point P=(e,0) , qui est simple .

o

Nous ne ferons pas la preuve des réciproques.

Les deux propositions (4) et (5) classifient les Cubiques de Weierstrass E avec les invariants $\Delta(E)$ et c_4(E)

Proposition 6

Soit les Cubiques de Weierstrass E, d'équation :

$$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ ,$$

avec leurs discriminants AÝEÞ *et leur invariant* $c_4(E)$.

Elles sont classifiées en quatre classes :

(We 1) classe des Cubiques de Weierstrass qui ont un noeud, lorsque AÝEÞ *=0 et* $c_4(E) \neq 0$

(We2) classe des Cubiques de Weierstrass qui ont un point de rebroussement ; lorsque AÝEÞ *=0 et* $c_4(E) = 0$

(We 3) classe des Courbes Elliptiques qui coupent l'axe réel Ox en trois point simples , lorsque AÝEÞ x 0 .

(We 4) classe des Courbes Elliptiques qui coupent l'axe réel Ox en un seul point , qui est simple ,lorsque AÝEÞ ß0 .

Preuve : avec les deux propositions (4) et (5)

o

Application à la famille des Cubiques E(t,m) :

EÝt, mÞ ¢y² + 2Ýt ? 1Þxy = x³ ? Ýt ? 1Þ²x² ? 3mx ? m 5 ¥ßx, yà

Les invariants

$b_2 = 0,$ $b_4 = ?2 \times 3m;$ $b_6 = ?2^2 m,$ $c_4 = 2^4 3^2 m,$ $c_6 = 2^5 3^3 m$

Le discriminant : $\Delta(t,m) = 27.16m^2(4m-1)$

L ' invariant modulaire: $j(E(t,m)) = \frac{-2^8.3^3 m}{(4m-1)}$

Etude de la famille E(t,m):

Cas 1: $\Delta(t,m) = 0$

Cela implique m =0 ou m=1/4 , la famille E(t,0) est la famille des Cubiques singulières avec un point de rebroussement

Cas 2: si $\Delta(t,m) = 0 \ et \ c_4(t,m) \neq 0$

Cela implique m $= \frac{1}{4}$;la famille E(t, $\frac{1}{4}$) est la famille des Cubiques singulières avec un noeud

Cas 3: $\Delta(t,m)$ ¤ 0 implique $27.16m^2(4m-1)$ ⟩ 0 ;il en résulte $m \rangle \frac{1}{4}$

Cela implique la famille $E(t,m)$ des Courbes Elliptiques qui coupent l'axe réel Ox en trois points simples

Cas 4: $\Delta(t,m)$ ® 0 implique $27.16m^2(4m-1)$ ⟨ 0 ; il en résulte $m \langle \frac{1}{4} \ et \ m \neq 0,$

implique la famille $E(t,m)$ des Courbes Elliptiques qui coupent l'axe réel Ox en un seul point simple.

2) Cubique $E(0,0)$: $y^2 - 2xy = x^3 - x^2 \in \mathrm{Q}[x,y]$

Ses points singuliers ont été étudiés dans la page 17

Les invariants*: $b_2=0$, $b_4=0$, $b_6=0$, $c_4=0$, $c_6=0$*

L $^{\text{ième}}$ invariant modulaire: $j(E(t,m)) = 0$

Le discriminant : $\Delta(t,m) = 0$ et $c_4 = 0$;il en résulte que la Cubique E(0,0) admet un point de rebroussement .

Le tracé de la Courbe avec le logiciel S-W-place

L'intersection avec l'axe O*x*

y =0 implique deux racines *x*=0 et *x*=1, donc deux points d'intersection $(0,0)$ et $(1,0)$.

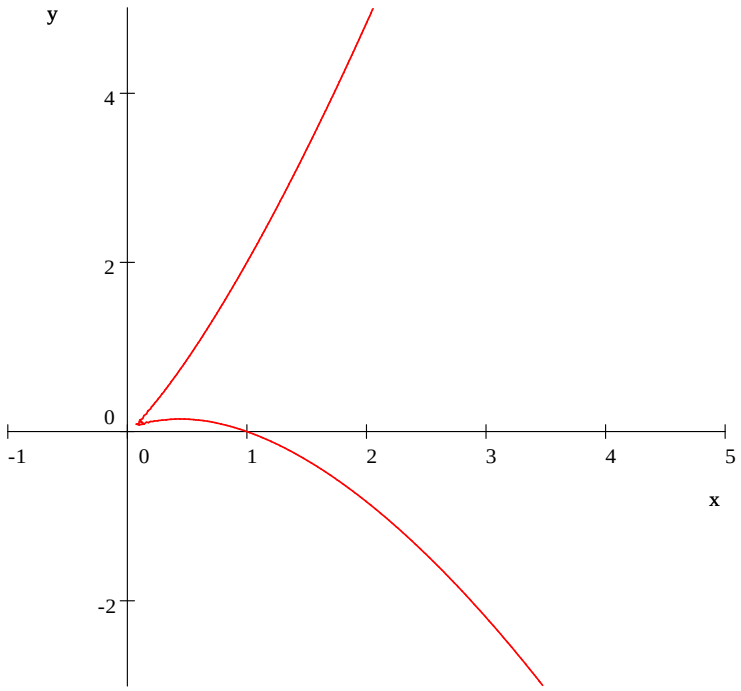
L'intersection avec l'axe O*y*

x=0 ,y^2=0, racine double $y_1=y_2=0$

Au point (0,0), la dérivée $y' = \dfrac{3x^2 - 2x + 2y}{2y - 2x}$ prend la valeur $y'(0,0) = \dfrac{0}{0}$

Tableau des coordonnées de quelques points

x	$\frac{1}{2}$	2	-1	3
y	$\frac{1}{2} \pm \frac{1}{4}\sqrt{2}$	$2 \pm 2\sqrt{2}$	pas de y réel	$3 \pm \sqrt{13}$



3)Cubique $E\acute{Y}2,2\text{þ}: y^2 + 2xy = x^3 - x^2 - 6x - 2 \quad \in Q[x, y]$

Les invariants:

$$b_2 = 0, \quad b_4 = -2^2 \times 3, \quad b_6 = -2^3, \quad c_4 = 2^5 3^2 \quad c_6 = 2^6 3^3$$

L' invariant modulaire: $j(E(2,2)) = \frac{-2^9.3^3}{7}$,

Le discriminant : $\Delta(E(2,2)) = 2^7 3.5.19 \rangle 0$, implique que la Cubique est une Courbe Elliptique qui coupe l'axe O*x* en trois points simples,

Pour *y*=0 je trouve trois racines x_1=*-0.36333 et* x_2=*3.1249* et x_3=*-17616* il en résulte trois points simples :(*-0.36333,0*) , (*3.1249,0*) , (*-17616,0*)

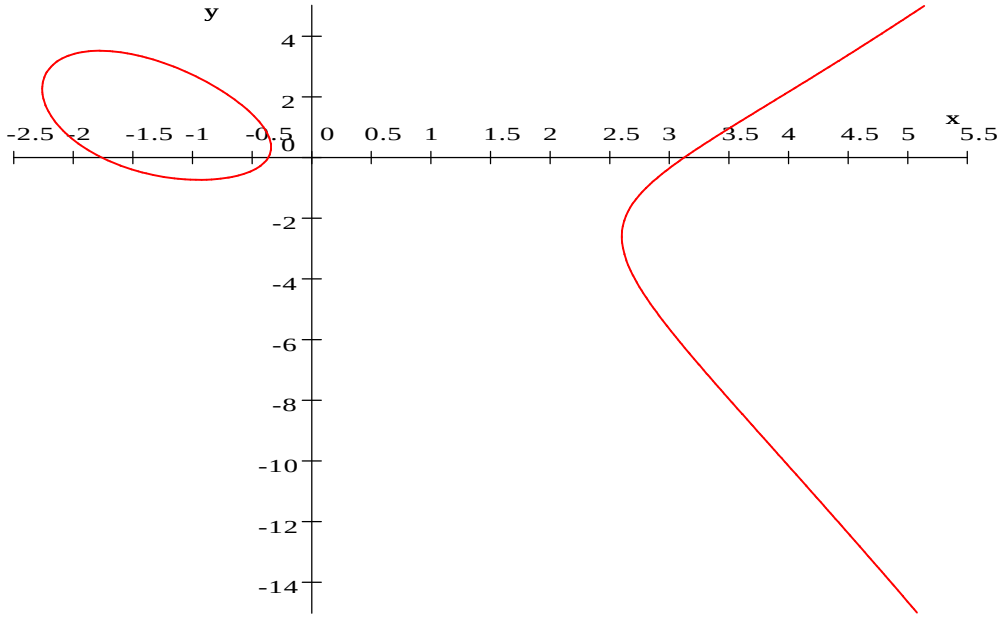
Le tracé de la Courbe avec le S-W-place

L'intersection avec l'axe O*y*.

x=0 je trouve y^2 =-2 donc pas de points d'intersections avec l'axe Oy.

Tableau des coordonnées de quelques points

x	0	-1	-2	-3	2	3	4
y	Pas de y réel.	$1\pm\sqrt{3}$	$2\pm\sqrt{2}$	Pas de y réel.	Pas de y réel.	-5.6458 et -0.35425	$-4\pm\sqrt{22}$



4) La Cubique $E(-1,-2)$: $y^2 - 4xy = x^3 - 4x^2 + 6x + 2$

Les invariants :$b_2=0$, $b_4=2^2.3$, $b_6=2^3$, $c_4=-2^5.3^2$, $c_6=2.431$

Le discriminant : $\Delta(t,m) = 27.16(-2)^2(4(-2)-1) = -977.2^219 < 0$,

L'invariant modulaire; $j(E(t,m)) = \frac{-2^8.3^3(-2)}{(4(-2)-1)}$ $=-2^9.3$ le discriminant est négatif ; la Cubique E(-1,-2) est une Courbe Elliptique qui coupe l'Axe Ox en un seul point (-0.27816,0)

Le tracé de la Courbe E(-1,-2) avec le W-place

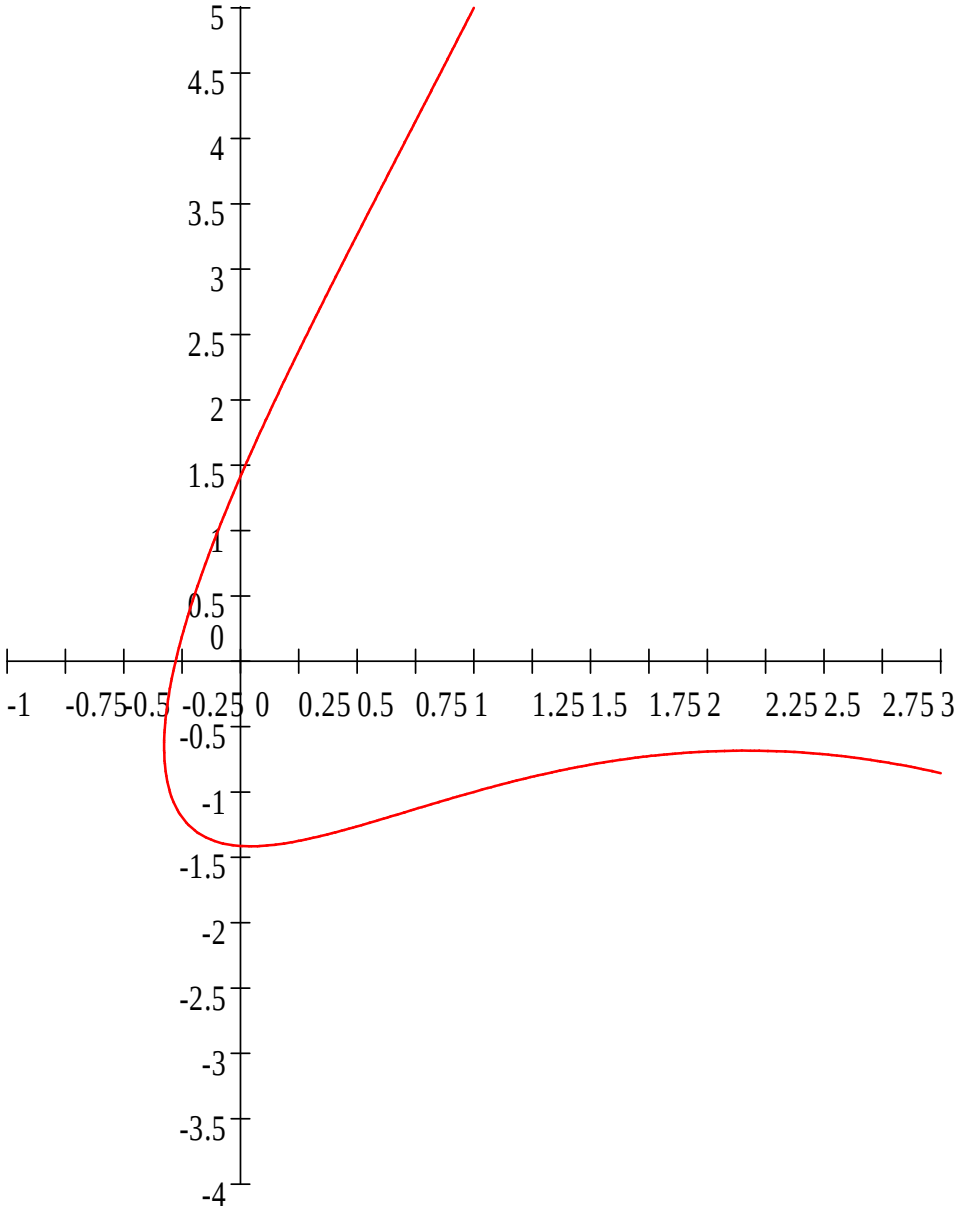
L'intersection avec l'axe Ox: un seul point P simple ,calculé précédemment P:$(-0.27816, 0)$

L'intersection avec l'axe O*y*

x=0 je trouve $y^2 = \pm\sqrt{2}$ deux points d'intersection $(0,-\sqrt{2})$ et $(0,+\sqrt{2})$

D'autre points

x	-1	0		1		2	
y	Pas de y reel.	$-\sqrt{2}$	$\sqrt{2}$	5	- 1	4 ? $\sqrt{22}$	$\sqrt{22}$ + 4



Chapitre- IV - Groupes de MORDELL-WEIL des Courbes Elliptiques .

Introduction

Poincaré a conjecturé que l'ensemble E(K) des points K-rationnels d'une Courbe Elliptique E est un groupe abélien de type fini . En 1922 , Mordell a prouvé cette conjecture.[13-3]-En 1925-1930 Weil a étendu cette propriété aux Variétés Abéliennes.

Nous allons construire ce groupe abélien E(K).

1) Groupe additif abélien sur l'ensemble E(K).

1-1 Soit une Courbe Elliptique E d'équation de Weierstrass:

$$y^2 + a_1xy + a_3 y = x^3 + a_2 x^2 + a_4x + a_6 \in K[x,y] \cdot \qquad (1)$$

Sur l'ensemble E(K) des points $P=(x,y)$ qui satisfont l'équation (1) , nous définissons une loi de groupe additif abélien d'élément neutre le point à l'infini O_E avec la :

Proposition 1

L'ensemble E(K) des points K- rationnels d'une Courbe Elliptique E, admet une structure de groupe additif abélien ,d'élément neutre le point à l'infini O_E, avec la règle géométrique:" Trois points colinéaires de E ont une somme nulle" : " $P_1 + P_2 + P_3 = O_E$ " , (2)

et la loi de composition interne

$$f: E(K) \times E(K) \longrightarrow E(K) \text{ , de valeur } f(P_1,P_2) = P_1 + P_2 = M$$

symétrique du point P_3 , de la formule (2) , par rapport à l'axe Ox .

Preuve

Vérifions les quatre axiomes d'un groupe abélien .

1)Le point à l'infini O_E est déterminé par la direction de l'axe O*y* ;c 'est un point simple sur la Courbe E.

Avec la règle géométrique de trois points colinéaires de la Courbe E nous obtenons la relation :

$$P+O_E+O_E = O_E+P+O_E = P \quad \text{. pour tout point P de E} \qquad (1)$$

L'axiome de l'élément neutre est vérifié.

2) La parallèle à l'axe O*y* passant par un point P de E coupe la Courbe en trois points colinéaires de somme nulle :

$P+R+O_E = O_E$;

Il en résulte le symétrique de P qui est le point R=-P :

3) Toute sécante P_1P_2 de la Courbe E est confondue avec la sécante P_2P_1.

L'axiome de commutativité est vérifié

$$(P_1+P_2)+P_3= (P_2+P_1)+P_3= O_E \ ; \quad (3)$$

Il en résulte la relation de commutativité

$P_1+P_2 = P_2+ P_1$, pour tous points P_1 et P_2 de la Courbe E. (4)

4) Pour vérifier l'axiome d'associativité de la loi il n y a pas de propriété géométrique ; il faut calculer les sommes :

$$P_1+P_2=M_1 \ ; \qquad M_1+R=R_1, \qquad P_2+R=M_2 \qquad \text{et} \quad P_1+M_2=R_2 .$$

Alors, nous obtenons l'égalité:

$$(P_1+P_2)+R=P_1+(P_2+R) , \qquad (5)$$

qui vérifie l'axiome d'associativité :

$$(P_1+P_2)+R =P_1+(P_2+R)=P_1+P_2+R$$

o

Définition 1: *le groupe abélien E(K) est le groupe de Mordell-Weil de la Courbe Elliptique E.*

Pour montrer que ce groupe E(K) est de type fini nous utilisons des fonctions hauteurs sur un groupe abélien ,[13-3] et [23].

1-2 ***Définition 2*****:** *une hauteur sur un groupe abélien additif A est une fonction* $h:A \longrightarrow IR^+$ *à valeurs réelles positives , qui satisfait les trois axiomes:*

(haut 1) à tout point P_1 *de A on peut associer une constante* $c_1(P_1,A)= c_1$ *telle que .*

$h(P_1 +R)=2h(R)+c_1$ *, pour tout point R de A ;*

(haut 2) il existe un entier naturel $m\geq 2$ *et une constante* c_2 *tels que :* $h(mR) \geq m^2h(R) - c_2$ *pour tout point R de A ;*

(haut 3) tout ensemble de points de A de hauteur bornée est fini : l'ensemble $\{R \in A; h(R) \leq c_3\}$ *est fini.*

Cette fonction hauteur est utilisée pour démontrer qu'un groupe abélien A tel que le groupe quotient A/mA est fini , est de type fini :

Proposition 2

Soit un groupe additif abélien A , un entier naturel $m\geq 2$ *tel que le groupe quotient A/mA soit fini et une fonction hauteur : h: A* $\longrightarrow IR+$*. Alors le groupe abélien A est de type fini .*

Preuve :

Considérons un système de représentants des classes de A/mA. $R_1,R_2,.....,R_s$ (1)

Construisons une suite infinie de points :$P,P_1,P_2,\ldots,P_n,\ldots$ de A

,$P=mP_1+R_{i1}$, $P_1=mP_2+R_{i,2}$, ..., $P_{n-1}=mP_n+R_{i,n}$, pour des indices i,n compris entre 1 et s: (2)

Prenons une combinaison linéaire de (2) .

$mP_{t+1} = P_t - R_{i,t}$ (3)

appliquons à la relation (3) l'axiome (haut2) à gauche et l'axiome (haut 1) à droite :

$m^2h(P_{t+1}) \leq 2h(P_t)+c_1$; (4)

Avec les inégalités (4) pour t=1,2,.....,n nous obtenons :

$h(P_n) \leq (2/m^2)\, h(P)+(m^{-2}+....+m^{-2n})c_4$, $c_4(c_1,c_2)$ (5)

L'hypothèse $m \geq 2$ et (5) impliquent l'inégalité

$h(P_n) \leq u(n)h(P)+m^{-2}\,(1+m^{-2})^{-1}$ avec $\lim_{n \to +\infty} u(n)=0$ (6)

Il en résulte que la hauteur $h(P_n)$ est bornée (7)

L'axiome (haut3) et (7) impliquent que l'ensemble de points $\{P_1, P_2...., P_n\}$ est fini ; (8)

Il en résulte que le groupe A est engendré par les points $R_1,R_2,....,R_s$ de (1) et $P_1,P_2....,P_r$ de (8):tout point P de A est une Z -combinaison linéaire .

$P=n_1P_1+....+n_sR_s+k_1P_1+....+k_r P_s$, (9) avec n_i et $k_j \in Z$

Donc le groupe abélien A est de type fini .

o

L'algorithme décrit dans la preuve est semblable à l'algorithme de descente infinie de FERMAT . FERMAT à utilisé une telle descente pour étudier certains problèmes d'arithmétique.

A titre d'exemple , utilisons cette descente infinie de Fermat pour montrer que le nombre $\sqrt{3}$ n'est pas rationnel.

Utilisons un raisonnement par l'absurde.

Supposons que ce nombre est rationnel : $\sqrt{3} = a/b$ (1)

a et b sont deux entiers rationnels premiers entre eux ; (2)

En élevant au carré les deux membres de (1) , nous obtenons l'équation diophantienne :

$a^2 = 3b^2$ (3)

Par un théorème de divisibilité de Gauss ; 3 divise a^2 .

$a=3a_1$ (4)

(3) et (4) impliquent l'équation diophantienne $b^2 = 3a_1^2$ (5)

Le théorème de divisibilité de Gauss et (5) impliquent l'équation diophantienne $b=3b_1$ (6)

Cet algorithme fournit 2 suites infinies d'entiers :

$a=3a_1$; $a_1 = 3a_2$, ...; $a_n = 3a_{n+1}$,.... (7)

et $b=3b_1$, $b_1 = 3b_2$, ..., $b_n = 3b_{n+1}$; .... (8)

Ce résultat est en contradiction avec l'hypothèse a et b sont des entiers rationnels premiers entre eux .

Donc la supposition " $\sqrt{3}$ est rationnel " est absurde.

Le nombre $\sqrt{3}$ n'est pas rationnel ; c'est un nombre algébrique irrationnel quadratique.

o

La proposition 1 s'applique aux groupes de Mordell-Weil E(K) des Courbes Elliptiques .

1-3 Il existe plusieurs types de hauteurs sur les Courbes Elliptiques Citons -en deux.

***Définition* 3** : *la hauteur de Weil d'une Courbe Elliptique E est la fonction* $h_W: E(Q) \longrightarrow IR+$ *de valeur* $h_W(P) = \log \max \{|a|, |b|\}$ *pour tout point*

P=(x,y) de E ; x =a/b et $h_W(O_E)=0$

***Définition* 4**. *la hauteur de Néron-Tate (hauteur canonique) d'une Courbe Elliptique E est la fonction :*

$\hat{h}: E(K) \longrightarrow IR+$

de valeur $\hat{h}(P)= \frac{1}{\deg f} \lim_{n\to-\infty} 4^{-n} h_f(2^n P)$

où f est une fonction paire et h la fonction logarithmique .

Cette hauteur est indépendante de f .Elle possède des propriétés énoncées dans la

Proposition 3

Soit une Courbe Elliptique E/K et la hauteur de Neron-Tate $\hat{h}$ *. Alors :*

1)pour tous points P et R de E(K) :

$\hat{h}(P+R)+\hat{h}(P-R)=2\hat{h}(P)+2\hat{h}(R);$

c'est la loi du parallélogramme.

2) $\hat{h}(mP)=m^2\hat{h}(P)$ *pour tout entier m* ≥ 2 *et P* $\in$ *E(K) ;*

3) $\hat{h}$ *induit une forme quadratique sur E*

$\langle .,. \rangle : E(K_{alg}) \times E(K_{alg}) \to \mathbb{R}^+$;

$\langle P,R \rangle = \hat{h}(P+R) - \hat{h}(P) - \hat{h}(R)$; *pour tous points* $P, R \in E(K)$

4) $\hat{h}(P)\geq 0$; $\hat{h}(P)=0$ *si et seulement si P est un point de torsion* $mP = O_E$

Preuve

C'est un théorème de Néron-Tate (Théorème 9-3 ,[26])

o

La structure Algébrique du groupe de Mordell-Weil E(K) dépend du groupe de torsion T(E(K)) et des générateurs P_1,P_2 ,....,P_r de la proposition 2.

Proposition 4

Le groupe de Mordell-Weil E(K) d'une Courbe Elliptique E est isomorphe à un produit direct : $E(K) \approx T(E) \times Z^r$

ou T(E)=groupe de torsion de E et Z^r = r copies du groupe additif abélien infini Z.

***Définition* 5** : *l'entier r=r(E) de l'isomorphisme ci-dessus est le rang arithmétique de la Courbe Elliptique E , c'est le nombre de points $P_1,\ldots,P_r$ d'ordre infini et indépendants qui engendrent la partie E(K)-T(E) infinie* .

Le rang r(E) est donc un entier naturel ≥ 0.

Le calcul de cet invariant ne s'obtient pas avec une formule du type rang du groupe des unités d'un corps de nombres algébriques .

2-Coordonnées des points -P, P_1+P_2 et mP.

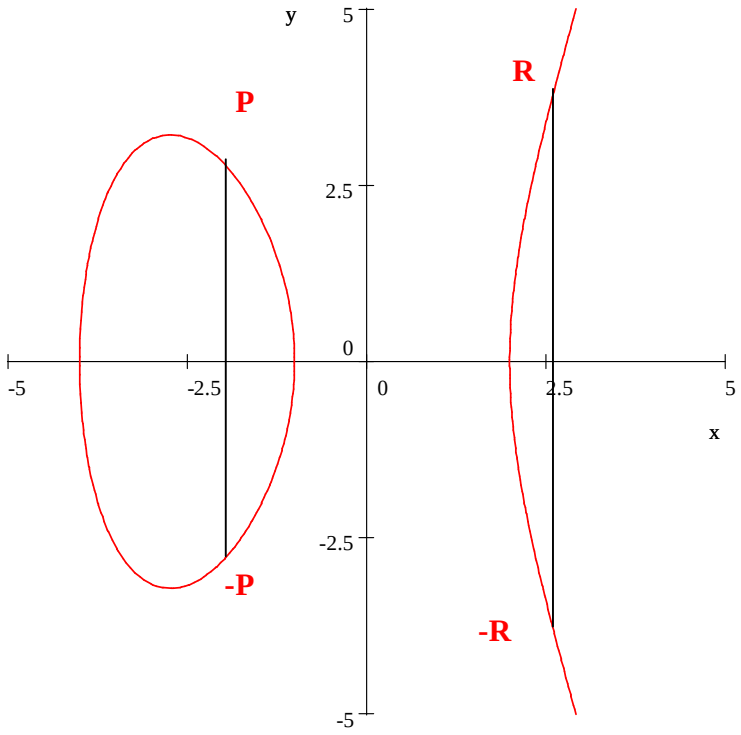
2-1 Le symétrique -P d'une Courbe Elliptique E s'obtient avec l'équation de la parallèle à Oy passant par $P=(x_P,y_P)$ et l'équation de Weierstrass

$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x,y]$. (1)

Pour $x=x_P$, cette équation du deuxième degré en y admet deux racines $y_1=y_P$ et $y_2=y(-P)$ (2)

Leur somme est égal à :

$y_1+y_2=-a_1x_P-a_3$; (3)



Il en résulte les coordonnées de –P :

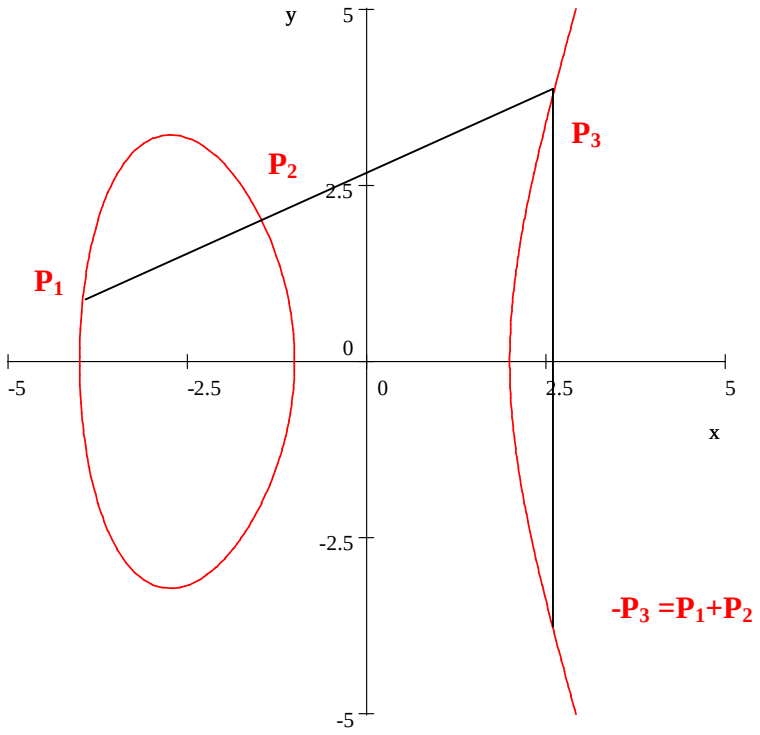
$x(-P)=x_P$,$y(-P)= -y_P - a_1x_P - a_3$ (4)

2-2 Soient deux points $P_i=(x_i,y_i) \in E(K)$ et $P_1 \neq \pm P_2$

Alors la sécante P_1P_2 coupe la Courbe E en un troisième point P_3: $P_1+P_2+P_3 = O_E$ (5)

Equation de la sécante P_1P_2

$$y = t\,(x - x_1) + y_1 \quad , \text{et} \quad t = \frac{y_1 - y_2}{x_1 - x_2} \qquad (6)$$



L'équation de Weierstrass (1) devient une équation cubique en x qui admet trois racines simples x_1, x_2, x_3, (7)

La somme de ces trois racines est égale à :

$$x_1 + x_2 + x_3 = t^2 + a_1 t - a_2 \quad ; \qquad (8)$$

Il en résulte les coordonnées du P_3

$$x_3 = t^2 + a_1 t - a_2 - x_1 - x_2$$

$$y_3 = t\,(x_3 + x_1) \qquad (9)$$

La somme $P_1+P_2=M$ est le symétrique $-P_3$ du point P_3 .Avec le calcul j'obtiens les coordonnées du point $M=P_1+P_2$

$$\left.\begin{array}{l} x_M = t^2 + a_1 t - a2 - x_1 - x_2 \quad \text{avec} \quad t = \dfrac{y_1 - y_2}{x_1 - x_2} \\ y_M = -t^3 - 2a_1 t^2 + (a_2 - a_1^2 + 2x_1 + x_2)t + a_1 a_2 - a_3 + a_1(x_1 + x_2) - y_1 \ ; \end{array}\right\} (10)$$

2-3 Pour obtenir les coordonnées du point 2P =P+P j'utilise la tangente à la Courbe E au point P

Equation de la tangente en $P=(x_P,y_P)$:

$y=y'(x-x_P)+y_P$ avec

$$y'=\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} \quad (11)$$

Avec l'équation de Weierstrass de E j'obtiens les coordonnées :

$x_{2P}= y_P'^2 + a_1y'_P-2x_P$;

$y_{2P}=- y_P'^3 - 2a_1y_P'^2 + (a_2 + a_1^2 + 3x_P)y'_P+a_1a_2 - a_3 + 2a_1x_P - y_P$;

avec $y'= \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$;(12)

Les résultats (4) , (10) , et (12) sont rassemblés dans la

Proposition 4

Soit une Courbe Elliptique E d'équation de Weierstrass

$E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \in K[x,y]$.

1)les coordonnées du symétrie -P d'un point $P=(x_P,y_P)$ de E sont égales à: $x(-P)=x_P$ et $y(-P)=-y_P-a_1x_P-a_3$;

2)les coordonnées de la somme $P_1+P_2=M$ de deux points $P_1\neq\pm P_2$ sont égales à :

$x_M=t^2+a_1t-a_2-x_1-x_2$; avec $t=(y_1-y_2)/(x_1-x_2)$.

$y_M=-t^3-2a_1y^2+(a_2-a_1^2+2x_1+x_2)t+a_1a_2-a_3+a_1(x_1-x_2)-y_1$,

3) les coordonnées du point 2Psont égales à:

$P=(x_P,y_P)$, $2P=(x_{2P},y_{2P})$ avec $y'=((3x^2+2a_2x+a_4-a_1y)/(2y+a_1x+a_3))$;

$x_{2P}=y'^2(P)+a_1y'(P)-a_2-2x_P$,

$y_{2P}=-y'^3(P)-2a_1y'^2(P)+(a_2-a_1^2+3x_P)y'(P)+a_1a_2-a_3+2a_1x_P-y_P$

o

2-4- pour tout point P d'une Courbe Elliptique E le symbole mP signifie mP=P + P +...+P, m fois P pour m > 0;

mP =(-P) + (-P) +...+ (-P) , -m fois (-P) pour m négatif

et $0.P=O_E=(\infty,\infty)$ pour m=0.

Dans (4) nous trouvons des formules pratiques mP pour une équation de Weierstrass $y^2=x^3+Ax+B$.

***Proposition 5*:(Lemme 7-2,(4))**

Soit une Courbe Elliptique E d'équation de Weierstrass .

E: $y^2=x^3+Ax+B \in Z[x,y]$ *, avec* $4A^3+27B^2\neq 0$

Soit un entier rationnel m et un point $mP=(x_m,y_m)$

Alors les coordonnées de mP sont des fractions rationnelles .

$$x_m = \frac{\phi_m}{\psi_m^2} \quad et \quad y_m = \frac{\theta_m}{\psi_m^3}$$

Les ψ_m *sont des polynômes satisfaisant les relations :*

$$\psi_{-1} = -1 \ ,$$

$$\psi_0 = 0 \ ; \psi_1 = 1 \ ; \psi_2 = 2y \ ; \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \text{ et}$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 + 4Ax - 8B^2 - A^3$$

formules de recurrence :

$$\psi_{2m} = 2\psi_m(\ \psi_{m+1}\psi_{m-1} - \psi_{m-2}^2\psi_{m+1}^2).$$

$$\psi_{2m+1} = \ \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3) \quad pour \quad m \geq 2$$

Les polynômes numérateurs satisfont les relations

$$\phi_m = x\psi_m^2\psi_{m+1} \ ;et$$

$$4y\theta_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-1}\psi_{m+1}^2 \ pour \ m \geq 1$$

o

3-Groupe de torsion des Courbes Elliptiques

Dans l'Algèbre Générale , un point de torsion dans un groupe G d'élément neutre e est un point g de G tel que mg=e pour un certain entier m.

***Définition* 5**: *le sous groupe de m-torsion d'une Courbe Elliptique E est l'ensemble des points P de E :*

$E[m]=\{ P \in E ; mP = O_E\}$

L'ensemble des points P d'ordre fini est la réunion des points P de torsion .

***Définition* 6**: *le groupe de torsion d'une Courbe Elliptique E est l'ensemble des points d'ordre fini.*

$T(E)=\{P \in E ; mP=O_E, m \text{ fini}\}$

Tous les groupes de torsion T(E) déterminés sont finis .La structure de ces groupes dépend du corps de base de la Courbe Elliptique .

Proposition 6 (Théorème de Mazur , [14])

Le groupe de torsion d'une Courbe Elliptique E/Q est un groupe abélien additif fini isomorphe à l'un des 15 groupes abéliens additifs :

Z/nZ pour $1\leq n\leq 10$ *et* $n=12$ *;* $Z/2Z \times Z/2dZ$ pour $1\leq d\leq 4$

Preuve :" dans [14] p 129-162)"

o

Pour l'équation de Weierstrass $y^2=x^3+Ax+B$, il y a la

Proposition 7 (Théorème de Lutz)

Soit une Courbe Elliptique de Weierstrass $y^2=x^3+Ax+B \in Z[x,y]$ *avec* $4A^3+27B^2 \neq 0$,

Tout point de torsion P=(x,y) a des coordonnées entières , $x, y \in Z$ *, Il y a deux cas possibles:*

Soit $2P=O_E$, *soit* y^2 *divise* $4A^3+27B^2$

Pour une autre équation particulière de Weierstrass il y a la

o

Proposition 8

Soit une Courbe Elliptique E d'équation de Weierstrass

$E:y^2=x^3+d \in Q[x,y]$

Alors son groupe de torsion est de la forme :

$T(E(Q)) \approx \{O_E\}$ *si d n'est ni un carré ni un cube ;*

$\approx Z/2Z$ *si d est un cube et* $d \neq 1$

$\approx Z/3Z$ *si d est un carré et* $d \neq 1$

$\approx Z/6Z$ *si d=1 et d =-432*

4-ISOMORPHISME DES COURBES ELLIPTIQUES

Soit deux Courbes Elliptiques sur un corps K de carac(K) $p \neq 2,3$, l'isomorphisme de E et E' se présente dans la :

Proposition 9 (d'après [23])

Soit une Courbe Elliptique E d'équation de Weierstrass ;

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in K[x; y]$$

Soit le changement de variables

$x=u^2X+r$ *et* $y=u^3Y+su^2X+t$ *, avec* $u,r,s,t \in K$ *et* $u \neq 0$

Alors la transformée de la Courbe Elliptique E est une Courbe Elliptique E' d'équation de Weierstrass:

$E':Y^2+a'_1XY+a'_3Y=X^3+a'_2X^2+a'_4X+a'_6 \in K[X,Y]$.

Les coefficients et les invariants des Courbes Elliptiques isomorphes sont liés par des relations que l'on obtient par le calcul avec les formules du

changement de variables

Preuve :elle est obtenue par le calcul avec les formules du changement de variables

o

Soit deux Courbes Elliptiques E,E' isomorphe , il y a des relations entre les coefficients et leurs invariants que nous allons déterminer:

4-1 Relation entre les cœfficients a_i et a'_i :

u $a'_1 = a_1 + 2s;$

u^2 $a'_2 = a_2 - sa_1 + 3r - s^2;$

u^3 $a'_3 = a_3 + ra_1 + 2t;$

u^4 $a'_4 = a_4 - s\,a_3 + 2ra_2 - (rs + t)a_1 + 3r^2 - 2st;$

u^6 $a'_6 = a_6 + ra_4 - ta_3 + r^2a_2 - rta_1 - t^2;$ (Is-1)

Relations entre les invariants b_{2i} et b'_{2i};

u^2 $b'_2 = b_2 + 12r;$

u^4 $b'_4 = b_4 + rb_2 + 6r^2;$

u^6 $b'_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3;$

u^8 $b'_8 = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4;$ (Is-2)

Relations entre les invariants c_{2i} et c'_{2i};

u^4 $c'_4 = c_4$ et u^6 $c'_6 = c_6;$ (Is-3)

Relation entre les discriminants u^{12} $\Delta(E') = \Delta(E);$ (Is-4)

Relations entre les invariants modulaires: j(E') = j(E); (Is-5)

Les points neutres sont dans la même classe du plan projectif IP^2 :

$O_{E'} = O_E = (0, 1, 0);$

4-3 ISOGENIES des COURBES ELLIPTIQUES

***Définition* 7 d'après SHIMURA [22]:** *soit deux Courbes Elliptiques E et E' sur le même corps K, d'éléments neutres respectifs* O_E *et* $O_{E'}$ *, de groupes de Mordell- Weil E(K) et E'(K).Une isogénie de E sur E' est un homomorphisme*

λ : *E(K)* $\longrightarrow$ *E'(K) qui satisfait les conditions :*

1) $\lambda(O_E) = O_{E'}$;

2) $\lambda \neq 0$;

3) λ *est surjectif;*

4) le noyau de λ *est un sous groupe fini de E(K);*

5) $\lambda(P + R) = \lambda(P) + \lambda(R)$ *pour tous points P et R du groupe E(K).*

Par la théorie des morphismes de Variétés, les conditions (1),(2),(3) et (4) sont équivalentes.

Une isogénie possède des invariants :un degré et une isogénie duale .

***Définition* 8:1)** *lorsqu'une Courbe Elliptique E est isogène à une courbe E', le noyau de cette isogénie est un sous groupe fini du groupe E(K) le degré de l'isogénie* λ *est égal à l'ordre de ce noyau*

2) *l'isogénie duale d'une isogénie de degré d :* λ *:E(K)→E'(K) est le morphisme de groupes :* λ' *:E'(K)* $\longrightarrow$ *E(K) qui satisfait les 2 composées :* $\lambda\lambda'$ *est la multiplication par d sur E'(K) et* $\lambda'\lambda$ *est la multiplication par d sur E(K).*

A chaque isogénie est associée une isogénie duale par la.

Proposition 10

Soit deux isogénies $\lambda : E(K) \to E'(K)$ *et* $\mu : E'(K) \to E_1(K)$

1) la composée : $\mu\lambda : E(K) \to E_1(K)$ *est une isogénie de Courbes*

Elliptiques;

2) les degrés des isogénies satisfont les relations:

$$deg(\lambda) = \deg(\hat{\lambda}) \quad et \quad deg(\mu) = deg(\hat{\mu}) .$$

Preuve [30]

o

Proposition 11

Soit un entier rationnel m , premier à carac(K) d'un corps K , une Courbe Elliptique E de groupe E(K) de Mordell-Weil . Alors, la multiplication:

$$t_m : E(K) \to E(K), \quad de\ valeur$$

$$t_m(P) = mP \quad est\ une\ isogénie\ de\ degré\ m^2.$$

Preuve [23]

o

L'ensemble des Courbes Elliptiques isogènes à une courbe E est fini.

***Définition* 9** *les Courbes Elliptiques isogènes à une courbe elliptique E , sur un corps K, forment une classe d'isogénie de E .*

4-3 EXEMPLES deVelu [25]

Soit une Courbe Elliptique E d'équation de Weierstrass:

E : $y^2 + y = x^3 ? x^2 ? 10x ? 20$ 5 ¥ßx, yà

Invariants :discriminant AÝEÞ = ?11 et conducteur N(E)=11^2.

Le point L = (5;5) du groupe E(Q) engendre un sous groupe F d'ordre 5:

F=$\{L; 2L = (16,-61); \ 3L = (16; 60); \ 4L = (5;-6); 5L = O_E)\}$

Equations de l'isogénie :

E(Q) → E'(Q) = E(Q)/F.

$$x \quad \to \quad x + \frac{110}{x-5} + \frac{121}{(x-5)^2} + \frac{12x121}{x-16} + \frac{121^2}{(x-16)^2};$$

$$y \quad \to \quad y - \frac{121(2y+1)}{(x-5)^3} - \frac{110y+55}{(x-5)^2} - \frac{121^2(2y+1)}{(x-16)^3} - \frac{132y+726}{(x-16)^2} \quad .$$

Velu a obtenu l'équation de la courbe isogène :

E' : $y^2 + y = x^3 - x^2 - 7820x - 263580$; AÝE$^{\vee}$þ = ?11^5.

5-Réduction des Courbes Elliptiques

La réduction d'une Courbe Elliptique est basée sur la théorie des valuations d'un corps de nombres que l'on trouve dans les ouvrages de Théorie Algébrique des Nombres .

Dans la suite , nous nous limitons à un bref exposé.

5-1 Valuations d'un corps de nombres.

***Définition* 10** : *une valuation d'un corps K est une fonction*

$v : K \longrightarrow IR^+$

Qui satisfait les trois axiomes :

(val 1) v(x) ≥0 pour tout élément x du corps ; v(x)=0 si et seulement si x=0;

(val 2) v(xy) = v(x).v(y) pour tous éléments x et y de K ;

(val 3) il éxiste une constante réelle positive c telle que v(x)≤1 implique v(x+1) ≤c.

Donc une valuation est un homomorphisme des groupes multiplicatifs K^* et IR^* .

Exemples

1)K=corps IR des nombres réels ; v(x)= max{x,-x }; c'est la valeur absolue d'un nombre réel x.

L'axiome (val 3) est satisfait pour c=2

$v(x) \leq 1$ implique $v(x+1) \leq 2$

2) Valuation p-adique du corps Q des nombres rationnels pour tout nombre premier p :

$v_p(p)=1/p$ et $v_p(q)=1$ pour tout nombre premier $q \neq p$.

L'axiome (val3) est satisfait pour c=1 ,

$v_p(x) \leq 1$ implique $v_p(x+1) \leq 1$.

3) Valuation triviale d'un corps K.

v (x)=1 pour tout nombre $x \neq 0$ de K et v(0)=0

5-2 Classification des valuations d'un corps

Elle dépend de la valeur de la constante c de l'axiome (val 3)

***Définition* 11**

Une valuation $v: K \longrightarrow IR^+$ *est archimédienne si elle satisfait la relation*

v(x) $1 \leq$ *implique v(x+1)* $\leq$ *2 pour tout élément x de K.*

Une valuation $v:K \longrightarrow IR+$ *est non archimédienne si elle satisfait la relation:*

v (x) ≤ 1 *implique v(x+1)* $\leq$ *1 pour tout élément x de K*

Ainsi, la valeur absolue v(x) =max {x,-x} est une valuation archimédienne : les valuations p-adiques sont des valuations non archimédiennes

Il en résulte la structure de l'ensemble V(K) des valuations d' un corps K :

$V(K) = V_\infty(K) \cup V_O(K)$,

Où $V_\infty(K)$= {valuation archimédienne de K }et $V_O(K)$ ={ valuation non archimédienne de K}

On démontre que

1) toute valuation archimédienne est équivalente à la valeur absolue

2) Toute valuation non archimédienne est équivalente à une valuation p-adique .

***Définition* 12** :*une valuation* $v:K \longrightarrow IR^{+}$ *est discrète si l'image v(K) est discrète ,alors v(K) est isomorphe à Z ou un sous groupe de Z*

5-3 Réduction d'une Courbe Elliptique .

Soit une Courbe Elliptique E d'équation de Weierstrass :

E: $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \in Q[x,y]$ (1)

Pour tout nombre premier p introduisons la réduction modulo p :

$n \longrightarrow \bar{n}$, congru à n mod p. (2)

Alors la Courbe réduite $\bar{E}$ modulo p est une Cubique de Weierstrass :

$E: \bar{y}^2 + \bar{a}_1\bar{x}\bar{y} + \bar{a}_3\bar{y} = \bar{x}^3 + \bar{a}_2\bar{x}^2 + \bar{a}_4\bar{x} + \bar{a}_6$ $E: \in IF_p[\bar{x}, \bar{y}]$;(3)

Ses invariants sont réduits modulo p

$\bar{b}_{2i}$, $\bar{c}_{2i}$, $\Delta(\bar{E})$, $j(\bar{E})$, etc.... (4)

Il en résulte une classification des réductions

Définition* 13 :Soit une Courbe Elliptique E , et sa réduction modulo un nombre premier p.*

1) *la réduction est bonne si la Courbe réduite* $\bar{E}$ *est une Courbe Elliptique*

2) *la réduction est mauvaise si la Courbe réduite* $\bar{E}$ *est singulière , elle est multiplicative si elle admet un noeud ; elle est additive si elle admet un point de rebroussement.*

Autre vocabulaire :réduction stable (bonne) , semi stable (multiplicative) et instable (additive).

5-4 Application

Cubique E(5,8) de la famille E(t,m) .

$y^2+8xy=x^3-16x^2-24x-8 \in Q[x,y]$

Appliquons une réduction v_p modulo p

Pour p=3 , la Courbe réduite a pour équation :

$$\overline{E}_3(5,8): y^2+2xy=x^3+2x^2+1 \in IF_3[x,y]$$

Calcul des invariants:

$b_2=0$, $b_4=0$, $b_6=1$, $b_8=0$, $\Delta(\overline{E}) = 0$ *et* $c_4(\overline{E}) = 0$

Il en résulte que la Courbe réduite $\overline{E}_3$ est singulière avec un point de rebroussement.

Cette réduction v_3 est additive, donc instable

Pour p=7 , la Courbe réduite a pour équation:

$$\overline{E}_7 : y^2 + xy = x^3 + 5x^2 + 4x + 6 \in IF_7[x, y]$$

Calcul des invariants :

$b_2=0$; $b_4=1$, $b_6=4$, $b_8=4$, $\Delta\left(\overline{E_7}\right) = 3$;

donc la Courbe réduite modulo 7 est une Courbe Elliptique .

Cette réduction est bonne , donc elle est stable .

Pour p=11 , la Courbe réduite a pour équation :

$$\overline{E}_{11} : y^2 + 8xy = x^3 + 6x^2 + 9x + 3 \in IF_{11}[x, y]$$

Calcul des invariants :

$b_2=0$; $b_4=7$, $b_6=1$, $b_8=7$, $\Delta\left(\overline{E_{11}}\right) = 1$, $c_4(\overline{E}) = 8.$

Il en résulte que cette réduction est bonne .

Ces réductions modulo un nombre premier p nous conduisent à l'étude des Courbes Elliptiques sur les corps finis IF_q à $q=p^n$ éléments.

Chapitre V: Application à la CRYPTOLOGIE

Selon les spécialistes, la cryptologie actuelle utilise la Théorie des Corps finis et la Théorie des Courbes Elliptiques .C'est par les Corps que nous commençons ce chapitre.

1-Structure algébrique des corps finis

Un corps fini est un corps qui contient un nombre fini q d'éléments dont les éléments neutres O et 1 des deux opérations " addition" et multiplication".Ce nombre q est une puissance $q=p^n$ d'un nombre premier p.

Proposition 1

Tout corps fini IF_q contient un sous corps premier fini $IF_p=Z/pZ$ pour un nombre premier $p\geq 2$ et $q=p^n$

Tout corps fini IFp possède une structure de IFp- espace vectoriel d'après l'algèbre linéaire.

o

Proposition 2

Pour tout nombre premier $p\geq 2$ et $q=p^n$, $n\geq 1$, le corps fini IF_q est un IF_p- espace vectoriel de dimension n.

Tout élément x de IF_p est une combinaison linéaire d'une base $e_1, e_2, \ldots, e_n$, de la forme: $x=a_1e_1+a_2e_2+\ldots+a_n e_n$, avec $a_1, a_2, \ldots, a_n$ dans IF_p .

o

D'après l'Algèbre des polynômes ; tout corps fini IF_q est le corps de décomposition d'un polynôme $f(x) \in IF_p[x]$ de degré q

$F(x)= x^q-x=x.g(x)$ avec $g(x)=x^{q-1}-1$

Ce polynôme admet q racines $x_1=0$, $x_2,\ldots,x_n=1=e$.

La nature de ces racines est déterminée par la dérivée $f'(x)=qx^{q-1}-1$, la valeur $f'(x)\equiv 0 \bmod q$, $f'(x)=qx^{q-1}-1$ et $f'(1)=q-1\equiv 0 \bmod q$ implique que les q racines $x_1,x_2,\ldots,x_n$ sont simples.

Les nombres entiers $a \in Z$ premiers à l'entier rationnel q satisfont la fonction arithmétique d'Euler .

2-Arithmétique : fonction d'Euler, congruences, théorème des restes Chinois

***Définition* 1 :**

la fonction arithmétique d'Euler est la fonction $\varphi : Z \longrightarrow IN$, *de valeur* $\varphi(n)$ *=nombre des entiers a>0 premiers à n et inférieurs à n .*

Tableau de petites valeurs $\varphi(n)$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6

Toutes les valeurs $\varphi(n)$ peuvent être calculées avec la :

Proposition 3

La fonction arithmétique φ *d'Euler satisfait les propriétés :*

1) $\varphi(1)=1$; $\varphi(p)=p-1$ *et* $\varphi(p^r)=(p-1)p^{r-1}$ *pour tout nombre premier p,*

2) $\varphi(2n)=\varphi(n)$*pour tout entier impair n:*

3) $\varphi(m.n)=\varphi(m).\varphi(n)$ *pour tous entiers m et n premiers entre eux,*

4) $\varphi(n)$ *est un entier pair pour tout entier n>1.*

o

Cette fonction φ d'Euler permet de déterminer les éléments inversibles d'un corps finis IF_q

Proposition 4

Les éléments inversibles d'un corps fini IF_q *,* $q=p^n$ *, forment un groupe multiplicatif cyclique* $IF^{\times}_q$ *d'ordre* $\varphi(q)$*:*

$IF^{\times}_q = \{g, g^2, \ldots, g^{\varphi(q)} = 1\}$

o

La recherche d'un tel générateur g peut être menée à l'aide d'un algorithme de puissance $a, a^2, \ldots, a^n = \pm 1$

Exemple :corps fini IF_q pour $q=5^2$.

Alors $\varphi(q)=20$.

Nous obtenons $2^{10}=-1$; $3^{10}=-1$,$6^5=1$,$7^2=-1$;

Il en résulte les deux générateurs g=2 et g=3 de $IF^{\times}_q$.

Les entiers a=6 et b=7 engendrent seulement des sous groupes du groupe multiplicatif IF_q .

Théorie des congruences

Dans une congruence linéaire de degré 1.

$ax=b \bmod(q)$ (1)

les entiers a et b sont premiers entre eux .

Les racines de cette congruence (1) dépendent du p g c d des entiers a et q:soit m=pgcd(a,q), alors a=m a' et q=mq' avec a' et q' premiers entre eux.

Il y a deux cas possibles:

1) a est premier au module q alors il y a une seule solution

2)pgcd(q,a)=m >1 , alors ma'x=b+mq't ,

a) si m ne divise pas b , pas de solution,

b)si m divise b ; alors il y a m solution

Exemple 1:

$6\mathbf{x} \equiv 5 \bmod 11$

6 et 11 sont premier entre eux , la table de multiplication dans IF_{11} implique la relation $6 . 10 = 60 \equiv 5 \bmod 11$. je trouve la solution x=10

Exemple 2 .

$12x \equiv 8 \bmod 20$.

Alors pgcd(12,20)=4=d ,d=4 divise b=8 ,les racines sont $x_1=4$, $x_2=9$,$x_3=14$, $x_4=19 \bmod 20$.

Dans le cas de plusieurs congruences , nous pouvons utiliser un autre résultat.

Propositions 5 (**Théorème des restes chinois**)

Soit t entiers $m_1,m_2,....,m_t$ premiers entre eux deux à deux et le système de t congruences linéaires.

$x \equiv a_1 \bmod m_1$, $x \equiv a_2 \bmod m_2$, ... ,$x \equiv a_t \bmod m_t$.

Alors , ce système admet une solution y de la forme

$y=M_1d_1a_1+M_2d_2a_2+....+M_td_ta^t \bmod M$ *aec*

$M=m_1.m_2.m_3....m_t$, $M=\frac{M}{m_i}$, $M_id_i \equiv 1 \bmod m_i$;$i=1;2;3...,t$

Preuve dans des ouvrages de Théorie Analytique des Nombres (S.Lang, Léonard Eugène Dickson , etc…)

o

Exemple :

système de trois congruences

$x \equiv 2 \bmod 3$; $x \equiv 3 \bmod 5$ et $x \equiv 5 \bmod 8$.

Appliquons le théorème des restes chinois

Avec M=3 . 5 . 8=120

M_1=5 . 8=40 , M_2=3 . 8 =24, M_3=15

$M_i d_i \equiv 1 \bmod m_i$

Les congruences $40d_1 \equiv 1 \bmod 3$, $24d_2 \equiv 1 \bmod 5$, $15d_3 \equiv 1 \bmod 8$ admettent les solutions d_1=1 ,d_2=4 et d_3=5 , la solution du système est x=53.

Pour résoudre les congruences linéaires $ax \equiv b \bmod p$ .pour p premier ,il est pratique d'utiliser la table de multiplication modulo p .

Exemple :

Table de multiplication dans IF_{11} ; $a.b \equiv c \bmod 11$

b \ **a**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

3- Endomorphismes de Frobenius et Courbes Elliptiques sur un corps fini.

Ce sont des automorphismes particuliers des corps finis

***Définition* 2:**

L'endomorphisme de Frobenius d'un corps fini IF_q, pour $q=p^n$ et p premier est l'application : Frob :IF_q , de valeur frob(x)=x^p .

Proposition 6

Les automorphismes d'un corps fini IFq , pour $q=p^n$ et p premier. forment un groupe cyclique Aut(IFq) d'ordre n engendre par l'endomorphisme de Frobenius :

Aut(IFq)={ frob ,$frob^2$,....,$frob^n=Id$}

Preuve

Les puissances de frob ont pour image :

Frob(x)=x^p , $frob^2(x)=x^{p^2}$,…. ,$frob^n(x)=x^{p^n}=x$.

o

3-2 Soit une Courbe Elliptique E sur un corps fini IF_p:

$E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \in IF[x,y]$, $q=p^n$, p premier

Le nombre A_q de points rationnels de la courbe E peut être calculé avec [7] lorsque q=p premier :

$A_p=card\ (Z/Z_p)^{\times}=p-1$ ou

$A_p=card\ (Z/d_1Z \times Z/d_2Z)$, avec d_1 divise d_2 et d_2 divise p-1

Lorsque $q=p^n$ et $n\geq 1$, l'ordre du groupe E(IFq) a été évalué par Ogg et démontré par Hasse .

Proposition 7

Soit une Courbe Elliptique E sur un corps fini IF_q à $q=p^n$ éléments , p premier et $n \geq 1$.

1)l'ordre du groupe abélien E(IFq) est égal à :

A_q*=1+q-Tr(frob) ,où Tr = trace du Frobenius ,*

2)cet ordre satisfait les inégalités.

1) $1+q-2\sqrt{q} \leq A_q \leq 1+q+2\sqrt{q}$.

o

L'invariant "groupe de torsion $T(E/IF_q)$"classifie ces Courbes Elliptiques en deux classes :

1) Courbes Elliptiques ordinaires si :

$T(E/IF_q) \approx Z/qZ$,

2)Courbes Elliptiques supersingulièrs si $T(E/IF_q)$ est trivial;

Le discriminant de telles Courbes n'est pas nul: $\Delta(E) \neq 0$

Il existe d'autres critères pour trouver les Courbes Elliptiques supersingulières [SILVERMAN]

Exemple:

Courbe Elliptique E d'équation de Weirstrass :

E : $y^2=x^3-5x+4$ $IF_p[x,y]$

Calcul des invariants :

$b_2=0$,$b_4=-10$, $b_6=16$, $b_8=-25$, $c_4=240$ et $\Delta(E)=17_x64$

Pour p=3 , alors $\Delta(E)=2$ et $c_4=0$, la Courbe E/IF_3 est supersingulière

Pour p=7 , alors $\Delta(E)=3$ et $c_4=2$, la Courbe E/IF_7 est ordinaire .

4-La "science du secret " : la CRYPTOLOGIE

Les ouvrages traitant cette science sont nombreux ; nous en avons cité quelque uns dans la bibliographie.

***Définition* 3**

La CRYPTOLOGIE est la science des échanges secrets d'information entre deux individus A et B ; elle est formée de deux parties .

1) la CRYPTOGRAPHIE , discipline qui traite les codages et l'écriture secrète des messages échangés .

2) la CRYPTANALYSE , discipline qui vise la pénétration des messages secrets par le décodage illégal des codes d'émission de messages secrets entre deux individus A et B

4-1- Notions de CRYPTOGRAPHIE

On peut les trouver dans les ouvrages "Cryptography ", (1981), par Konhen A.G,"Applied Cryptography ",(1996), par Schneier B,"Cryptography ", (1994) par N.Koiblitz , "Elementary Number Theory and its applications " (1984) , par K.H.Rosen , etc….

Les procédes de codage sont basés sur l'arithmétique des corps finis .Le secret est préservé par des clefs publiques et privées

Nous indiquons quelques systèmes utilisés par les spécialistes

4-2 Système DIFFIE-HELLMAN (1976)

C'est un algorithme utilisé par deux individus A et B pour coder un message confidentiel .

Pour trouver une clef mutuelle A et B choisissent un nombre premier p et un générateur g du groupe multiplicatif IF^{x}_{p} .

A prend au hasard un entier a dans l'intervalle [2,p-2],

Alors le nombre $k_A=g^a \bmod p$ est une clef publique pour A.

L'individu B prend au hasard un entier b dans [2,p-2]

Alors le nombre $k_B=g^b \bmod p$ est une clef publique pour B.

La clef mutuelle est le nombre : $k_{AB}=g^{ab} \bmod p$.

Il faut ensuite mettre en œuvre le codage du message , sa signature , sa certification , etc,….

4-3 Systeme RSA (1978)

Il a été inventé par trois auteurs :**R**ivest, **S**hamir et **A**dleman .

Pour coder un message , il faut choisir deux nombres premiers p et q distincts.

La clef publique est le couple (N=pq , E) ; où ,E est un entier dans l'intervalle [3,N-2], premier au produit $\varphi(N)=(p-1)(q-1)$.

La clef privée est le nombre $D=E^{-1} \bmod (p-1)(q-1)$, c'est un nombre secret .

La difficulté provient de la factorisation de l'entier N en un produit N=pq de deux nombres lorsqu'on choisit un nombre N formé de plus de 10^6 chiffres par exemple .

Plusieurs méthodes de factorisation ont été utilisées : méthode de Fermat, méthode de Pollard, méthode de Lucas ; méthode de Lenstra , méthode des Courbes Elliptiques ; etc…. Les cryptographes utilisent un "jargon" spécial le message en clair à envoyer est le plaintext , le message chiffré est un cryptogramme (cipher text en anglais), il est chiffré à l'aide d'une clef de chiffrement (Public Key cryptographie en anglais), chiffrer (cipher en anglais) ;un cryptosystème est une paire d'algorithmes (enciphering et deciphering)

Un message en clair peut être condensé par une fonction de hachage : un envoi de message secret peut être accompagné d'une signature de l'émetteur A et d'un certificat de garantie.

Les autres expressions s'acquièrent à l'usage

4-4- Cryptographie Elliptique

Elle est basée sur les invariants des Courbes Elliptiques sur un corps fini IF_p : groupe abélien de Mordell-Weil $E(IF_p)$,discriminant , points d'ordre fini , groupe de torsion $T(E/IF_p)$,…

Un émetteur A veut envoyer un message secret M à un récepteur B .Il choisit une Courbe Elliptique E d'équation de Weierstrass :

$E:y^2=x^3+ax+b \in IF_p[x,y]$.

Les formules d'addition P_1+P_2 et 2P deviennent :

$P_i=(x_i,y_i)$, $P_1+P_2=M=(x_M,y_M)$, $P_1 \neq P_2$

$x_M=t^2+(2x_1+x_2)t-y_1$; $t=(y_1-y_2)/(x_1-x_2)$,

$y_M=-t^3+(2x_1+x2)t-y_1$,

Pour un point $P=(x_P,y_P)$ de E/IF_p alors $-P=(x_P,-y_P)$;

$2P=(x_{2P},y_{2P})$ avec $x_{2P}=y'^2_P-2x_P$, $y'=\frac{3x^2+a}{2y}$ et $y_{2P}=-y'^3_P+3x_Py'_P-y_P$.

A et B choisissent ensemble un point $P=(x_P,y_P)$ sur la Courbe Elliptique $E/IF_p[x,y]$.Alors $y'^2=x^3_P+ax_P+b$. A choisit une clef k_A inconnue de B , k_A est un entier modulo p puis il envoie à B les coordonnées du point k_A ;B choisit une clef k_B inconnue de A ; k_B est un entier modulo p; B envoie à A les coordonnées du point k_B P.

Chacun calcule les coordonnées du point k_Ak_BP.

Cependant la connaissance des coordonnées des points P et k_Ak_BP est insuffisante pour trouver les clefs k_A et k_B.

Pour cela ,il faut utiliser l'algorithme du logarithme discret .

5-Exemples

5-1 Exemple (Jacques Serres, CERIST,avril 2007 , Alger)

A et B choisissent la Courbe Elliptique E sur IF_{17}.

$E: y^2=x^3+x+1$ $IF_{17}[x,y$

Ils choisissent le point P=(0,1) sur $E(IF_{17})$

Ils se munissent de la table de multiplication sur le corps fini IF_{17} pour trouver les coordonnées des points 2P,3P,….,16P.

A choisit la clef secrète k_A =3 et calcule 3P=(4,16) ; il envoie 3P=(4,16) à B .

B choisit la clef secrète k_B=5 , calcule 5P=(16,4) et envoie 5P=(16,4) à A

La coïncidence (4,16)-(16,4) est fortuite

A calcule 3(16,4)=(4,1) et B calcule 5(4,16)=(4,1)

Aucun d'eux ne sait que la clef commune est égale à k_Ak_B=15

A et B peuvent calculer les coordonnées des points nP pour n=2,3,… pour trouver (4,1)

5-2 Exemple (R.Candall et C.Pomerance ...2002)

Deux individus A et B veulent échanger un message secret par la méthode des Courbes Elliptiques sur un corps fini IF_p; A choisit une Courbe Elliptique E d'équation de Weierstrass :

$E: y^2=x^3+ax+b \in IF_p[x,y]$, $f(x)=x^3+ax+b$

tel que $E(IF_p)$ soit d'ordre f r $=A_p$ et r un grand nombre premier

A cherche un point P=(x,y) sur $E(IF_p)$ d'ordre r ; il prend au hasard une clef privée $k_A \in$ [2,r-2], il calcule les coordonnées du point $k_AP=(x_1,y_1)$

Il calcule les nombres $R \equiv x \bmod r$ et $s \equiv k^{-1}_A(h(M)+Rk_A) \bmod r$; M est le message à envoyer à B , h est une fonction de hachage convenable .

A transmet le message M à B avec sa signature (R,s).

B connait l'équation de Weierstrass de la Courbe E , le point P=(x,y) , le nombre premier r et le point $k_AP=(x_1,y_1)$

B calcule les nombres $w \equiv s\text{-}1 \bmod r$, $u \equiv h(M)\, w \bmod r$,

$u_2 \equiv R$ w mod r , les coordonnées du point u_1 P $+u_2(k_A P)= (x_0,y_0)$ et le nombre $v \equiv x_0$ mod r

Lorsque v=R , alors B accepte la signature du message reçu , si non il la rejette .

Actuellement la tendance est de prendre des corps finis IF_q à $q = 2^r$ éléments formés des chiffres 0 et 1.

Exemple : IF_q $q=2^3$, donc nombre de 8 chiffres

A=10011010 et b=01010101 alors a+b=10001111

6-Prespectives

Je compte approfondir les techniques de la cryptographie ; il y a les Algorithmes de Diffie-Hellman ; les fonctions de Hachage , les fonctions d'authentification des messages transmis par un utilisateur ; la vérification de l'intégrité des messages ; la signature électronique ; la certification des clefs .

Plus tard j'aborderai le domaine de la cryptanalyse .Il faut étudier les "stream ciphers " modernes qui opèrent par bloc de 64 bits ou moins pour transformer des messages .

Il faut utiliser des méthodes de Théorie de Nombres pour trouver des générateurs de corps finis IF_p et pour factoriser des grands entiers (fractions continues ; théorème de Fermat ,.....).D'autre méthodes sont basées sur les Courbes Elliptiques sur les corps finis.

Signalons deux articles parus dans Lecture Notes in computer of Science n°3494(May 2005) qui enrichissent le domaine de la cryptographie

1)"Pratical cryptograph in High Dimensional " ; par Marten Van Dyk-Robert , Granger-Dan page- Kane Rubin-Alice Siherberg-Martyn Stam et David Woodruff.

2)" A fast Cryptanalysis of the Isomorphisms of Polynomials with one Secret Problem"; par Ludovic Perret.

[1].ARTIN-E-: Algebraic Numbers and Algebraic Functions - Gordon and Breach- New York-(1967)

[2]. APOSTOL-T-M-: Modular Functions and Dirichlet Series -2e Ed (1982)-GTM-41;

[3].BOREVICH,Z- and Shafarevich,I-R-:Théorie des Nombres-Gauthier Villars-Paris (1967

[4].CASSELS, J-W-S-: Equation Diophantine with Special References to Elliptic Curves- Lond. Math. Soc. (1965-66) 193-291.

[5].EDWARDS:Fermat's last Theorem-Graduate Text in Mathematics. 50(1977)

[6].HARTSHORNE,R-: Algebraic Geometry ; 3e Ed. - Springer-Graduate Texte in Mathematics 52(1983) QA565-H25.

[7]. HASSE, H-: Number Theory -Springer (1980)

[8].HELLEGOUARCH ,Y-: Invitation aux Mathématiques de Fermat- Wiles -2ème Edit.Masson-Paris (1997)

[9].HUSEMÖLLER : Elliptic Curves ; Graduate Text in Mathematics 111 (1987)

[10].KNAPP, A-W- : Elliptic Curves-Princeton Univ. Press , 40-New Jersey (1992)

[11] KOBLITZ,N-:

1)- :Introduction to Elliptic Curves and Modular Forms 2e Ed.(1984) G.T.M. 97.

2)- A course in Number Theory and Cryptography- 2eme Ed. (1988) G.T.M. 114-Springer 12-Kostrikine,A-I- and Shafarevich I-R- : Algebra I - Springer (1987) 12-XX-20-XX.

[12]. KNAPP, A-W- : Elliptic Curves -Princeton Univ. Press ,40-New Jersey (1992)

[13].LANG,S-

1)- Algebra ,Addison -Weisley (1965)

2)- Diophantine Geometry-Interscience-John Wiley (1962)

3)- Elliptic Curves- Diophantine Analysis -Springer (1978) AMS(1970)-10B45-10F99-14G25-14H2

4)- Cyclotomic Fields I and II - Springer Verlag -Graduate Text in Mathematics 59 et 69

[14]. MAZUR,B- : Rational isogenies of prime degree -Inv. Math. 44(1978) Page 129-162.

[15]. MUNFORD : Abelian Varieties - Oxford Uni. Press (1974)

[16]. MOMOSE,F- : Isogenies of prime degree over number fields – Compo. Math. 97 -North Holland (1995) 329-348.

[17]. OGG, A-P- :Elliptic Curves and wild ramification -Amer. Math. J. (1967)1-21.

[18]. ROBERT : Elliptic Curves - Lect. N. Math. 326 (1973)

[19].SCHAEFER, Ed,:An Introduction to Cryptography-Santa Clara University -USA(2000).

[20]. SERRE ,J-P, :Propriétés galoisiennes des points d'ordre fini des Courbes Elliptiques- Inventionnes. Mathematical. 15 (1972) 259 -331 .

[21]. SHAFAREVICH, I-R- : Basic Algebraic Geometry -Springer Verlag- Berlin-New York(1977).

[22].SHIMURA,G-: Introduction to the Arithmetic Theory of Automorphic Functions - Princeton University. Press – Publication of Mathematical Society Japan. n° 11(1971)

[23]. SILVERMAN ,J-H-:The Arithmetic of Elliptic Curves - Springer Graduate Texte in Mathematics. 106 (1986)

[24].TATE, J :

1) Endomorphism of Abelian Varieties over Finite Fields - Inv. Math. 2 (1966) 34-144.

2) The Arithmetic of Elliptic Curves - Inv. Math. 23 (1974) 179-206.

[25]. VELU,J :1) Isogénies entre Courbes Elliptiques-Compte Rendu de l'Academie des Sciences de Paris - (26 juillet 1971)p. 238-241.

[26]. WALKER, R,J,: Algebraic Curves-Springer Verlag (1978)

[27]. WEIL ,A :

1) Foundations of Algebraic Geometry - Publication. 29- American. Mathematical. Society- Providence (1946)

2) Courbes Algébriques et Variétés abéliennes - Hermann-Paris.(1970)

[28]. WEISS , Ed. :Algebraic Number Theory - Mac Graw Hill - New York - (1966)

[29]. ZARISKI and Samuel : Commutative Algebra Volumes I et II – Springer - Graduate Texte in Mathematics n° 28 et 29 .

[30].ZITOUNI ,M,: Courbes Elliptiques : Arithmétique - Geométrie - Algorithmique-ed.OPU-Alger(2007).