N° d'ordre : 19/2005-M / MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE D'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
« HAOUARI BOUMEDIEN »
FACULTE DE MATHEMATIQUES

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

EN : Mathématiques

Spécialité : Algèbre et Théorie des Nombres

Par : YOUMBAÏ Ahmed El Amine

Sujet

Conjecture de Birch et Swinnerton-Dyer et rang de courbes elliptiques

Soutenue le : **22 / 11 / 2005, devant le jury composé de :**

M. BEBBOUCHI Rachid	Professeur	(U.S.T.H.B)	Président
M. ZITOUNI Mohamed	Professeur	(U.S.T.H.B)	Directeur de thèse
M. AÏDER Meziane	Professeur	(U.S.T.H.B)	Examinateur
M. HERNANE Mohand Ouamar	Maître.Conf	(U.S.T.H.B)	Examinateur

Table des Matières

Chapitre I : Géométrie des courbes elliptiques

1-Introduction :

La conjecture de Birch et Swinnerton-Dyer a été formulée lors de l'étude de courbes elliptiques. [2].

Conjecture :

1) *la série* $L(E,s)$ *de Dirichlet-Hasse d'une courbe elliptique E, admet au point* $s=1$, *un zéro d'ordre égal au rang* r *du groupe de Mordell-Weil* $E(\mathbb{Q})$.
2) *Cette série* $L(E,s)$ *est liée à d'autres invariants de E par la relation :*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\prod_p c_p\,\frac{\Omega(E)\,.\,R(E)\,.\,card\left(Ш(E)\right)}{card\left(T(E)\right)^2}.$$

Nous commençons par l'étude algébrique et géométrique des courbes elliptiques.

2-Courbes algébriques planes :

Un point *P* du plan *Oxy* admet deux coordonnées : $P=(x,y)$.

Définition 1. *Une courbe algébrique plane est l'ensemble des points du p,an dont les coordonnées satisfont une équation algébrique de degré* $n\geq 1$:

$$C: f(x,y)=0,\ f(x,y)\in K[x,y],\ K=corps\ commutatif\ global,\ local\ ou\ fini$$

Exemples :

1) Pour $n=1$, $f=d_1x+d_2y+d_3=0$ $\quad(1)$
est l'équation d'une droite.

2) Pour $n=2$ et f irréductible :

$$f=d_1x^2+d_2xy+d_3y^2+d_4x+d_5y+d_6=0 \qquad (1-2)$$

est l'équation d'un cercle ou d'une conique selon la valeur des cœfficients d_i.

$$f(x,y)=(x-d_1)^2+(y-d_2)^2-r^2=0 \qquad (1-3)$$

est l'équation d'un cercle de centre (d_1,d_2) et de rayon $r\geq 0$.

Lorsque f est réductible,

$$f(x,y)=(d_1x+d_2y+d_3)(d_4x+d_5y+d_6) \qquad (1-4)$$

est l'équation du produit de deux droites.

3) Pour $n=3$ et f irréductible :

$$f(x,y)=d_1x^3+d_2x^2y+d_3xy^2+d_4y^3+d_5x^2+d_6xy+d_7y^2+d_8x+d_9y+d_{10} \qquad (1-5)$$

est l'équation d'une cubique non dégénérée.

Lorsque f est réductible, la cubique est dégénérée dans deux formes :

$$f(x,y)=(d_1x^2+d_2xy+d_3y^2+d_4x+d_5y+d_6)(d_78+d_8y+d_9)=0 \qquad (1-6)$$

est l'équation du produit d'une conique par une droite ;

$$f(x,y)=(d_1x+d_2y+d_3)(d_4x+d_5y+d_6)(d_7x+d_8y+d_9)=0 \qquad (1-7)$$

est l'équation du produit de trois droites.

4) Pour $n\geq 4$ et f irréductible,
$f(x,y)=0$ est l'équation d'une courbe plane hyperelliptique.
C'est une quartique pour $n=4$, une quintique pour $n=5$, une sextique pour $n=6$, etc…

3-Singularités et genre d'une courbe algébrique :

Définition 2. *Un point $P=(x_p,y_p)$ d'une courbe algébrique C d'équation $f(x,y)=0$ est singulier si ses coordonnées satisfont le système :*

$f(P)=f_x'(P)=f_y'(P)=0$ *et* $f_x''(P)\neq 0$ *pour un point double,*

$f(P)=f_x'(P)=f_y'(P)=f_{x^2}''(P)=f_{xy}''(P)=f_{y^2}''(P)=0$ *et* $f_x'''(P)\neq 0$ *pour un point triple,* $(1-8)$

$f(P)=f_x'(P)=.....=f_{x^{n-1}}^{(n-1)}(P)=.....=f_{y^{n-1}}^{(n-1)}(P)=0$ *et* $f_x^{(n)}(P)\neq 0$ *pour un point multiple d'ordre n.*

Dans ces équations, les symboles f_x',f_y' désignent les dérivées partielles,

$$f_{x^3}^{(3)}=\frac{\partial^3 f}{\partial x^3},\ f_{x^2y}^{(3)}=\frac{\partial^3 f}{\partial x^2\partial y},\ \text{etc....} \qquad (1-9)$$

Le degré n et le nombre s de points singuliers d'une courbe algébrique C sont associés à l'invariant « genre de la courbe ».

Définition 3. *Le genre d'une courbe algébrique C plane, irréductible, de degré $n \geq 2$, possédant s points singuliers, est l'entier non négatif :*

$$g(C) = \frac{1}{2}(n-1)(n-2) - s \qquad (1-10)$$

Exemples :

1) le genre d'une conique (C) est égal à $g(C) = 0$;
2) le genre d'une cercle (C) est égal à $g(C) = 0$;
3) le genre d'une cubique 3ingulière (C) est égal à $g(C) = 0$;
4) le genre d'une cubique (C) non singulière est égal à $g(C) = 1$

D'après la formule $(1-5)$ précédente, l'équation d'une cubique plane, irréductible, dépend de dix cœfficients.
Il y a des équations particulières de cubiques irréductibles avec cinq cœfficients.

Définition 4. *L'équation de Weierstrass d'une cubique plane, irréductible E est de la forme :*

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

Les 5 coefficients a_1, a_2, a_3, a_4, a_6 sont des éléments d'un corps commutatif *K*, les 2 variables *x* et y sont des éléments d'une clôture algébrique de *K*.

Cette équation est unitaire en y^2.
Des transformations linéaires de cette équation seront étudiées dans un autre paragraphe.

4-Espaces affines, espaces projectifs :

Ces notions d'espaces affines, projectifs se trouvent dans des ouvrages de Géométrie Algéb2ique comme « Algebraic Geometry » de HARTSHORNE, « Basic Algebraic Geometry » de SHAFAREVITCH.

Considérons un corps commutatif *K* et le *K*-espace vectoriel K^n des points $a = (a_1, ..., a_n)$ à n coordonnées a_i dans *K*.

Définition 5. *Un n-espace affine est l'ensemble des points de l'espace K^n* **:**

$$\mathbb{A}^n = \mathbb{A}^n(K) = \{a = (a_1, ..., a_n) \; ; \; a_1, ..., a_n \in K\} \qquad (3)$$

C'est un espace de dimension n.

Exemple :

1) l'espace affine $\mathbb{A}^2(\mathbb{R})$ est représenté par le plan réel *Oxy* , tout point P de cet espace a deux coordonnées x , y .

2) L'espace affine $\mathbb{A}^1(\mathbb{C})$ est représenté par une droite ; tout point P de cet espace a une coordonnée *z* qui est un nombre complexe.

3) L'espace affine $\mathbb{A}^3(\mathbb{R})$ est représenté par l'espace *Oxyz* à 3 dimensions ; chaque 0oint *P(x,y,z)* a 3 coordonnées réelles.

Avec une relation d'équivalence sur un $(n+1)$-espace affine $\mathbb{A}^{n+1}$, nous construisons un espace projectif $\mathbb{P}^n$.

Définition 6. *Un n-espace projectif* $\mathbb{P}^n(K)$ *est l'espace quotient d'un (n+1)-espace affine* $\mathbb{A}^{n+1}(K)$ *par la relation d'équivalence T qui satisfait la condition :*

$a=(a_1,...,a_{n+1})T\,(b_1,...,b_{n+1})=b$ *si et seulement si :*

$a=\lambda b$ *pour* $\lambda\neq 0$ *et* $\lambda\in K$.

Alors $\mathbb{P}^n(K)=\mathbb{A}^{n+1}/T$.

Cette définition implique qu'un point *P* de l'espace projectif $\mathbb{P}^n$ admet $(n+1)$ coordonnées

$$P=(x_1,x_2,...,x_{n+1})\in\mathbb{P}^n \qquad (4)$$

Chaque point P est donc le représentant d'une classe :

$$cl\,(P)=\{(x_1,x_2,...,x_{n+1}),(\lambda x_1,\lambda x_2,...,\lambda x_{n+1}),(tx_1,tx_2,...,tx_{n+1}),...\}$$

Les coordonnées $x_1,...,x_{n+1}$ sont les coordonnées homogènes d'un point du plan pro*ectif $\mathbb{P}^n$.

Exemple : dans l'espace projectif $\mathbb{P}^2(\mathbb{R})$, il y a une infinité de classes.

$$\begin{aligned} cl\,(1,1,1)&=\{(1,1,1),(-1,-1,-1),(2,2,2),...\}\\ cl\,(0,0,1)&=\{(0,0,1),(0,0,-1),(0,0,2),...\}\\ cl\,(0,1,0)&=\{(0,1,0),(0,-1,0),(0,2,0),...\}\end{aligned} \qquad (5)$$

L'équation de Weierstrass d'une cubique E dans le plan projectif $\mathbb{P}^2$ est de la forme:

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

C'est un polynôme homogène de 3 variables et de degré 3.
Dans un plan projectif $\mathbb{P}^n$, les polynômes sont homogènes à $n+1$ variables et de degré $d \geq 1$.

Le passage du plan projectif $\mathbb{P}^2$ au plan affine $\mathbb{A}^2$ s'obtient avec la transformation linéaire

$$(x, y, z) \to (x, y, 1) \in \mathbb{A}^2$$

Le passage du plan affine $\mathbb{A}^2$ au plan projectif $\mathbb{P}^2$ s'obtient avec 2 opérations :
une transformation rationnelle

$$(x, y) \to \left(\frac{x}{z}, \frac{y}{z}\right)$$

et une multiplication par $z^d, d =$ degré du 0olynôme f (second membre de l'équation de *E*).

$$z^d f\left(\frac{x}{z}, \frac{y}{z}\right) = g(x, y, z)$$

Exemples :
1) $f(x, y, z) = 2x^5 - 3y^2x^3 + 4xyz^3 - 2z^5 \in \mathbb{P}^2$
Ce polynôme homogène est transformé en un polynôme affine :

$$f(x, y, 1) = g(x, y) = 2x^5 - 3y^2x^3 + 4xy - 2 \in \mathbb{A}^2.$$

2) Le polynôme affine $u(x, y) = x^4 - 2x^3y + x^2y + 5 \in \mathbb{A}^2$ de degré 4
est transformé en

$$u\left(\frac{x}{z}, \frac{y}{z}\right) = \frac{x^4}{z^4} - 2\frac{x^3y}{z^4} + \frac{x^2y}{z^3} + 5$$

puis, par multiplication par z^4, en un polynôme homogène de degré 4 :

$$z^4 u\left(\frac{x}{z}, \frac{y}{z}\right) = x^4 - 2x^3y + x^2yz + 5z^4 \in \mathbb{P}^2.$$

5-Variétés algébriques affines, projectives, abéliennes

Pour munir les espaces affines $\mathbb{A}^n$ et projectifs $\mathbb{P}^n$ d'une structure de variétés algébriques, il faut introduire une topologie convenable.

Définition 7. *La topologie de Zariski sur l'espace affine $\mathbb{A}^n$ est déterminée par les ensembles algébriques de l'espace $\mathbb{A}^n$ comme ensembles fermés et leurs complémentaires comme ensembles ouverts.*

Dans cette topologie, seuls l'espace affine $\mathbb{A}^n$ et l'ensemble vide pos3èdent la propriété d'être ouverts et fermés à la fois. Cette topologie n'est pas de Hausdorff.

Définition 8 :

1) *Un ensemble algébrique dans un espace affine* $\mathbb{A}^n(K)$ *est l'ensemble des zéros d'une famille de polynômes* $f_1,...,f_d$ *de l'anneau* $K[X_1,...,X_n]$.

2) *Une variété affine est une partie irréductible et fermée d'un espace affine.*

Cette définition s'étend aux variétés projectives.

Définition 9. *Une variété projective est une partie irréductible et fermée d'un espace projectif.*

Une variété algébrique possède deux parties intéressantes.

Définition 10 :

1) *Une sous variété projective d'une variété projective V est une partie X de V qui a une structure de variété.*

2) Une variété quasi projective est une partie ouverte d'une variété projective.

Une variété projective peut être munie d'une structure de variété abélienne.

Définition 11. *Une variété abélienne est une variété projective A munie d'une addition et de deux applications :*

$A\times A\to A$; $(a,b)\to a+b$ *, loi de groupe abélien ;*

$A\to A$, $a\to a^{-1}$, *application inverse.*

Exemple :

Soit une courbe elliptique *A* d'équation de Weierstrass **:**

$$A: y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz^2+a_6z^3; \qquad (1)$$

et son groupe de Mordell-Weil $A(K)$ (Confère chapitre 2).

Alors les deux applications :

$$A(K)\times A(K)\to A(K)\ ;\ (P,Q)\to P+Q \qquad (2)$$

et $$A(K)\to A(K)\ ;\ P\to -P \qquad (3)$$

munissent la courbe elliptique d'une structure de variété abélienne.

Sa dimension est égal à : $\dim\mathbb{P}^n$ – nombre de relations.

L'équation (1) indique que le groupe $A(K)$ est dans le plan projectif $\mathbb{P}^2$; l'équation (1) constitue une relation.

Donc, une courbe elliptique est une variété abélienne de dimension 1. (4)

6-Transformation de l'équation de Weierstrass :

Par définition, l'équation de Weierstrass d'une cubique est de la forme :

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

Pour éliminer certains monômes dans (1), il faut des transformations convenables :
Nous éliminons les monômes en xy et en y avec le changement de variables :

$$(x, y) \to \left(X, \frac{1}{2}(Y - a_1X - a_3)\right) \qquad (1-2)$$

Nous obtenons pour un corps K de $carac(K) \neq 2$, l'équation de Weierstrass :

$$E_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \in K[x, y] \qquad (1-3)$$

Les trois coefficients b_{2i} sont des polynômes « homogènes » de degré $2i$ de l'anneau $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$:

$$b_2 = a_1^2 + 4a_2;\ b_4 = a_1a_3 + 2a_4;\ b_6 = a_3^2 + 4a_6 \qquad (1-4)$$

L'élimination du coefficient 4 et du monôme en x^2 dans l'équation de E_1 s'obtient avec le changement de variables :

$$(X, Y) \to \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right) \qquad (1-5)$$

Pour $carac(K) \neq 2, 3$, nous obtenons l'équation de Weierstrass :

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6 \in K[x, y] \qquad (1-6)$$

Les deux coefficients c_4 et c_6 sont des polynômes « homogènes » de degré $2i$ de l'anneau $\mathbb{Z}[b_2, b_4, b_6]$:

$$c_4 = b_2^2 - 24b_4;\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \qquad (1-7)$$

Les deux changements de variables $(1-2)$ et $(1-5)$ sont des applications bijectives d'inverses :

$$(X, Y) \to (x, 2y + a_1x + a_3); \quad \text{et} \quad (x, y) \to (36X + 3b_2, 108Y) \qquad (1-8)$$

Ces formules des b_{2i} et c_{2i} se trouvent dans l'ouvrage « Lecture Note in Mathematic n°476 ».

D'autres transformations permettent d'obtenir d'autres modèles d'équations de Weierstrass :

Le modèle $E_3 : y^2 = x^3 + Ax + B \in K[x, y]$ $(1-9)$

Le modèle de Legendre :

$$E_4 : y^2 = x(x-1)(x-t) \in K[x, y],\ t \neq 0,1 \qquad (1-10)$$

Le modèle de Kubert :

$$E_5 : y^2 + (1-c)xy - by = x^3 - bx^2 \in K[x, y] \qquad (1-11)$$

Le modèle de Deuring :

$$E_6 : y^2 + txy + ty = x^3 \in K[x, y],\ t \neq 27 \qquad (1-12)$$

Le modèle de Tate :

$$E_7 : y^2 + xy = x^3 + ax + b \in \mathbb{C}[x, y] \qquad (1-13)$$

Selon Silverman, les cœfficients a et b sont des séries de puissances formelles dans l'anneau $\mathbb{Z}[[q]],\ q = \exp(2\pi iz)$,

$$a = -5\sum_{n\geq 1} n^3 q^n / (1-q^n)$$
$$b = -\frac{1}{12}\sum_{n\geq 1} (7n^5 + 5n^3) q^n / (1-q^n)$$

Signalons la transformation de l'équation de la courbe cubique de Fermat dans « The Arithmetic of Elliptic Curves » de Tate.

Equation de Fermat :

$$E_1 : x^3 + y^3 = z^3$$

Le changement de variables rationnel :

$$X = \frac{3z}{x+y}\ ,\ Y = \frac{9(x-y)}{2(x+y)} + \frac{1}{2}$$

admet un changement inverse unique :

$$x = \frac{z(Y+4)}{3X}\ ,\ y = \frac{z(5-Y)}{3X}$$

L'équation obtenue est de la forme :

$$E_2 : Y^2 - Y = X^3 - 7$$

7-Invariants d'une cubique :

Les cubiques possèdent des invariants nombreux : géométrique, arithmétique, algébrique, différentiel, analytique…
Nous commençons par étudier 3 invariants ; le discriminant, l'invariant modulaire et l'invariant différentiel.

Définition 12. *Le discriminant d'une cubique d'équation 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 de l'anneau $\mathbb{Z}[b_2, b_4, b_6, b_8]$ *égal à*

$$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8$$

où l'on a posé $4b_8 = b_2b_6 - b_4^3$ *et pour* $carac(K) \neq 2, 3$.

Calculs de discriminants de courbes elliptiques précédentes:

1) Courbe de Fermat : $E : y^2 - y = x^3 - 7$
$$\Delta(E) = -3^9.$$

2) Modèle $E : y^2 = x^3 - 27c_4x - 54c_6$
$$\Delta(E) = 108^3\left(c_4^3 - c_6^2\right)$$

3) Modèle de Legendre : $E : y^2 = x(x-1)(x-t)$, $t \neq 0,1$
$$\Delta(E) = 16t^2(t-1)^2$$

4) Modèle de Tate : $\Delta(E) = q\prod_{n\geq 1}\left(1-q^{2n}\right)^{24}$, $q = \exp(2i\pi z)$.

5) Modèle $E : y^2 = x^3 + Ax + B$:
$$\Delta(E) = -16\left(4A^3 + 27B^2\right)$$

Définition 13. *l'invariant modulaire d'une cubique d'équation de Weierstrass*

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

est l'élément j(E) du corps K égal à

$$j(E) = c_4^3/\Delta(E)$$

Calculs d'invariants modulaires des modèles précédents :

1) Modèle $E : y^2 = x^3 + Ax + B$.
$$j(E) = 1728(4A)^3/\left(4A^3 + 27B^2\right)$$
2) Modèle de Legendre :

$$j(E) = 2^8 \left(t^2 - t + 1\right)^3 \Big/ t^2 (t-1)^2$$

Définition 14. *L'invariant différentiel d'une cubique d'équation de Weierstrass :*

$$f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$$

est l'élément différentiel :

$$\omega(E) = \frac{dx}{2y + a_1 x + a_3} = \frac{-dy}{3x^2 + 2a_2 x + a_4 - a_1 y} = \frac{dx}{f'_y} = \frac{-dy}{f'_x}.$$

Les dénominateurs sont les dérivées partielles du polynôme $f(x, y)$:

$$df = f'_x\, dx + f'_y\, dy = 0$$

Calculs d'invariants différentiels des modèles précédents :

1) Modèle $E : y^2 = x^3 + Ax + B$

$$\omega(E) = \frac{dx}{2y} = \frac{-dy}{3x^2 + A}$$

2) Modèle $E : y^2 = x^3 - 27c_4 x - 54c_6$

$$\omega(E) = \frac{dx}{2y} = \frac{-dy}{3x^2 - 27c_4}$$

Le discriminant $\triangle(E)$ d'une courbe elliptique *E* est lié au discriminant $dis(f)$ d'un polynôme $f(x) \in K[x]$.

Pour l'étude des discriminants nous nous sommes inspirés des ouvrages « Introduction à l'algèbre » de Kostrikine et « A classical invitation to algebraic numbers and class fields » de Harvey Cohn.

L'équation de Weierstrass d'une cubique peut se mettre sous la forme $y^2 = f(x)$.

Le discriminant $\triangle(E)$ de la cubique peut être calculé avec la formule de la définition.

Nous cherchons une relation entre les discriminants $\triangle(E)$ de la cubique et $dis(f)$ du polynôme f .

Un polynôme $f(x) \in K[x]$ de degré $n > 1$ admet n racines $\theta_1, ..., \theta_n$ dans une clôture algébrique K_{alg} du corps *K*.

Ces racines peuvent être simples ou multiples :

$$n > 1,\ f(x) = d_0 x^n + d_1 x^{n-1} + \cdots + d_n \in K[x]; \qquad (1)$$

$$= d_0 (x - \theta_1)(x - \theta_2) \cdots (x - \theta_\cdot) \in K_{alg}[x]; \qquad (1-1)$$

Les polynômes $f(x)$ admettent plusieurs invariants :

Un degré, des racines, un groupe de permutations, un discriminant,… Lorsque $d_0 = 1$, le polynôme est unitaire.

Définition 15. *Le discriminant d'un polynôme f(x), formules* (1) *et* $(1-1)$ *est l'élément dis(f) du corps K égal à*

$$dis(f) = d_0^{2n-2} \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2 \qquad (2)$$

Donc le discriminant $dis(f)$ est une fonction quadratique de ses racines θ_i. Il est aussi une fonction des fonctions symétriques S_t de ses racines :

$$S_1 = \sum_i \theta_i = -d_1/d_0 \ ; S_2 = \theta_1\theta_2 + \cdots + \theta_{n-1}\theta_n = d_2/d_0 \ ; \ldots S_n = \prod_i \theta_i = (-1)^n d_n/d_0$$

La formule (2) de la définition de $dis(f)$ implique la

Proposition 1 : *Le discriminant d'un polynôme f(x) de degré n>1 est nul si et seulement si il admet deux racines égales.*

□

Selon H. Cohn, le discriminant $dis(f)$ se met sous la forme d'un déterminant d'ordre égal au degré *n* du polynôme $f(x)$.

Proposition 2 :

Soit un polynôme unitaire f(x) de degré n>1

$$f(x) = x^n + d_1 x^{n-1} + \ldots + d_n \in K[x].$$

Alors son discriminant $dis(f)$ *est égal au déterminant symétrique d'ordre n :*

$$dis(f) = \begin{pmatrix} n & s_1 & s_2 & \cdot & \cdot & s_{n-1} \\ s_1 & s_2 & s_3 & \vdots & \vdots & s_n \\ s_2 & 3_3 & s_4 & \vdots & \vdots & s_{n+1} \\ \cdots & \cdots & \cdots & \vdots & \vdots & \cdots \\ s_{n-1} & s_n & s_{n+1} & \vdots & \vdots & s_{2n-2} \end{pmatrix}$$

où S_t *= somme des produits des racines t à t*

La relation de récurrence $s_m = -md_m - \cdots + s_{m-1}d_1$ *permet de calculer ces nombres*

Preuve : Cf. H cohn.

□

Calculs de discriminants de polynômes particuliers :

1) polynôme cubique $f(x) = d_0x^3 + d_1x^2 + d_2x + d_3$

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

(formule de Lang dans « Algebra », V-exercice11, p141).

2) polynôme cubique $f(x) = x^3 + Ax + B$.

Alors $dis(f) = -\left(4A^3 + 27B^2\right)$.

3) polynôme cubique $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$
Alors $dis(f) = 16\left(9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8\right)$.

4) Polynôme de degré n : $f(x) = \left(x^n + a\right)$
Alors : $dis(f) = (-1)^{\frac{n(n-1)}{2}} \cdot a^{n-1} \cdot n^n$

5) Polynôme de degré $n-1$: $f(x) = \left(x^n - 1\right)/(x-1)$
Alors : $dis(f) = (-1)^{\frac{(n-1)(n-2)}{2}} \cdot n^{n-2}$
Ces exemples impliquent des relations entre les discriminants $dis(f)$ et $\triangle(E)$.

Proposition 3 :
Soit une cubique E d'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \in K[x]$$

Alors les discriminants $\triangle(E)$ *de E et* $dis(f)$ *de* f *satisfont la relation*

$$dis(f) = 16\triangle(E)$$

Preuve : exemple (3) ci-dessus. □

Proposition 4 :
Soit une cubique E d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B = f(x) \in K[x]$$

Alors les discriminants $\triangle(E)$ *de E et* $dis(f)$ *de* f *satisfont la relation*

$$\triangle(E) = 16 \cdot dis(f)$$

Preuve :
la valeur $dis(f)$ se trouve dans l'exemple (2).
Par le calcul nous obtenons les invariants de E
$b_2 = 0$; $b_4 = 2A$; $b_6 = 4B$; $b_8 = -A^2$ et $\triangle(E) = -16\left(4A^3 + 27B^2\right)$.
Il en résulte la relation $\triangle(E) = 16 \cdot dis(f)$.
□

La proposition 3, où $dis(f) = 16 \cdot \triangle(E)$, et la proposition 4, où $\triangle(E) = 16 \cdot dis(f)$ impliquent que les discriminants $dis(f)$ et sont multiples l'un de l'autre.
Lorsque le polynôme $f(x)$ est unitaire, $dis(f)$ est unitaire; lorsque $f(x)$ n'est pas unitaire, $dis(f)$ ne l'est pas ; cela implique la différence des 2 relation.
Le discriminant d'un polynôme $f(x)$ a un lien avec le résultant de ce polynôme et de sa dérivée.

8-Résultant de 2 polynômes :

La théorie du résultant se trouve dans plusieurs ouvrages comme « Algebra » de Lang et « Introduction à l'algèbre » de Kostrikine.

Définition 16. *Soient deux polynômes :*

$f(x)=d_0x^n+d_1x^{n-1}+\cdots+d_n$, de degré $n\geq 1$,

et $g(x)=r_0x^t+r_1x^{t-1}+\cdots+r_t$, de degré $t\geq 1$.

Leur résultant est le déterminant d'ordre $n+t$ *égal à :*

$$\mathrm{Res}(f,g)=\begin{vmatrix} d_0 & d_1 & d_2 & \dots & d_{n-1} & d_n & 0 & 0 & \dots & 0 \\ 0 & d_0 & d_1 & \dots & d_{n-2} & d_{n-1} & d_n & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_0 & d_1 & d_2 & d_3 & \cdots & d_n \\ r_0 & r_1 & r_2 & \dots & r_{t-1} & r_t & 0 & 0 & \dots & 0 \\ 0 & r_0 & r_1 & \dots & r_{t-2} & r_{t-1} & r_t & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r_0 & r_1 & r_2 & r_3 & \dots & r_t \end{vmatrix}$$

formé de t lignes $(d_0d_1..d_n)$ *et r lignes* $(r_0r_1...r_t)$*, les termes manquants sont remplacés par des zéros.*

Les résultants $\mathrm{Res}(f,g)$ possèdent plusieurs propriétés.

Proposition 5. *Soient deux polynômes* **:**

$f(x)=d_0\prod_{1\leq i\leq n}(x-\theta_i)$, de degré $n\geq 1$ et

$\mathrm{g(x)}=r_0\prod_{1\leq j\leq t}(x-\psi_j)$, de degré $t\geq 1$

Leur résultant satisfait les relations :

$$\begin{aligned}\mathrm{Res}(f,g)&=d_0^t\prod_{i=1}^{n}g(\theta_i)\\&=(-1)^{nt}\prod_{j=1}^{t}f(\psi_j)\\&=d_0^t\ r_0^n\prod_{i,j}(\theta_i-\psi_j)\end{aligned}$$

Preuve : Lang .

□

La $3^{ième}$ relation implique le :

Corollaire 1. *Le résultant Res(f,g) de deux polynômes* $f(x)$ et $g(x)$ *est nul si est seulement si les deux polynômes ont une racine commune.*

□

En remplaçant le polynôme $g(x)$ par la dérivée f' de $f(x)$ nous obtenons le résultant $\mathrm{Res}(f, f')$ du polynôme $f(x)$.

Corollaire 2 : *Le résultant* $Res(f, f')$ *d'un polynôme* $f(x)$ *et de sa dérivée* $f'(x)$ *est égal à* :

$$Res(f, f') = d_0^{n-1} \prod_{i=1}^{n} f'(\theta_i)$$

□

Pour un polynôme $f(8)$, le discriminant *dis(f)* et le résultant $Res(f, f')$ sont liés par la

Proposition 6 : *Soit un polynôme* $f(x)$ *de degré* $n \geq 1$

$$f(x) = d_0 x^n + d_1 x^{n-1} + \cdots + d_n \in K[x], \text{ de racine } \theta_i,$$

Alors le discriminant dis(f) et le résultant $Res(f, f')$ *satisfont la relation :*

$$\begin{aligned} Res(f, f') &= (-1)^{\frac{n(n-1)}{2}} \cdot d_0 \cdot dis(f) \\ &= d_0^{2n-1} \prod_{i \neq j} (\theta_i - \theta_j) \end{aligned}$$

Preuve : On applique le corollaire 2 et la proposition 5.

□

Nous classifions les cubiques planes E grâce au discriminant $\triangle(E)$ de la courbe E et $dis(f)$ du polynôme *f* de l'équation de Weierstrass $f(x) = y^2$ de *E*.

Considérons les cubiques planes E d'équation de Weierstrass

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

Lorsque le polynôme

$$f(x, y) = y^2 + a_1 xy + a_3 yx^3 - x^3 - a_2 x^2 - a_4 x - a_6 \in K[x, y] \qquad (2)$$

est irréductible et sans point singulier, alors il est représenté par une courbe elliptique.

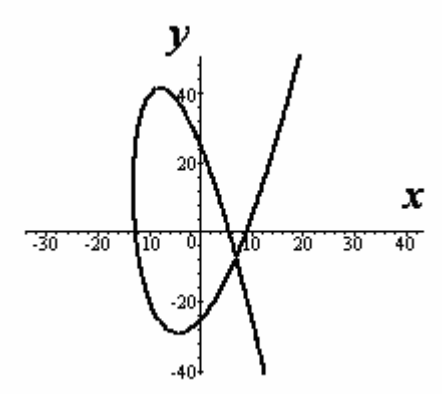
Définition 17. *Une courbe elliptique est une cubique plane irréductible, non singulière, qui a une équation de Weierstrass*

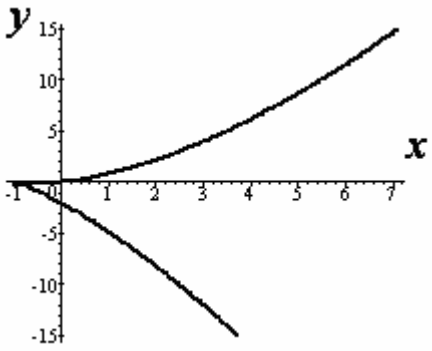
$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y].$$

Les 5 cœfficients a_1, a_2, a_3, a_4 et a_6 sont des éléments d'un corps commutatif K global, local ou fini.

Les 2 variables x et y sont des racines de l'équation algébrique de Weierstrass ; donc x et y sont des éléments d'une clôture algébrique $K_{a\lg}$ de K.
Il en résulte que la nature du corps de base K influe sur les propriétés de la courbe elliptique. Lorsque K est un corps de nombres, nous étudions la courbe elliptique avec les idéaux de K, la ramification, les entiers, les équations diophantiennes, les valuations, etc…
Lorsque K est le corps des nombres complexes, nous utilisons l'analyse complexe (fonction $\wp(z)$ de Weierstrass, tores complexes, fonctions elliptiques, fonctions modulaires, etc…) et la géométrie algébrique (plan projectif, variétés abéliennes, diviseurs, cohomologie, etc…).

Une cubique E peut admettre 0 ou 1 point singulier. Le point singulier est soit un nœud, point singulier où la cubique E admet deux tangentes distinctes, soit un point de rebroussement, point singulier où la cubique admet deux tangentes confondues.





$E : y^2 + 2xy = x^3 - 2x^2 - 133x + 637$ $\qquad$ $E : y^2 + 2xy + 2y = x^3 + 2x^2 + x$

NŒUD : (7,-7) $\qquad$ *POINT DE REBROUSSEMENT : (-1,0)*

Figure1

Le point à l'infini $O_E = (\infty, \infty)$ associé à une cubique E joue un rôle important pour la cubique E.

Proposition 7 :

Soit une cubique E d'équation de Weierstrass projective :

$E : f(x, y, z) = y^2 z + a_1 xyz + a_3 yz^2 - 8^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3 = 0.$

Le point $(0,1,0) = O_E$ *à l'infini est un point simple de la cubique.*

Preuve de « O_E est un point de la cubique E »

Calculons la valeur $f(O_E)$; nous obtenons :

$$f(O_E) = f(0,1,0) = 0$$

Il en résulte que le point 0_E est sur la cubique E.

Preuve de « O_E est un point simple E »
Calculons les trois dérivées partielles du polynôme homogène f :

$$f_x' = -3x^2 + a_1yz - 2a_2xz - a_4z^2 \quad (1)$$
$$f_y' = 2yz + a_1xz + a_3z^2 \quad (2)$$
$$f_z' = y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2 \quad (3)$$

La valeur $f_z'(0_E) = f_z'(0,1,0) = 1 \neq 0$ implique que le point 0_E est simple.
□
Etudions les cubiques singulières E avec leurs invariants $\Delta(E)$ et $c_4(E)$

Proposition 8 :

Soit une cubique de Weierstrass E, d'invariants $\Delta(E)$ et $c_4(E)$.

1) *la cubique est singulière si et seulement si* $\Delta(E) = 0$;
2) *elle admet un nœud si et seulement si* $\Delta(E) = 0$ et $c_4(E) \neq 0$;
3) *elle admet un point de rebroussement si et seulement si* $\Delta(E) = 0$ et $c_4(E) = 0$.

Preuve de « *E est singulière » implique «* $\Delta(E) = 0$ » :
Par définition, une cubique singulière est une cubique E ayant un point singulier.
Donc ce point est double. (1)
L'équation de Weierstrass de la cubique est de la forme

$E : y^2 = (x-e)^2(x-e') = f(x)$; $S = (e,0)$ est le point double. (2)

D'après la théorie des discriminants des polynômes,
$dis(f) = 0$ si et seulement si f a une racine double (3)
(2) et (3) impliquent $dis(f) = 0$ (4)
La relation $\Delta(E) = 16\, dis(f)$ et (4) impliquent :

$$\Delta(E) = 0 \quad (5)$$

Preuve de « E admet un nœud implique « $c_4(E) \neq 0$ »
La cubique E admet deux tangentes distinctes au nœud ; (6)
La pente d'une tangente à une courbe est égale à la dérivée y' de y.
Prenons une équation de Weierstrass de E de la forme :

$$E : y^2 = x^3 - 27c_4x - 54c_6 \quad (7)$$

Calcul de la dérivée y' de y :

$$y' = \frac{3x^2 - 27c_4}{2y} = \frac{N(x)}{2y} \qquad (8)$$

L'hypothèse de deux tangentes distinctes au nœud implique :
2 racines réelles distinctes du polynôme $N(x)$ (9)

Donc son discriminant $dis(N(x))$ n'est pas nul :

$$dis(N(x)) = 12 \times 27c_4 \neq 0 \text{ pour } carac(K) \neq 2,3 \qquad (10)$$

Cela implique un invariant $c_4(E) \neq 0$.

Preuve de « *E* admet un point de rebroussement » implique « $\Delta(E) = 0$ et $c_4(E) = 0$ »
L'hypothèse « *E* admet un point de rebroussement » implique que la cubique est singulière, donc :

$$\Delta(E) = 0 \qquad (11)$$

Gardons l'équation de Weierstrass (7) et la dérivée $y' = \frac{N(x)}{2y}$. Au point de rebroussement, la cubique admet deux tangentes confondues, cela implique $dis(N(x)) = 0$;

D'après (10), $dis(N(x)) = 12 \times 27c_4 = 0$ (12)

Il en résulte $c_4(E) = 0$ pour $carac(K) \neq 2,3$ (13)

□

Les preuves des réciproques se trouvent dans [15].
Nous nous intéressons maintenant aux courbes elliptiques.

Proposition 9 :

Soit une cubique de Weierstrass E de discriminant $\Delta(E)$

1) *la cubique E est une courbe elliptique si et seulement si* $\Delta(E) \neq 0$ *;*
2) *La courbe elliptique E coupe l'axe Ox en trois points simples si et seulement si* $\Delta(E) > 0$
3) *La courbe elliptique E coupe l'axe Ox en un seul point si et seulement si* $\Delta(E) < 0$.

(1) Preuve de « la cubique *E* est une courbe elliptique » implique « $\Delta(E) \neq 0$ »

d'après la proposition 8, une cubique *E* est singulière si et seulement si $\Delta(E) = 0$.

Il en résulte qu'une cubique est non singulière si et seulement si $\Delta(E) \neq 0$.

Par définition, une cubique non singulière est une courbe elliptique.

(2) Preuve de « une courbe elliptique E coupe l'axe Ox en 3 points simples » implique « $\Delta(E)>0$ »

Considérons une courbe elliptique E qui coupe l'axe Ox en 3 points simples

$$P_i=(e_i,0):\ i=1,2,3\ ;\ e_i\neq e_j \qquad (1)$$

Elle admet une équation de Weierstrass de la forme :

$$E: y^2=(x-e_1)(x-e_2)(x-e_3)=f(x)\in\mathbb{R}[x,y] \qquad (2)$$

Le discriminant du polynôme $f(x)$ est égal à :

$$dis(f)=\prod_{1\le i<j\le 3}(e_i-e_j)^2 \qquad (3)$$

Les 3 racines e_i sont des nombres réels, il en résulte que les carrés $(e_i-e_j)^2$ de nombres réels sont positifs :

$$dis(f)>0 \qquad (4)$$

La formule (4) et la relation entre les discriminants de f et de E impliquent

$$\Delta(E)>0 \qquad (5)$$

(3) Preuve de « une courbe elliptique coupe l'axe Ox en un seul point » implique « $\Delta(E)<0$ ».

Considérons une courbe elliptique qui coupe l'axe Ox en un seul point $P(e,0)$.

Cela implique que les deux autres racines e_1 et e_2 du polynôme $f(x)=y^2$ sont conjuguées complexes.

$$e_1=r+is\ ,\ e_2=r-is\ ,\ r \text{ et } s \text{ réels} \qquad (6)$$

Le discriminant du polynôme $f(x)$ est égal à

$$dis(f)=\left((e-e_1)(e-e_2)(e_1-e_2)\right)^2 \qquad (7)$$

Avec le calcul nous obtenons la valeur :

$$dis(f)=-4s^2\left((e-r)^2+s^2\right) \qquad (8)$$

Les carrés des nombres réels sont positifs. Il en résulte le signe du $dis(f)$

$$dis(f)<0 \qquad (9)$$

La relation entre $dis(f)$ et $\triangle(E)$ implique :

$$\triangle(E) < 0 \qquad (10)$$

□

Nous ne ferons pas les preuves des réciproques.
En rassemblant les résultats des propositions (8) et (9), nous obtenons une classification des cubiques de Weierstrass par leurs invariants $\Delta(E)$ et $c_4(E)$.

Proposition 10 :

Les cubiques E de Weierstrass sont classifiées par leurs invariants $\Delta(E)$ et $c_4(E)$ en 4 classes.

1) *La classe CubI des cubiques qui ont un nœud ; donc $\triangle(E) = 0$ et $c_4(E) \neq 0$.*
2) *La classe CubII des cubiques qui ont un point de rebroussement ; donc $\triangle(E) = 0$ et $c_4(E) = 0$.*
3) *La classe CubIII des courbes elliptiques qui coupent l'axe Ox en 3 points simples ; donc $\triangle(E) > 0$.*
4) *La classe CubIV des courbes elliptiques qui coupent l'axe Ox en un seul point ; donc $\triangle(E) < 0$.*

□

Illustrons cette classification par un exemple de chacune des 4 classes :

1) Cubique de Weierstrass qui a un nœud :

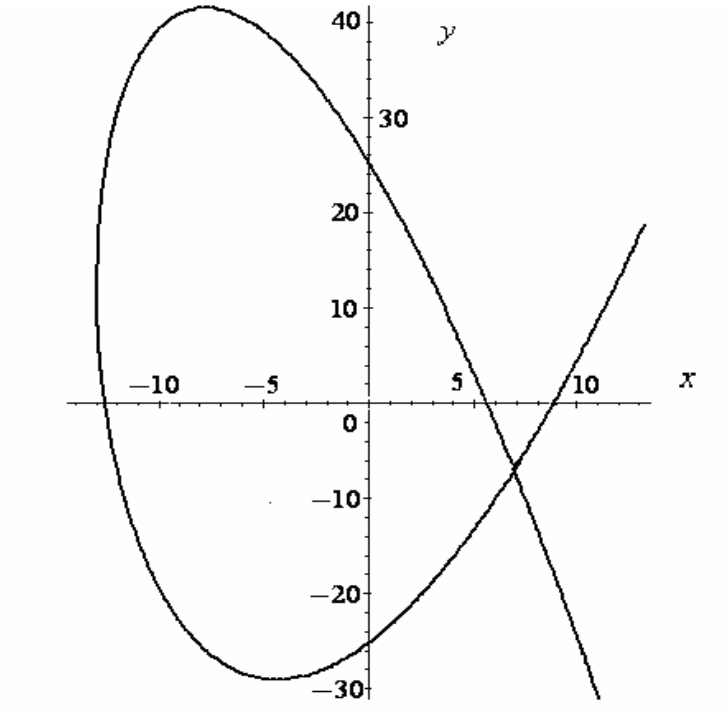
Cubique E_1 d'équation de Weierstrass

$$E_1 : y^2 + 2xy = x^3 - 2x^2 - 133x + 637 \in \mathbb{R}[x, y]$$

Calcul des invariants :

$$\Delta(E) = 0 \quad \text{et} \quad c_4 = 16 - 24(266) = -2^5.199 \neq 0$$

Cela implique que la cubique possède un nœud.



Courbe tracée avec le logiciel « *ScientificWorkPlace* »

Figure 2

Coordonnées de quelques points :

x	-11	-10	-5	0	5	7	10
y	$11 \pm 18\sqrt{2}$	$10 \pm 17\sqrt{3}$	$5 \pm 24\sqrt{2}$	$\pm 7\sqrt{13}$	$-5 \pm 6\sqrt{2}$	-7	$-10 \pm 3\sqrt{23}$

Cette courbe possède un nœud de coordonnées : $N = (7, -7)$.

2) Cubique de Weierstrass qui a un point de rebroussement.

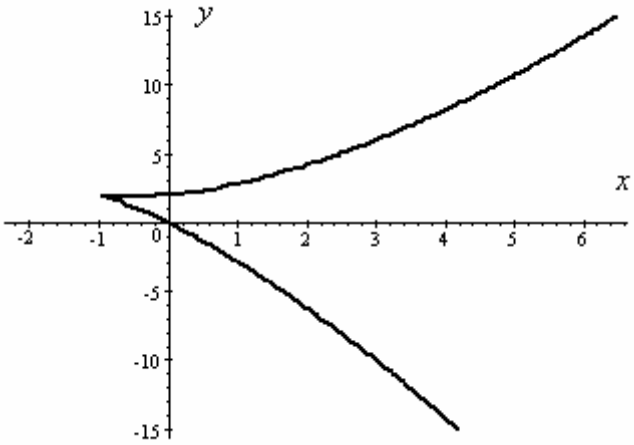
Cubique E_2 d'équation de Weierstrass :

$$E_2 : y^2 + 2xy + 2y = x^3 + 2x^2 + 5x \in \mathbb{R}[x, y]$$

Calcul des invariants :

$$\triangle(E_2) = 0 \text{ et } c_4 = 0$$

Cela implique que la cubique possède un point de rebroussement



Courbe tracée avec le logiciel « *ScientificWorkPlace* »
Figure 3

Coordonnées de quelques points :

x	-1	0	1/2	1	2	3
y	2	0 et 2	$(1/2) \pm (3/4)\sqrt{6}$	2 et -2	$(-1) \pm 3\sqrt{3}$	-10 et 6

Cette courbe possède un point de rebroussement de coordonnées $S = (-1, 2)$.

3) Courbe elliptique qui coupe l'axe *Ox* en 3 points simples.

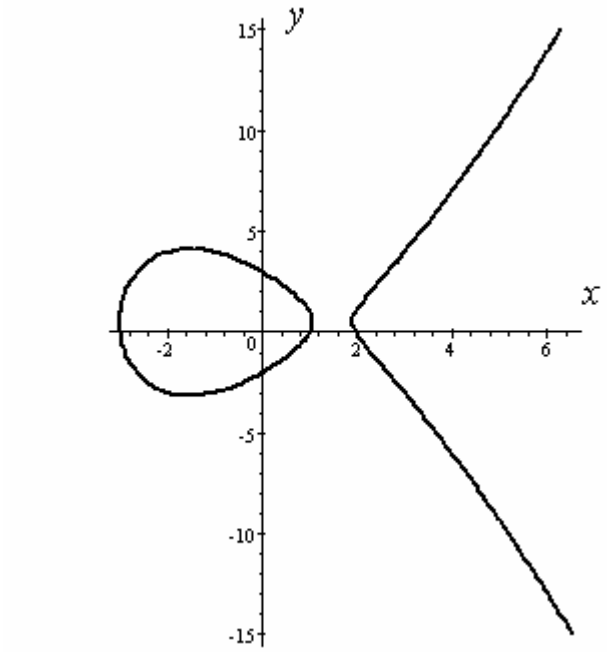
Cubique E_3 d'équation de Weierstrass :

$$E_3 : y^2 - y = x^3 - 7x + 6 \in \mathbb{R}[x, y]$$

Calcul du discriminant :

$$\Delta(E_3) = 5077 > 0$$

Cela implique que la courbe E_3 coupe l'axe *Ox* en trois points.



Courbe tracée avec le logiciel « *ScientificWorkPlace* »
Figure 4

Coordonnées de quelques points :

x	-3	-2	-1	0	1	2	3
y	0 et 1	-3 et 4	-3 et 4	-2 et 3	0 et 1	0 et 1	-3 et 4

Coordonnées des points d'intersection de la courbe E_3 avec l'axe *Ox* :

$$P_1 = (-3,0), P_2 = (1,0), P_3 = (2,0)$$

4) Courbe elliptique qui coupe l'axe *Ox* en un seul point :

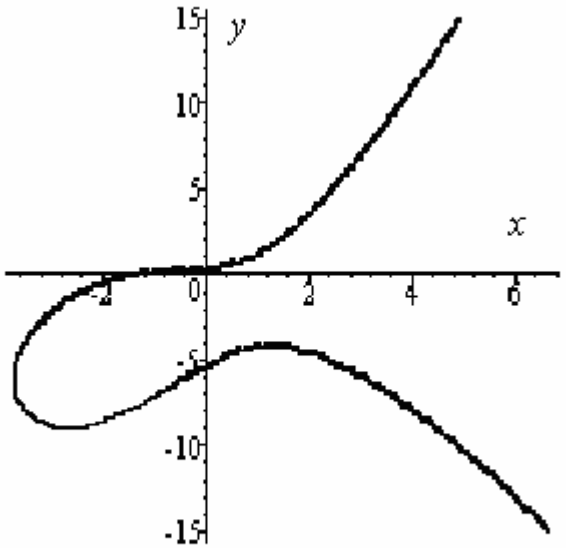
Cubique E_4 d'équation de Weierstrass :

$$E_4 : y^2 - 2xy + 5y = x^3 + x^2 + x + 2 \in \mathbb{R}[x, y]$$

Calcul du discriminant :

$$\Delta(E_4) = 64 - 27(33)^2 = -29339 < 0$$

Cela implique que la courbe elliptique coupe l'axe *Ox* en un seul point.



Courbe tracée avec le logiciel « *ScientificWorkPlace* »

Figure 5

Coordonnées de quelques points :

x	-3	$-2 \leq x \leq -1$	-1	0	1	2
y	$-\frac{9}{2} \pm \frac{1}{2}\sqrt{65}$	0	$-3 \pm \sqrt{10}$	$\frac{5}{2} \pm \frac{1}{2}\sqrt{33}$	$-\frac{3}{2} \pm \frac{1}{2}\sqrt{29}$	$\frac{1}{2} \pm \frac{1}{2}\sqrt{65}$

Coordonnées du point d'intersection de la courbe E_4 avec l'axe *Ox* : $P = (-1, 0)$.

Chapitre II : Groupe de Mordell-Weil d'une courbe elliptique

1-Loi de groupe sur une courbe elliptique :

Considérons l'ensemble $E(K)$ des points *K*-rationnels d'une courbe elliptique E et le point à l'infini $O_E = (\infty, \infty)$ de *E*.

Construisons sur l'ensemble $E(K)$ une loi de groupe abélien d'élément neutre le point O_E.

Proposition 1.

L'application $f : E(K) \times E(K) \to E(K)$ *de valeur* $f(P,R) = P + R$ *munit l'ensemble* $E(K)$ *d'une structure de groupe abélien d'élément neutre* O_E *avec la règle géométrique :*
trois points colinéaires de la courbe E *ont une somme nulle :*

$$P + R + S = O_E$$

Preuve :

Vérifions les axiomes d'un groupe abélien :

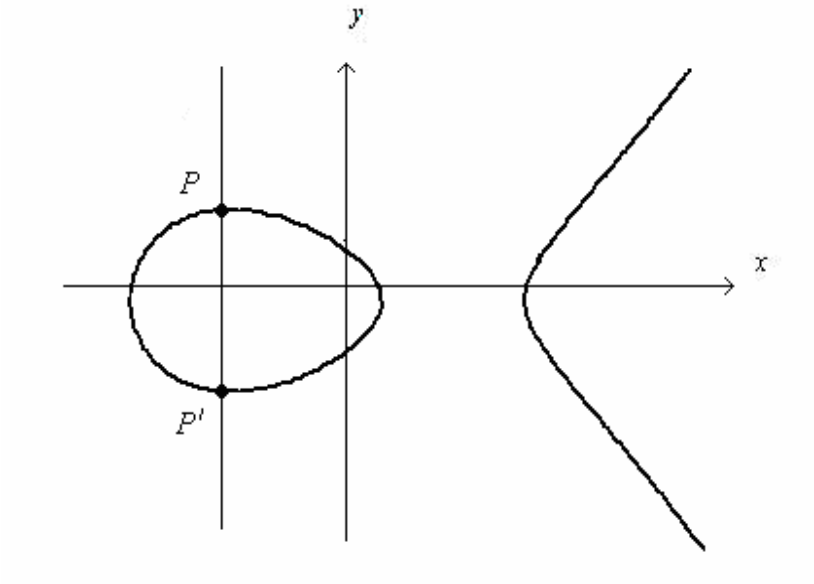
Axiome de symétrique :
Le point O_E à l'infini est déterminé par la direction de l'axe Oy (1)
Le symétrique P' d'un point P satisfait la relation :

$$P + P' = O_E \quad (2)$$

La règle de trois points colinéaires de *E* implique :

$$P + P' + O_E = O_E \quad (3)$$

D'après (1) la sécante passant par P, P' et O_E est parallèle à Oy.
Il en résulte que le symétrique P' de P est l'intersection de la parallèle à Oy passant par *P*, avec la courbe *E*.



$E : y^2 + y = x^3 - 7x + 3$
Courbe tracée avec le logiciel «ScientificWorkPlace»
Fi'ure1

Axiome de commutativité :
Soit une sécante passant par trois points P, R et S de la courbe ; alors :

$$P + R + S = O_E \qquad (1)$$

La sécante passant par les points R et P est confondue avec la sécante PR.
Il en résulte l'égalité :

$$P + R = R + P = -S$$

Axiome d'associativité :
Soit trois points non colinéaires M, N et P.
Pour vérifier l'associativité de la loi, il faut comparer les points

$$(M + N) + P \text{ et } M + (N + P)$$

Il faut donc calculer les coordonnées des sommes :

$$M + N = A \ , \ A + P = B \ , \ N + P = C \text{ et } M + C = D$$

Avec le calcul nous obtenons l'égalité $B = D$ et l'associativité :

$$(M + N) + P = M + (N + P)$$

□

2-Formules du symétrique $-P$ de la somme $P_1 + P_2$ et de la somme $P + P = 2P$:

Calcul des coordonnées d5 symétrique $-P$ d'un point P :

Soit un point $P = (x_P, y_P)$ sur une courbe elliptique E.
Son symétrique est l'intersection P' de la courbe E par la parallèle à Oy passant par P.
Equation de la parallèle : $x = x_P$ (1)
Cette parallèle coupe la courbe E en deux points de même abscisse $x = x_P$, et d'ordonnée y_P et $y_{P'}$ racines de l'équation du 2^e degré en y.

$$y^2 + a_1 x_P y + a_3 y = x_P^3 + a_2 x_P^2 + a_4 x + a_6 \qquad (2)$$

La somme des 2 racines est la fonction symétrique :

$$y_P + y_{P'} = -a_1 x_P - a_3 \qquad (3)$$

Cela implique les coordonnées du symétrique P' de P :

Pour $P = (x_P, y_P)$, alors $-P = P' = (x_P, -y_P - a_1 x_P - a_3)$ (4)

Calcul de la somme P_1+P_2 de deux points $P_i=(x_i,y_i)$, $P_1\neq\pm P_2$:

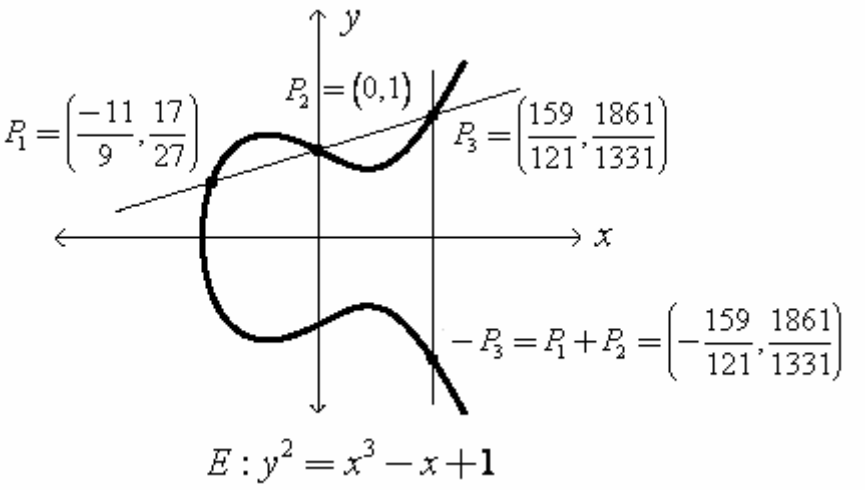


Image copiée de l'article « Rank of elliptic curves » de Alice Silverberg
Figure 2

D'après la règle géométrique de trois points colinéaires P_1,P_2,P_3 de la courbe E

$$P_1+P_2+P_3=O_E \qquad (1)$$

Cela implique la somme :

$$P_1+P_2=-P_3 \qquad (2)$$

Donc le point $P_1+P_2=M$ est l'intersection de la parallèle à Oy passant par P_3 avec la courbe.
Equation de la sécante P_1P_2 :

$$y-y_1=t(x-x_1)\ ,\ t=(y_1-y_2)/(x_1-x_2) \qquad (3)$$

Les abscisses des trois points P_1,P_2,P_3 sont les racines de l'équation cubique en x :

$$t^2(x-x_1)^2+t(x-x_1)(a_1x+a_3)=x^3+a_2x^2+a_4x+a_6 \qquad (4)$$

La somme $x_1+x_2+x_3$ est la fonction symétrique :

$$x_1+x_2+x_3=\frac{-\text{ coefficient de } x^2}{\text{coefficient de } x^3}=-a_2+t^2+a_1t \qquad (5)$$

Cela implique l'abscisse x_3 du point P_3 :

$$x_3 = t^2 + a_1 t - a_2 - x_1 - x_2 \qquad (6)$$

Les formules (3) et (6) impliquent l'ordonnée y_3 du point P_3 :

$$y_3 = t(x_3 - x_1) + y_1 \qquad (7)$$

Le point $P_1 + P_2 = -P_3$ est le symétrique de P_3.
Avec le calcul nous obtenons les coordonnées de la somme $P_1 + P_2$:

$$P_1 + P_2 = M = \begin{cases} x_M = t^2 + a_1 t - a_2 - x_1 - x_2 \\ y_M = t^3 + a_1 t^2 - t(a_2 + 2x_1 + x_2) + y_1 \\ t = (y_1 - y_2)/(x_1 - x_2) \end{cases} \qquad (8)$$

Rassemblons les résultats précédents sur $-P$ et $P_1 + P_2$

Proposition 2. *Soit une courbe elliptique E d'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) Le symétrique d'un point $P = (x_P, y_P)$ *de E est le point* $-P = (x_P, -y_P - a_1 x_P - a_3)$
2) Les coordonnées de la somme $P_1 + P_2$ *de deux points* $P_i = (x_i, y_i)$ *de E ,* $P_1 \neq \pm P_2$ *sont égales à :*

$$P_1 + P_2 = M = (x_M, y_M)$$
$$x_M = t^2 + a_1 t - a_2 - x_1 - x_2$$
$$y_M = t^3 + a_1 t^2 - t(a_2 + 2x_1 + x_2) + y_1$$
$$t = (y_1 - y_2)/(x_1 - x_2)$$

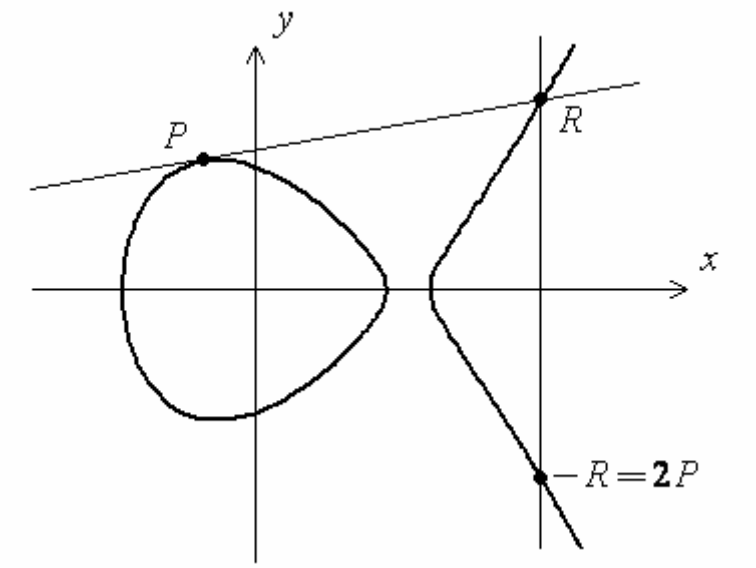
Preuve : □

Définition 1. *L'ensemble E(K) des points K-rationnels muni du point à l'infini* $O_E = (\infty, \infty)$ *est le groupe de Mordell-Weil de la courbe elliptique E.*

D'après la théorie des groupes abéliens, le groupe abélien de Mordell-Weil $E(K)$ possède des sous groupes abéliens et des sous groupes cycliques. Ces sous groupes cycliques sont engendrés par un point P du groupe de Mordell-Weil.
$\{P, 2P = O_E\}$, $\{M, 2M, 3M = O_E\}$, etc...

Calcul des coordonnées du point $P+P=2P$ pour $P=(x_P, y_P)$:

D'après la règle géométrique de trois points colinéaires de *E*,
la sécante passant par *P* et *P* est la tangente à la courbe elliptique *E*. (1)



$E : y^2 = x^3 - 4x^2 - 9x + 36$

Courbe tracée avec le logiciel «ScientificWorkPlace»

Figure 3

Cette tangente recoupe la courbe *E* en un troisième point simple :

$$R = (x_R, y_R) \qquad (2)$$

Equation de la tangente à *E* en *P* :

$$y - y_P = y'_P (x - x_P) \ , \ y'_P = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3} \qquad (3)$$

Avec le calcul nous obtenons les coordonnées de *R* :

$$R = (x_R, y_R) \text{ où } \begin{cases} x_R = y'^2_P + a_1 y'_P - 2x_P - a_2 \\ y_R = y'_P (x_R - x_P) + y_P \end{cases}$$

Avec la formule du symétrique $-R$ du point R, nous obtenons les coordonnées du point

$$2P=\left(x_{2P},y_{2P}\right),\begin{cases}x_{2P}=y_P'^2+a_1y_P'-2x_P-a_2\\ y_{2P}=-y_P'^3-2a_1y_P'^2+\left(a_2-a_1^2+3x_P\right)y_P'+a_1a_2-a_3+2a_1x_P-y_P\\ y'=\dfrac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}\end{cases}$$

Nous avons démontré la :

Proposition 3. *Soit une courbe elliptique E d'équation de Weierstrass*

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

Soit un point $P=\left(x_P,y_P\right)$ *de E. Alors les coordonnées du point* $P+P=2P=\left(x_{2P},y_{2P}\right)$ *sont égales à :*

$$x_{2P}=y_P'^2+a_1y_P'-2x_P-a_2$$
$$y_{2P}=-y_P'^3-2a_1y_P'^2+\left(a_2-a_1^2+3x_P\right)y_P'+a_1a_2-a_3+2a_1x_P-y_P$$
$$y'=\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}.$$

□

Avec ces deux propositions nous pouvons calculer les coordonnées de tout point mP, $m>2$.
Ainsi $3P=2P+P$, $4P=2\left(2P\right)$, $5P=4P+P$, etc...
Ces coordonnées sont des fonctions rationnelles de la forme :

$$x_{mP}=\frac{A\left(x_P,y_P\right)}{D\left(x_p,y_P\right)^2}\ \text{ et }\ y_{mP}=\frac{B\left(x_P,y_P\right)}{D\left(x_P,y_P\right)^3}.$$

On peut trouver des formules plus précises dans [*Cassels, Diophantine équation with spécial référence to elliptic curves*] et dans [*S.Lang, Elliptic curves. Diophantine analysis*].

3-Points d'ordre fini d'une courbe elliptique :

Dans la théorie des groupes, un point d'ordre fini est un point de torsion.
Un point P d'ordre m satisfait : $mP=O_E$.

Le symbole mP signifie : $\begin{cases}P+\cdots+P,\ m\ fois\ si\ m>0\\ \left(-P\right)+\cdots+\left(-P\right),\ \left(-m\right)\ fois\ si\ m<0\\ 0P=O_E\ \ pour\ m=0\end{cases}$

Etudions les sous groupes de *m-torsion* et le groupe de torsion d'une courbe elliptique.

Définition 2.

1) Pour tout entier $m \geq 2$, *le sous groupe de m-torsion d'une courbe elliptique E est l'ensemble :*

$$E(K)[m] = \{P \in E(K) \ ; \ mP = O_E\}.$$

2) Le groupe de torsion d'une courbe elliptique E est l'ensemble des points d'ordre fini :

$$T(E) = \{P \in E(K) \ ; \ mP = O_E \ \text{ pour } m \in \mathbb{Z}\}.$$

Donc le groupe de torsion est la réunion infinie des sous groupes de *m-torsion* :

$$T(E) = \bigcup_{m \in \mathbb{Z}} E(K)[m]$$

Il y a plusieurs résultats sur les points de *m-torsion*

Proposition 4. *Soit une courbe elliptique E d'équation de Weierstrass :*

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

dont les 5 coefficients a_1, a_2, a_3, a_4 et a_6 *soient des éléments de l'anneau* A_K *des entiers du corps K.*
Soit un point $P \in E(K)$ *d'ordre* $m \geq 2$, *m non puissance d'un nombre premier, alors les coordonnées du point P sont des entiers du corps K.*
□

Pour $K = \mathbb{Q}$, les coordonnées sont plus précises.

Proposition 5. *Soit une courbe elliptique d'équation de Weierstrass :*

$$E : y^2 = x^3 + Ax + B \ , \ A, B \in \mathbb{Z}, \ 4A^3 + 27B^2 \neq 0$$

Soit un point P de m-torsion de E, $m \geq 2$. *Alors :*
1) Les coordonnées de P sont des entiers rationnels.
2) Lorsque $2P \neq O_E$, *l'ordonnée* y_P *divise* $4A^3 + 27B^2$.

Preuve :
Lorsque $2P = O_E$, alors *l'ordonnée* $y_P = 0$.
Preuve par Lutz : « *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps p-adiques* » , *J.Reine Ang 177 (1937) 237-247*
et par Nagell : « *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre* » *Akad. Oslo (1935).*
□

Exemple de points de m-torsion :

Considérons la courbe elliptique d'équation de Weierstrass :

$$E : y^2 = x^3 - 43x + 166 \qquad (1)$$

Calcul du discriminant :

$$\Delta(E) = 4A^2 + 27B^2 = 425984 = 2^{15} \cdot 13 \qquad (2)$$

Pour $y = 0$ le polynôme $x^3 - 43x + 166$ est irréductible dans l'anneau $\mathbb{Q}[x]$. Donc il ne possède pas de racines rationnelles. Il en résulte que la courbe elliptique E ne possède pas de points rationnels d'ordre 2.
La proposition 5 implique que pour tout point $P = (x_P, y_P)$ d'ordre fini différent de 2, y_P divise le discriminant $\triangle(E) = 2^{15} \times 13$:

$$y_P = \pm 13 \text{ ou } \pm 2^t \text{ ou } \pm 13 \times 2^t \quad \text{avec } 0 \le t \le 15 \qquad (3)$$

(1) et (3) impliquent le groupe de torsion avec le calcul :

$$T\left(E(\mathbb{Q})\right) = \left\{(3, \pm 8),\ (-5, \pm 16),\ (11, \pm 32), O_E\right\}$$

La structure du groupe de torsion $T\left(E(\mathbb{Q})\right)$ d'une courbe elliptique *E* a été conjecturée par *Ogg* et démontrée par *Mazur.*

Théorème 1. *Le groupe de torsion $T\left(E(\mathbb{Q})\right)$ d'une courbe elliptique E est isomorphe à l'un des 15 groupes abéliens :*

$$\mathbb{Z}/n\mathbb{Z}\ ,\ 1 \le n \le 10 \text{ ou } n = 12$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\ ,\ 1 \le n \le 4$$

Preuve :
Mazur prouve qu'une courbe elliptique n'a pas de point de torsion d'ordre premier $N = 11$ ou $N \ge 13$, pour cela il utilise une courbe elliptique ayant bonne réduction potentielle en $p = 3$, les fibres de *Néron* sur le corps fini $\mathbb{F}_3$ et l'ordre du groupe de Mordell-Weil $E(\mathbb{F}_3)$.
Pour plus de détails, consulter Inv.Math. 44 «Rational isogenies of prime degre »(1978) 129-162.
□

4-Réduction de courbes elliptiques :

La réduction d'une courbe elliptique peut être utilisée pour la détermination d'un sous groupe de *m-torsion* .

Cette réduction s'obtient avec une valuation du corps *K* de la courbe elliptique.

La théorie des valuations se trouve dans les ouvrages de Théorie des Nombres comme :

"Algebraic Numbers and Algebraic Functions" par Artin
"Algebraic Numbers" par Lang
"Algebraic Number Theory" par Weiss
"Number Theory" par Hasse

Définition 3. *Une valuation sur un corps K est une fonction à valeurs réelles positives*

$$v : K \to \mathbb{R}^+$$

qui satisfait les axiomes :

(Val1) $v(x) \geq 0$, $v(x) = 0$ *si est seulement si* $x = 0$.

(Val2) $v(xy) = v(x)v(y)$ *pour tous éléments* x *et* y *du corps K.*

(Val3) $v(x+y) \leq c \max\{v(x), v(y)\}$ *pour* $c = 1$ ou $c = 2$.

La valuation v est triviale lorsqu'elle prend les valeurs :

$v(0) = 0$ et $v(x) = 1$ pour $x \neq 0$.

Les valuations sont classifiées selon la valeur de la constante c :

Pour $c = 1$, la valuation est non archimédienne.
Pour $c = 2$, la valuation est archimédienne.

Sur un corps *K* de caractéristique p , toutes les valuations non triviales sont non archimédiennes.

Valuation exponentielle :

Soit une valuation *v*. Par l'axiome $v(xy) = v(x)v(y)$, elle est multiplicative.
Cette valuation implique la fonction $\varphi : K \to \mathbb{R} \cup \infty$ de valeur $\varphi(x) = -\log v(x)$, c'est la valuation exponentielle ; elle satisfait les 3 axiomes $\varphi(x) = \infty$ si est seulement si $x = 0$, $\varphi(xy) = \varphi(x) + \varphi(y)$ et $\varphi(x+y) \geq \min\{\varphi(x), \varphi(y)\}$.
Cette valuation φ est additive.

Exemple de valuation non archimédienne : $c = 2$

Valuation p-adique v_p *du corps* $\mathbb{Q}$ *, p premier :*

Elle prend les valeurs $v_p(1) = 1$, $v_p(p) = \frac{1}{p}$ et $v_p(q) = 1$ pour tout nombre premier $q \neq p$.

Soit un nombre rationnel $x = a.p^r$, avec a premier à p. Alors $v_p(x) = \frac{1}{p^r}$. Cette valuation satisfait les axiomes des valuations non archimédiennes.

Exemple de valuation archimédienne : $c=1$

La valeur absolue sur $\mathbb{Q}$: $|x|=\max\{x,-x\}$.
Ainsi $|+3|=|-3|=3$, $|-101{,}8(=101{,}8$.

Cette notion de valuation est utilisée pour réduire les courbes elliptiques.

Définition 4. *Soit une courbe elliptique E, son corps de base K et une valuation v de K. La réduction modulo v est l'application :*

$$\begin{aligned} K &\longrightarrow \tilde{K} \\ a &\longrightarrow \tilde{a}=v(a) \end{aligned}$$

Elle s'applique aux points $P=(x_P,y_P)$ du groupe $E(K)$ par l'application :

$$\begin{aligned} E(K) \quad &\longrightarrow \quad \tilde{E}\left(\tilde{K}\right) \\ P=(x,y) &\longrightarrow \quad \tilde{P}=\left(v(x),v(y)\right) \end{aligned}$$

La réduction d'un point *P* est le point réduit $\tilde{P}$; la réduction de la courbe elliptique $E(K)$ est la courbe réduite $\tilde{E}\left(\tilde{K}\right)$. Cette réduction modulo v détermine deux sous ensembles du groupe $E(K)$:

$$E_0(K)=\left\{P\in E(K)\ ;\ \tilde{P} \text{ non singulier dans } \tilde{E}\left(\tilde{K}\right)\right\}$$
$$E_1(K)=\left\{P\in E(K)\ ;\ \tilde{P}=O_{\tilde{E}}\right\}$$

Exemple de réduction :
Soit la courbe elliptique *E* d'équation de Weierstrass :

$$E: y^2-10xy+6y=x^3+12x^2-14x+11\in\mathbb{Q}[x,y]$$

Appliquons la valuation *p-adique* v_p, pour $p=3$:
Nous obtenons l'équation de la courbe réduite

$$\tilde{E}: y^2+2xy=x^3+x+2\in\mathbb{F}_3[x,y]$$

Il y a plusieurs types de réductions suivant la valeur du discriminant de la courbe réduite. Selon Silverman les réductions sont classées par la :

Définition 5. *Soit une courbe elliptique E et sa courbe réduite $\tilde{E}$ modulo une valuation v du corps K.*

1) E a une bonne réduction sur K si la courbe réduite $\tilde{E}$ est elliptique.

2) E a une réduction multiplicative si $\tilde{E}$ a un nœud .

3) E a une réduction additive si $\tilde{E}$ a un point de rebroussement .

Dans les 2 cas où $\triangle(\tilde{E}) = 0$ la réduction est mauvaise

4) La réduction est stable si elle est bonne,
La réduction est semi stable si elle est multiplicative,
La réduction est instable si elle est additive.

Lorsque la valuation v est non archimédienne et discrète, nous considérons les 4 ensembles : l'anneau des v-entiers $A_v = \{x \in K \ , \ v(x) \geq 0\}$, l'idéal v-premier $M_v = \{x \in K, v(x) > 0\}$, le groupe des v-unités $U_v = \{x \in K \ , \ v(x) = 0\}$ et le corps résiduel A_v / M_v .

Les réductions sont classifiées par la

Proposition 6. *Soit une courbe elliptique E, une valuation v sur le corps K, les invariants $\triangle(E)$ et $c_4(E)$ de la courbe elliptique.*

1) E a une bonne réduction en v si et seulement si $v(\triangle(E)) = 0$; alors $\triangle(E)$ est une unité de $\tilde{K}$.

2) E a une réduction multiplicative si et seulement si $v(\triangle(E)) > 0$ et *$v(c_4) = 0$. Dans ce cas la partie $\tilde{E}_{ns}$ non singulière de la courbe réduite $\tilde{E}$ est isomorphe au groupe multiplicatif*

$$\tilde{E}_{ns}(\tilde{K}) \simeq \tilde{K}^*$$

3) E a une réduction additive en v si est seulement si $v(\triangle(E)) > 0$ et *$v(c_4) > 0$. Dans ce cas la partie non singulière $\tilde{E}_{ns}$ de la courbe réduite $\tilde{E}$ est isomorphe au groupe additif*

$$\tilde{E}_{ns}(\tilde{K}) \simeq \tilde{K}^+$$

□

Cette réduction possède plusieurs propriétés intéressantes

Proposition 7. *Soit une valuation non archimédienne discrète v et un entier m de valuation $v(m) = 0$. Soit une courbe elliptique E qui a bonne réduction en v. Alors l'application réduction :*

$$E(K)[m] \to \tilde{E}(\tilde{K})$$

est injective.

□

Le groupe de Galois d'une clôture algébrique de *K* et un sous groupe de m-torsion sont liés par l'application bilinéaire de Kummer :

Définition 6. *L'application bilinéaire de Kummer est l'application :*

$$\lambda : E(K) \times G\left(K_{a\lg} / K\right) \to E(K)[m]$$

de valeur $\lambda(P,\sigma) = \sigma(R) - R$ avec $P = mR$.

Proposition 8.

1) L'application de Kummer est bilinéaire ;

2) Son noyau à gauche est le sous groupe $mE(K)$ *;*

3) Son noyau à droite est le groupe de Galois
$G\left(K_{a\lg} / L\right)$ où $L = K\left(m^{-1}E(K)\right) =$ composé de tous les corps $K(R)$ lorsque $mR \in E(K)$.

4) L est une extension abélienne d'exposant m :
tout élément de L est d'ordre divisant m.

Preuve : Proposition 1-2 et 1-5 du chapitre VIII « Silverman ».
□

Illustrons cette théorie par quelques exemples :

Exemple 1 :

Courbe elliptique E_1 d'équation de Weierstrass :

$$E_1 : y^2 = x^3 + 3x^2 + 22x - 24$$

Calculs des invariants :

$$\triangle(E_1) = 1000000 = 2^6 \times 5^6$$

$$c_4(E_1) = 1200 = 2^4 \times 3 \times 5^2$$

Réduction de la courbe E_1 modulo la valuation v_5 :

$$v_5\left(\triangle(E_1)\right) = 6 > 0$$

$$v_5\left(c_4(E_1)\right) = 2 > 0$$

D'après la proposition 6, il en résulte que la courbe elliptique E_1 a une réduction additive modulo la valuation v_5

Exemple 2 :

Courbe elliptique E_2 d'équation de Weierstrass :

$$E_2 : y^2 = x^3 + 6x^2 - x - 6$$

Calculs des invariants :

$$\triangle(E_2) = 78400 = 2^6 \times 5^2 \times 7^2$$

$$c_4(E_2) = 624 = 2^4 \times 3 \times 13$$

Réduction de la courbe E_2 modulo la valuation v_5 :

$$v_5\left(\triangle(E_2)\right) = 2 > 0$$

$$v_5\left(c_4(E_2)\right) = 0$$

On en déduit que la courbe E_2 a une réduction multiplicative modulo la valuation v_5.

Réduction de la courbe E_2 modulo la valuation v_{13} :

$$v_{13}\left(\triangle\left(E_2\right)\right)=0$$

On en déduit que la courbe E_2 a une bonne réduction modulo la valuation v_{13}.

Chapitre III : Rang d'une courbe elliptique

1. Introduction :

Selon l'ouvrage « elliptic curves, diophantine analysis » chapitre IV, Height de Lang, c'est en 1922 que Mordell a prouvé une conjecture de Poincaré prévoyant que le groupe des points rationnels d'une courbe elliptique est de type fini. En 1929/1930 Weil a étendu ce résultat aux variétés abéliennes.
C'est sans doute de là que vient le vocable de groupe de Mordell-Weil d'une courbe elliptique.

Proposition 1. *Le groupe* $E(K)$ *des points K-rationnels d'une courbe elliptique E est de type fini.*
□

La démonstration de cette proposition comporte deux parties.
Une partie où l'on prouve que le groupe quotient $E(K)/mE(K)$ est fini pour $m=2$.
Une autre partie, basée sur des fonctions hauteurs, où l'on détermine la structure du groupe abélien $E(K)$.
C'est le théorème de *Mordell-Weil*.

2. Groupe quotient $E(K)/2E(K)$:

Etudions le groupe quotient $E(K)/2E(K)$

Proposition 2. *Le groupe quotient* $E(K)/2E(K)$ *est fini***.**

Preuve :
On utilise des homomorphismes de groupes abéliens :

$$\theta_i : E(K) \to K^* / K^{*2}$$

dont les noyaux satisfont la relation :

$$\bigcap_{i=1}^{3} \ker \theta_i \subset 2E(K)$$

L'équation de Weierstrass de la courbe E est de la forme :

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3)$$

Pour $carac(K) \neq 2,3$ les fonctions θ_i prennent les valeurs :

$$\theta_i(O_E) = 1 \ ; \ \theta_i(x,y) = x - e_i \text{ si } x \neq e_i$$
$$\theta_i(e_i, 0) = (e_i - e_*)(e_i - e_k)$$

Pour d'autres détails consulter [Lang] et [Silverman].
□

3. Hauteurs sur une courbe elliptique :

Nous introduisons des fonctions particulières : les hauteurs sur les groupes abéliens.

Définition 1. *Une hauteur sur un groupe abélien A est une fonction à valeurs réelles sur A*

$$h : A \to \mathbb{R}$$

qui satisfait les 3 axiomes :

(h1) Soit un point P_0 *de A ; alors il y a une constante réelle* $c_0(P_0, A) = c_0$ *telle que :*

$h(P_0 + P) \leq 2h(P) + c_0$, pour tout point $P \in A$.

(h2) Il y a un entier $m \geq 2$ *et une constante* $c_1(A) = c_1$ *tels que :*

$h(mP) \geq m^2 h(P) - c_1$, pour tout point $P \in A$.

(h3) Pour toute constante c, l'ensemble des points de hauteur bornée par c :

$$\{P \in A \,;\, h(P) \leq c\}$$

est fini.

Une telle fonction hauteur n'est pas unique, elle est déterminée par sa valeur $h(P)$: hauteur logarithmique, hauteur de Weil, hauteur canonique, hauteur locale, etc…

Proposition 3. *Soit un groupe abélien* A *tel que le groupe quotient* A/mA *soit fini. Alors le groupe* A *est de type fini*.

Preuve :
Nous utilisons un algorithme de descente infinie pour construire une suite infinie $P,\ P_1,...,\ P_n,...$ de points de A.
Choisissons des représentants $T_1,\ T_2,...,\ T_r$ des classes A/mA (1)
Soit un point $P \in A$ égal à la combinaison linéaire

$$P = mP_1 + T_{i_1} \quad \text{pour } 1 \leq i_1 \leq r \qquad (2)$$

Le point P_1 est une combinaison linéaire

$$P_1 = mP_2 + T_{i_2} \quad \text{pour } 1 \leq i_2 \leq r \qquad (3)$$

Nous obtenons une suite de points $P_i \in A$ combinaisons linéaires

$$P_j = mP_{j+1} + T_{i_{j+1}} \quad \text{pour } 1 \leq i_{j+1} \leq r \qquad (4)$$

……

$$P_{n-1} = mP_n + T_{i_n} \quad \text{pour } 1 \leq i_n \leq r \qquad (5)$$

Appliquons à la relation :

$$P_{j-1} - T_{i_j} = mP_j \qquad (4-1)$$

l'axiome *(h1)* à gauche et l'axiome *(h2)* à droite

$$h(P_j) \le \frac{1}{m^2}\left[2h(mP_{j-1}+1)+c_j\right] \qquad (6)$$

Addi4ionnons membre à membre les inégalités (6) de P à P_n.

Nous obtenons l'inégalité :

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2}+\frac{2}{m^4}+\cdots+\frac{2^{n-1}}{m^{2n}}\right).c_4$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{c_4}{m^2-2} \qquad (7)$$

L'hypothèse $m \ge 2$ implique : $\frac{2}{m^2} \le 2$

La formule (7) implique l'inégalité :

$$h(P_n) \le \frac{h(P)}{2^n} + \frac{c_4}{2} < 1 + \frac{c_4}{2} \qquad (8)$$

L'axiome *(h3)* appliqué à l'inégalité (8) implique que l'ensemble $\{P_n\}$ est fini.

$$\{P_n\} = \{B_1, B_2, ..., B_N\} \qquad (9)$$

Les relations $(1), (2)$ et (9) impliquent que tout élément $P \in A$ est une combinaison linéaire :

$$P = k_1T_1 + \cdots + k_rT_r + l_1B_1 + \cdots + l_NB_N \ , \ k_i \text{ et } l_j \in \mathbb{Z} \qquad (10)$$

Donc le groupe abélien *A* est de type fini.
□

Cette méthode est la descente infinie sur une courbe elliptique.

Corollaire. *Le groupe de Mordell-Weil $E(\mathbb{Q})$ d'une courbe elliptique E est de type fini.*

Preuve :
Le groupe quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ est abélien fini. Les représentants $T_1, T_2, ..., T_r$ de l'ensemble des classes et les points $B_1, ..., B_N$ fournis par l'algorithme de la descente infinie engendrent le groupe abélien $E(\mathbb{Q})$.
□

La structure du groupe de Mordell-Weil est semblable à la structure du groupe des unités d'un corps *K*.

Théorème 1. *(Minkowski). Les unités d'un corps K, de degré* $n = r + 2s$ *, où* r *est le nombre de corps conjugués réels et* s *le nombre de paires de corps conjugués complexes de K, forment un groupe abélien* $U(K)$ *isomorphe à un produit de groupes abéliens :*

$$U(K) \simeq C(K) \times \mathbb{Z}^t$$

$C(K) =$ *groupe des ra#ines de l'unité dans K,*

$t = r + s - 1 =$ *rang du groupe* $U(K)$ *des unités de K.*

□

4. Rang d'une courbe elliptique :

La structure du groupe de Mordell-Weil $E(K)$ est précisée par la

Proposition 4. *Soit une courbe elliptique E de groupe de torsion* $T(E)$ *et de groupe de Mordell-Weil* $E(K)$*. Alors le groupe abélien* $E(K)$ *est isomorphe au produit de groupes abéliens :*

$$E(K) \simeq T(E) \times \mathbb{Z}^r$$

où $r = r(E)$ *est un entier non négatif ,*

$\mathbb{Z}^r =$ *r copies du groupe abélien* $\mathbb{Z}$ *.*

□

Définition 2. *L'entier* $r = r(E)$ *de la formule d'isomorphisme est le rang de la courbe elliptique E.*

Si le calcul du rang t du groupe des unités $U(K)$ s'obtient avec une formule simple, il n'y a pas de formule simple permettant de calculer le rang $r(E)$ d'une courbe elliptique.

Le théorème de descente infinie indique un moyen d'obtenir des points $P_1, P_2, ..., P_r$, d'ordre infini, qui engendrent le groupe quotient $E(K)/T(E)$. Ce sont les points de hauteur minimale

Quelques hauteurs :

1. La hauteur d'un point de l'espace projectif $\mathbb{P}^N(\mathbb{Q})$ est la fonction :

$$\begin{aligned} h_{\mathbb{Q}} : \mathbb{P}^N(\mathbb{Q}) &\longrightarrow \mathbb{R}^+ \\ x \quad &\longrightarrow h(x) = \prod_v \max |x_i|_v \ , \ x = (x_1, ..., x_N, x_{N+1}) \end{aligned}$$

La formule du produit pour les valuations v sur le corps $\mathbb{Q}$:

$$\prod_v |a|_v = 1 \text{ pour } a \in \mathbb{Q},\ a \neq 0$$

implique que la hauteur $h_{\mathbb{Q}}$ est indépendante du choix des coordonnées.

2. La hauteur sur le corps $\mathbb{Q}$ des nombres rationnels est la fonction :

$$\begin{aligned} h_{\mathbb{Q}} : \mathbb{Q} &\longrightarrow \mathbb{R}^+ \\ a &\longrightarrow h\left(a = \frac{p}{q}\right) = \max\left\{|p|,|q|\right\} \end{aligned}$$

3. La hauteur logarithmique sur le groupe $E(\mathbb{Q})$ est la fonction :

$$\begin{aligned} h_x : E(\mathbb{Q}) &\longrightarrow \mathbb{R}^+ \\ P &\longrightarrow h_x\left(\frac{a}{b}\right) = \log \max\left\{|a|,|b|\right\} \text{ pour } x(P) = \frac{a}{b} \\ & h_x(O_E) = 0 \end{aligned}$$

C'est la hauteur de Weil.

4. Soit une courbe elliptique E de groupe $E(K)$ et une fonction paire $f \in K_{alg}(E)$, la hauteur relative à f est la fonction :

$$\begin{aligned} h_f : E\left(K_{alg}\right) &\to \mathbb{R} \\ P &\to h_f(P) = h\left(f(P)\right),\ h = \text{hauteur logarithmique} \end{aligned}$$

5. La hauteur canonique (ou de Néron-Tate) sur $E(K)$ est la fonction :

$$\begin{aligned} \hat{h} : E\left(K_{alg}\right) &\longrightarrow \mathbb{R} \\ P &\longrightarrow \hat{h}(P) = \frac{1}{\deg f} \cdot \lim_{N\to\infty} 4^{-N} h_f\left(2^N P\right) \end{aligned}$$

où f est une fonction paire non constante, $f \in K_{alg}(E)$.

Calculons les hauteurs logarithmiques de quelques points de la courbe elliptique d'équation

$$E : y^2 = x^3 - x + 1$$

Coordonnées de 3 points de la courbe :

$$\begin{aligned} P_1 &= \left(\frac{-11}{9}, \frac{17}{27}\right) \\ P_2 &= (0,1) \\ P_3 &= \left(\frac{159}{121}, \frac{1861}{1331}\right) \end{aligned}$$

Calcul des hauteurs logarithmiques de ces 3 points P_i :

$$h(P_1) = \log\left(\max\left\{|-11|,|9|\right\}\right) = \log(11)$$

$$h(P_2) = \log\max\left\{|0|,|1|\right\} = \log(1) = 0$$

$$h(P_3) = \log\left(\max\left\{|159|,|121|\right\}\right) = \log(159)$$

Ces 3 exemples ne suffisent pas pour déterminer des générateurs du groupe de Mordell-Weil $E(\mathbb{Q})$.

La hauteur canonique $\hat{h}$ possède plusieurs propriétés.

Proposition 5. *Soit la hauteur canonique $\hat{h}$ sur le groupe de Mordell-Weil $E(K)$. Alors $\hat{h}$ satisfait* **:**

1) $\hat{h}(P+R)+\hat{h}(P-R) = 2\hat{h}(P)+2\hat{h}(R)$ *pour tout* $P,R \in E$ *, c'est la loi du parallélogramme.*

2) $\hat{h}(mP) = m^2\hat{h}(P)$ pour tout entier $m \in \mathbb{Z}$.

3) Il existe une forme bilinéaire sur $E \times E$ associée à la forme quadratique $\hat{h}$:

$$\langle .,. \rangle : E(K) \times E(K) \to \mathbb{R}$$

de valeur :

$$\langle P,R \rangle = \frac{1}{2}\left[\hat{h}(P+R) - \hat{h}(P) - \hat{h}(R)\right]$$

4) $\hat{h}(P) > 0$ pour $P \neq O_E$ et $\hat{h}(P) = 0$ *si et seulement si P est un point de torsion de la courbe elliptique.*

Preuve : Cf. Silverman.

□

Soit un corps K muni d'une valuation discrète non archimédienne *v*. D'après la théorie des valuations, il admet un corps complet K_v.

Le degré local du corps K_v est égal à :

$$n_v = [K_v : \mathbb{Q}_v],\ \mathbb{Q}_v = \text{ complété de } \mathbb{Q} \text{ en } v$$

Définition 3. *La hauteur locale du groupe* $E(K)$ *en la valuation* v*, non archimédienne discrète, est la fonction* **:**

$$\lambda_v : E(K_v) - O_E \to \mathbb{R}$$

qui sati3fait les axiomes :

1) λ_v *est continue pour la topologie v-adique sur* $E(K_v)$ *et pour la topologie usuelle sur le corps* $\mathbb{R}$ *des réels.*

2) $\lim_{P \to O_E} \left(\lambda_v(P) + \frac{1}{2} v(x_P) \right)$ existe.

3) Pour tout point $P \in E(K_v)$ avec $2P \neq O_E$*, alors* :

$$\lambda_v(2P) = 4\lambda_v(P) + v(2y_P + a_1 x_P + a_3) - \frac{1}{4} v(\triangle(E))$$

4) Pour tout couple de points P,R de $E(K_v)$:

$$\lambda_v(P+R) + \lambda_v(P-R) = 2\lambda_v(P) + 2\lambda_v(R) + v(x_P - x_R) - \frac{1}{6} v(\triangle(E))$$

Preuve : Cf. Théorème 18.1, Silverman, C- paragraphe 18.
□

La hauteur canonique (de Néron-Tate) $\hat{h}$ est liée aux hauteurs locales λ_v par la

Proposition 6. *Soit une courbe elliptique E de point à l'infini* O_E*, un corps K, l'ensemble* V_K *des valuations non équivalentes du corps K, le degré local* $n_v = [K_v : \mathbb{Q}_v]$ *et les hauteurs locales* λ_v*.*

Alors la hauteur canonique $\hat{h}$ *est liée aux valuations* v *par* :

$$\hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in V_K} n_v \lambda_v(P)$$

Preuve : *Cf. théorème 18.2 Silverman.*
□

Signalons 2 publications sur la différence entre hauteurs sur les courbes elliptiques :

1) Zimmer: « On the difference of the Weil height and the Neron-Tate », Math Z, 147 (1976) pp 35-51.

Courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = 4x^3 - g_2 x - g_3$$

Hauteur de Weil : $h : E(K) \to \mathbb{R}$ de valeur :

$$h(x) = \log\left(H_K(x)\right)^{\frac{1}{N}} \ , \ N = [K : \mathbb{Q}], H_K(x) = \prod_v \max\left(1, v(x)\right)$$

et $h(O_E) = 0$.

Hauteur de Néron-Tate $\hat{h}(P) = \lim_{m \to \infty} m^{-2} h(mP)$, alors $\left| \hat{h}(P) - h(P) \right| \leq$ constante $c = c(g_2, g_3)$

2) J. H. Silverman : "the difference between the Weil height and the canonical height on elliptic curves " Math .Comp 35-192-(oct1990) 723-743.

C'est la différence $\hat{h}(P)-\frac{1}{2}h(x_P)$ qui est estimée par les inégalités

$$-\frac{1}{8}h(j(E))-\frac{1}{12}h(\triangle(E))-0.973\le\hat{h}(P)-\frac{1}{2}h(x_P)\le\frac{1}{12}h(j(E))+\frac{1}{12}h(\triangle(E))+1.03$$

5-Régulateur et Rang :

L'ensemble $\{P_1,...,P_r\}$ des r générateurs du groupe de Mordell-Weil $E(K)$ détermine un invariant : le régulateur de *E*.

Définition 4.

1) La forme bilinéaire de Néron-Tate sur le groupe de Mordell-Weil $E(K)$ est la forme quadratique positive :

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

de valeur :

$$\langle P,R\rangle \quad \hat{h}(P\quad R)\quad \hat{h}(P)\quad \hat{h}(R)$$

où $\hat{h}$ est la hauteur de Néron-Tate (hauteur canonique sur E).

2) Le régulateur d'une courbe elliptique E est le déterminant d'ordre r :

$$R(E)=\det\left(\langle P_i,P_j\rangle\right)\ ,\ 1\le i,j\le r$$

Par convention $R(E)=1$ *lorsque* $\det(\langle .,.\rangle)=0$.

Selon *A. BRUMER* et *K. KRAMER « The rank of elliptic curves, Duke math. J vol 44, des1977, p715 à 743 »,* les méthodes classiques de descente pour obtenir une borne supérieure du rang du groupe de *Mordell-Weil* d'une courbe elliptique dépendent de l'existence d'isogénies de degrés 2 ou 3 et d'équations explicites.

Des bornes pour le rang du groupe de *Selmer* des courbes elliptiques impliquent des bornes pour le rang du groupe de *Mordell-Weil* .

Ces résultats suggèrent que les courbes de conducteurs premiers ont les plus petits rangs. Cela est compatible avec les prédict)ons de parité de *Birch et Swinnerton-Dyer*.

Les deux auteurs ont obtenu plusieurs résultats.

1) Deux courbes elliptiques

$E_1 : y^2+xy+y=x^3-x^2-9x-8$, de rang $r(E)=0$.

$E_2 : y^2+xy=x^3-1$, de rang $r(E)=1$.

de même conducteur $N(E_i)=431$, et même discriminant $\Delta(E_i)=-431$.

2) deux courbes elliptiques :

$E_3 : y^2 + xy + y = x^3 - 84x - 301$, de groupe de *Selmer* $S(E_3)$ de rang 2.

$E_4 : y^2 + xy = x^3 - 3x - 2$, de groupe de *Selmer* $S(E_3)$ de rang 1.

d'invariant $\Delta(E_i) = N(E_i) = 443$.

3) deux courbes elliptiques :

$E_5 : y^2 + xy + y = x^3 - x^2 - 9x - 8$, de rang $r(E_5) = 3$

$E_6 : y^2 + xy + y = x^3 - x^2 - 9x - 8$, de rang $r(E_6) = 1$

de même discriminant $\Delta(E_i) = 18097$.

Chapitre IV : Série *L*(*E*,*s*) d'une courbe elliptique et Applications

Pour traiter ce chapitre nous nous sommes inspirés de plusieurs ouvrages.
« Modular Forms and Dirichlet Series » de OGG.
« Dirichlet Series and Automorphic Forms » de WEIL.
« The Arithmetic of Elliptic Curves » de SILVERMAN ».

1-Introduction :

La plus simple et la plus fameuse série de Dirichlet est la fonction Zêta de Riemann

$$\zeta(s)=\sum_{n\geq 1} n^{-s}=\prod_{p(\text{premier})}\left(1-p^{-s}\right)^{-1}, \operatorname{Re}(s)>1 \qquad (1)$$

Riemann a prouvé en 1859 que cette fonction zêta $\zeta(s)$ admet un prolongement analytique dans le demi *s*-plan sauf en $s=1$, qui est un pôle de résidu égal à 1. Cette fonction satisfait l'équation fonctionnelle :

$$Z(s)=\pi^{-s/2}\cdot\Gamma\left(\frac{s}{2}\right)\cdot\zeta(s)=Z(1-s) \qquad (2)$$

et

$$\Gamma(s)=\int_0^{\infty} t^{s-1}e^{-t}dt\ ,\ \operatorname{Re}(s)>1 \qquad (3)$$

Définition 1. *La fonction Zêta d'une courbe elliptique* E *sur un corps fini* $\mathbb{F}_q$ *est égale à :*

$$\zeta_E\left(s,\mathbb{F}_q\right)=\frac{1-q^{-s}+q^{1-2s}}{\left(1-q^{-s}\right)\cdot\left(1-q^{1-s}\right)}\ ,\ q=p^n, p \text{ premier} \qquad (4)$$

Elle satisfait l'équation fonctionnelle :

$$\zeta_E\left(s,\mathbb{F}_q\right)=\zeta_E\left(1-s,\mathbb{F}_q\right) \qquad (5)$$

Nous introduisons un invariant important des courbes elliptiques.

2-Série *L* d'une courbe elliptique :

La série *L* de Dirichlet joue un rôle important dans la conjecture de Birch et Swinnerton-Dyer, elle est donnée par la

Définition 2. *La série* $L(E,s)$ *de Dirichlet d'une courbe elliptique* $E/\mathbb{Q}$ *de discriminant* $\triangle(E)$ *et de conducteur* $N(E)$ *est égale à* **:**

$$L(E,s)=\prod_p\left(1-t_p p^{-s}\right)^{-1}\cdot\prod_q\left(1-t_q q^{-s}+q^{1-2s}\right)^{-1} \qquad (6)$$

où $p=$ diviseur premier de $\triangle(E)$ et $q=$ nombre premier ne divisant pas $\triangle(E)$.

Lorsque p divise le discriminant $\triangle(E)$ alors t_p satisfait :
$t_p = 1, -1$ ou 0 suivant que la courbe réduite $\tilde{E}(\mathbb{F}_p)$ a un nœud à tangentes rationnelles ou un nœud à tangentes quadratiques sur $\mathbb{F}_p$ ou un point de rebroussement. (7)

Dans le cas où p ne divise pas $\triangle(E)$, alors t_p est la trace de l'endomorphisme de Frobenius

$$\text{Frob} : E(\mathbb{F}_p) \to E(\mathbb{F}_p),\ x \to x^p$$

Ce nombre satisfait l'inégalité :

$$|t_p| \leq 2\sqrt{p} \qquad (8)$$

Le nombre t_p est de la forme :

$$t_p = 1 + p - A_p \qquad (9)$$

où $A_p =$ nombre de points du groupe de Mordell-Weil $\tilde{E}(\mathbb{F}_p)$.
Cette série de Dirichlet $L(E,s)$ est associée au conducteur $N(E)$ de la courbe E dans la fonction complexe :

$$\theta(E,s) = N(E)^{-s/2} \cdot (2\pi)^{-s} \cdot \Gamma(s) \cdot L(E,s) \qquad (10)$$

Conjecture 1. *La fonction complexe $\theta(E,s)$ est holomorphe dans le s-plan et satisfait l'équation fonctionnelle :*

$$\theta(E,s) = u \cdot \theta(E, 2-s) \text{ avec } u = \pm 1 \qquad (11)$$

Le nombre u est le signe de l'équation fonctionnelle $\theta(E,s)$ de la courbe elliptique E.

Dans « the arithmetic of ellipric curves de J. Tate » et « the arithmetic of elliptic curves de Silverman», il y a plus de renseignements sur cette fonction.

Les zéros de la fonction $L(E,s)$ ne sont calculables que dans les cas numériques. Dans le cas général, ils sont liés à une conjecture.

Selon Silverman, Weil et Taniyama ont conjecturé que l'équation fonctionnelle de la série de Dirichlet $L(E,s)$ est vraie si la courbe elliptique E est paramétrée par les fonctions modulaires.

Conjecture 2. *Soit une courbe elliptique* $E/\mathbb{Q}$ *de conducteur* $N(E)$ *et de série L égale à* $L(E,s)=\sum c(n).n^{-s}$. *Cette série* $L(E,s)$ *admet une transformée de Mellin inverse* $f(z)=\sum c(n).q^n$, *avec* $q=\exp(2\pi iz)$. *Alors :*

1) $f(z)$ *est une forme parabolique de poids 2 pour le sous groupe de congruence modulaire* $\Gamma_0(N)$ *du groupe modulaire* $SL(2,\mathbb{Z})$.

2) Pour chaque nombre premier p ne divisant pas $N(E)$, *l'opérateur de Hecke* $T(p)$ *opère sur la forme* f *par la formule :*

$$T(p).f=c(p).f$$

□

C'est la conjecture de Taniyama-Weil.

La théorie des opérateurs de Hecke est exposée dans un ouvrage de HECKE (1936) et dans d'autres ouvrages (G. SHIMURA (1971), T. APOSTOL (1980), J.H. SILVERMAN (1986)). Décrivons la définition et quelques propriétés.

Définition. *Soit l'espace vectoriel complexe* M_k *des formes modulaires de poids k ; les opérateurs de Hecke sont les opérateurs linéaires* $T(n):M_k\to M_k$, $n=1,2,...$

de valeur $\left(T(n)f\right)(z)=n^{k-1}\sum_d d^{-k}\sum_{0\le b\le d-1} f\left(\frac{nz+bd}{d^2}\right)$ *où d parcourt l'ensemble des diviseurs de n.*

Cette valeur se simplifie pour $n=p$ *premier.*

$$\left(T(p)f\right)(z)=p^{k-1}f(zp)+\frac{1}{p}\sum_{0\le b\le p-1} f\left(\frac{z+b}{d^2}\right)$$

Ces opérateurs $T(n)$ *dépendent donc de la nature de l'entier n.*

Proposition. *Les opérateurs de Hecke* $T(n)$ *satisfont les relations :*

1) $T(m)T(n)=T(mn)$ *pour tous les entiers m et n premier entre eux.*

2) $T(m)T(n)=T(n)T(m)$ *pour tous les entiers m et n.*

3) $T\left(p^{r+1}\right)=T\left(p^r\right)T(p)-p^{r-1}T\left(p^{r-1}\right)$ *pour tout nombre premier p et tout entier* $r\ge 1$.

4) $T(n)f=\lambda(n)f$ *pour n=1,2,…*

les coefficients $\lambda(n)$ *satisfont* $\lambda(n)=c(n)/c(1)$ *lorsque* $f=\sum c(n)q^n$.

□

L'ordre du zéro de la série de Dirichlet $L(E,s)$ en $s=1$ peut être calculé en fonction de certains invariants de la courbe elliptique $E/\mathbb{Q}$.

3-Conjecture de Birch et Swinnerton-Dyer :

Il est conjecturé que l'ordre du zéro de la série de Dirichlet $L(E,s)$ en $s=1$ est égal au rang r du groupe de Mordell-Weil $E(\mathbb{Q})$.

Conjecture 3.

(a) La série $L(E,s)$ a un zéro en $s=1$ d'ordre égal au rang du groupe de Mordell-Weil $E(\mathbb{Q})$.

(b) Soit r le rang du groupe $E(\mathbb{Q})$. Alors :

$$\lim_{s\to 1}(s-1)^{-r} L(E,s) = \Omega \cdot \text{Ш}(E) \cdot R(E) \cdot card\left(\text{T}\left(E(\mathbb{Q})\right)\right)^{-2} \cdot \prod_p c_p$$

Dans cette formule :

$\Omega = \int_{E(\mathbb{R})} \omega =$ période réelle ou 2 périodes réelles.

où $\omega = dx/(2y + a_1 x + a_3)$

$\text{Ш}(E) =$ Groupe de Tate-Shafarévitch de la courbe elliptique E.

$R(E) =$ Régulateur de la courbe elliptique E.

Définition 3. *Le nombre r figurant dans la conjecture Birch et Swinnerton-Dyer est le rang analytique r_{an} de la courbe elliptique E.*

Il y a plusieurs conjectures sur ce rang analytique.

Conjecture 4. *Le rang $r(E)$ et le rang analytique r_{an} d'une courbe elliptique E sont de même parité.*

C'est la conjecture de parité d'une courbe elliptique $E/\mathbb{Q}$.
Cette parité est liée au signe $u = \pm 1$ de l'équation fonctionnelle de la série $L(E,s)$ par la :

Conjecture 5. *Le rang $r(E)$ est pair si le signe de l'équation fonctionnelle de $L(E,s)$ est positif, $r(E)$ est impai2 si ce signe est négatif.*

Le calcul de la valeur de $L(E,s)$ et de ses dérivées en $s=1$ permet de trouver le rang analytique d'une courbe elliptique *E.*

Citons des exemples de calculs de rangs et de valeurs $L(E,s)$:

(1) « Rank zero of quadratic twists of modular elliptic curves » par K.Ono, composition Math vol 104 – n° 3 (1996) 304-319.

Soit la famille de courbes modulaires elliptiques d'équation :

$$E(M,N): y^2 = x^3 + (M+N)x^2 + MNx \ , \ \textit{avec des entiers } M \neq N$$

Le *D*-twist quadratique de la courbe *E*, par un entier $D \equiv 1 \mod N$ est la courbe elliptique d'équation de Weierstrass :

$$y^2 = x^3 + D(M+N)x^2 + D^2MNx$$

Pour $1 \leq t \leq 23$ et $D \equiv t \mod 24$, Ono a obtenu les couples :

$$(M,N) = 6D(4,3),\ 6D(1,-3),\ 6D(1,9), \text{ avec } 6D(a,b) = (6Da, 6Db)$$

(2) « On the conjecture B-S-D for an elliptic curve of rank 3 », par Buhler, Zagier et Gross. Math Comput. (1985) Vol (44) pages : 473-481.

Les auteurs ont étudié la courbe elliptique d'équation de Weierstrass :

$$E: y^2 = 4x^3 - 28x + 25 \in \mathbb{Q}[x,y] \qquad (1)$$

Calcul des invariants :

$$b_2 = 0 \ ; \ b_4 = -14 \ ; \ b_6 = 25 \ ; \ b_8 = -49 \ ; \ \triangle(E) = N(E) = 5077$$

Le changement de variable :

$$x \to x \ , \ y \to 2y + 1$$

transforme (1) en l'équation :

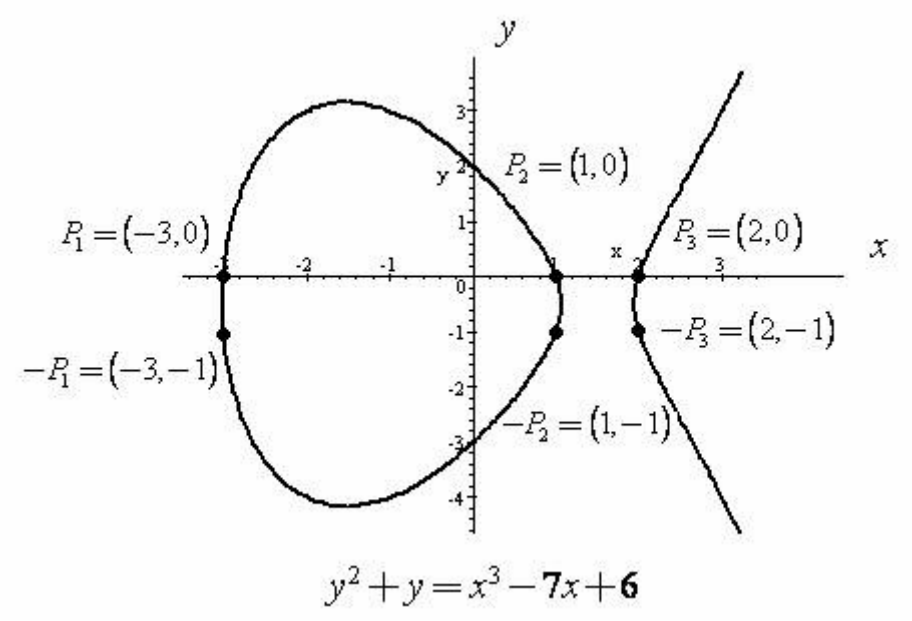
$$E_1: y^2 + y = x^3 - 7x + 6 \in \mathbb{Q}[x,y]$$

Calcul des coordonnées de quelques points de $E(\mathbb{Q})$:

$$P_1 = (-3,0); P_2 = (1,0); P_3 = (2,0)$$

et leurs symétriques :

$$-P_1 = (-3,-1); -P_2 = (1,-1); -P_3 = (2,-1)$$



Courbe tracée par le logiciel « ScientificWorkplace »

Pour obtenir le rang $r(E)$ de E, les auteurs utilisent la réduction modulo p.
Le nombre N_p de points du groupe $E(\mathbb{F}_p)$ est égal à :

$$N_3 = 7 \text{ pour } p = 3 \text{ et } N_7 = 10 \text{ pour } p = 7$$

Il en résulte que le groupe de Mordell-Weil $E(\mathbb{Q})$ est libre.
Avec la hauteur canonique $\hat{h}$ sur E, ils obtiennent 3 points de hauteur $\hat{h}(P)<1$:

$$P_1=(0,2)\ ,\ P_2=(1,0)\ ,\ P_3=(2,0)$$

Ces 3 points linéairement indépendants engendrent le group% $E(\mathbb{Q})$.

Cela implique que le rang $r(E)=3$.

Le rang analytique r_{an} est calculé avec la série L de Dirichlet de E :

$$L(E,s)=\left(1+5077^{-s}\right)^{-1}\prod_{P\neq 5077}\left(1-a_p p^{-s}+p^{1-2s}\right)^{-1}=\sum_{n\geq 1}a_n n^{-s}$$

La formule $A=\lim_{s\to 1}\dfrac{L(E,s)}{(s-1)^3}$ prend la valeur $A=1,731...$

Il en résulte l'égalité des rangs $r(E)=r_{an}=3$.

(3) « Algorithme de GEBEL – PETHO on Mordell's equation », Compos. Math 110 (1998) pages 335-367.

Les auteurs ont étudié la courbe elliptique *E* d'équation de Weierstrass :

$$E : y^2 = x^3 + k \in \mathbb{Z}[x, y]$$

Pour $k = -2^6 \times 3^3 \times 38593$, le groupe de torsion $T(E)$ est trivial.
Ils ont utilisé la conjecture de Birch et Swinnerton-Dyer pour évaluer le rang $r(E)$ de *E*.

Proposition. $r(E) = \min\{r_{an}\ ,\ L(E,1) = 0\}$

□
Dans ce cas, ils ont montré que l'équation fonctionnelle de la série de Dirichlet $L(E,s)$ a un signe égal à +1.

(4) *COATES and A.WILES* : « On the conjecture of Birch and Swinnerton-Dyer » Inv. Math. 39 (1977) pages 223-251.

Les deux auteurs ont montré pour une courbe elliptique *E* sur le corps des rationnels ou un corps quadratique imaginaire admettant une multiplication complexe par l'anneau des entiers de ce corps, que si $r(E) \geq 1$, alors la série $L(E,s)$ de la courbe *E* s'annule en $s = 1$.
En particulier ce résultat est appliqué à la famille de courbes elliptiques d'équation

$$y^2 = x^3 - Dx \in \mathbb{Q}[x, y]$$

Ces courbes admettent une multiplication complexe par l'anneau des entiers de Gauss.
Par exemple, pour $D = 17$:
La courbe obtenue est de rang $r = 2$ et sa série $L(E,s)$ s'annule en $s = 1$.

(5) *R. GREENBERG* : « On the conjecture of Birch and Swinnerton-Dyer » Inv. Math. 72 (1983) pages 241-265.

L'auteur a cité un résultat reliant la série $L(E,s)$ d'une courbe elliptique *E*, son rang r et son groupe de Tate-Shafarevitch $Ш(E)$.

Théorème. *Soit E une courbe elliptique sur le corps* $\mathbb{Q}$ *admettant une multiplication complexe par l'anneau des entiers d'un corps quadratique imaginaire K.*
Si la série $L(E,s)$ *de la courbe elliptique E possède en* $s = 1$ *un zéro d'ordre impair, alors :*

Ou bien le groupe $E(\mathbb{Q})$ *est de rang* $r \geq 1$ *ou bien la composante p-primaire du groupe de Tate-Shafarevitch est infinie pour tout nombre premier p de bonne réduction (excepté pour 2 et 3).*
□

(6) *K. RUBIN* : « elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer » Inv. Math. 64 (1981) pages 455-470.

Cet auteur a montré un résultat plus général que celui prouvé par Coates et Wiles concernant les courbes elliptiques qui admettent une multiplication complexe par les entiers d'un corps *K* quadratique imaginaire.

Théorème. *Si le groupe de Mordell-Weil* $E(F)$ *d'une courbe elliptique E sur un corps de nombre F qui admet une multiplication complexe par les entiers d'un corps quadratique imaginaire* $K \subset \mathbb{C}$ *est infini, alors :*

$$\zeta(E/F, s) \text{ s'annule en } s = 1$$

Pour $F = K$ c'est le résultat montré par Coates et Wiles.

(7) J.E. CREMONA : « Algorithm for modular elliptique curves » _ 2 nd edition. Cambridge-University press (1997).

Dans cet ouvrage de 376 pages, l'auteur a commencé par décrire un algorithme basé sur les symboles modulaires pour obtenir des courbes elliptiques modulaires. Ensuite il a déterminé des algorithmes pour décrire l'arithmétique de ces courbes et leurs courbes isogènes. Il a enfin rassemblé les résultats obtenus avec plusieurs logiciels (Magma, Maple, PARI, SIMATH, UBASIC, GP,…) dans 4 tables.
La table 4 contient les données relatives à la conjecture de Birch et Swinnerton-Dyer pour chaque courbe de Weil de la table1 précédente.
Il a utilisé la formule :

$$S = \frac{L^r(f,1)}{r!\Omega(f)} \Big/ \frac{\left(\prod c_p\right) R}{|T|^2}$$

Où r est le rang, $L^r(f,1)$ le développement de Fourier de la série L de Dirichlet de la courbe *E*, $f(z)$ est une « newform » pour $\Gamma_0(N)$, $\Omega(f)$ est la période réelle du réseau attaché à *E*, $R =$ le régulateur de *E*, $T =$ sous groupe de torsion de *E*.

Quelques données extraites de cette table

r	Ω	$L^r(1)/r!$	R	$L^{(r)}(1)/r!\Omega \cdot R$	S
0	1,2692…	0,2538…	1	1/5	1
1	5,9869…	0,3059…	0,0511	1,0000	1
0	3,3387…	1,1129…	1	1/3	1
1	3,1997…	0,6273…	0,0980…	2	1
0	0,2649…	2,1199…	1	8	1

Chaque ligne de données est associée à une courbe elliptique modulaire du tableau 1.

4-Applications :

Nous terminons cette étude par le calcul de la série $L(E,s=1)$ de Dirichlet des courbes elliptiques $E_i/\mathbb{Q}$ d'équations de Weierstrass :

$$E_1 : y^2 - 48y = x^3 - 8x - 8 \in \mathbb{Q}[x,y] \ ,$$
$$E_2 : y^2 + 11y = x^3 + 18x^2 + 41x \in \mathbb{Q}[x,y] \text{ et}$$
$$E_3 : y^2 + y = x^3 - 79x + 342 \in \mathbb{Q}[x,y]$$

Formule de la série $L(E,s)$ de Dirichlet d'une courbe elliptique E :

$$L(E,s) = \prod_p \left(1 - t_p \cdot p^{-s}\right)^{-1} \prod_q \left(1 - t_q q^{-s} + q^{1-2s}\right)^{-1}$$

où p : diviseur premier du discriminant $\triangle(E)$

q : nombre premier qui ne divise pas le discriminant $\triangle(E)$

4.1 Courbe E_1 :

Calcul du discriminant :

$$\triangle(E_1) = -139340800 = -2^{10} \times 5^2 \times 5443$$

Calcul des facteurs $\left(1 - t_p \cdot p^{-s}\right)^{-1}$ pour p divisant le discriminant :

$p = 2$; $t_2 = 0$; $\left(1 - t_2 \cdot 2^{-1}\right)^{-1} = 1$

$p = 5$; $t_5 = -1$; $\left(1 - t_5 \cdot 5^{-1}\right)^{-1} = 0.8333333$

$p = 5443$; $t_{5443} = -1$; $\left(1 - t_{5443} \cdot 5443^{-1}\right)^{-1} = 0.9998163$

Calcul des facteurs $\left(1 - t_q q^{-s} + q^{1-2s}\right)^{-1}$ pour les nombres premiers $q \leq 281$ et ne divisant pas le discriminant de la courbe elliptique E_1 :

Valeur de q	Nombre de solutions modulo q	Valeur de t_q	$\left(1 - t_q q^{-1} + q^{-1}\right)^{-1}$
3	4	0	0.7500000
7	12	-4	0.5833333
11	10	2	1.1000000
13	17	-3	0.7647059
17	18	0	0.9444444
19	28	-8	0.6785714
23	32	-8	0.7187500
29	35	-5	0.8285714
31	38	-6	0.8157884
37	31	7	1.1935480

41	31	11	1.3225810
43	52	-8	0.8269231
47	51	-3	0.9215686
53	59	-5	0.8983051
59	50	10	1.1800000
61	72	-10	0.8472222
67	72	-4	0.9305556
71	72	0	0.9861111
73	69	5	1.0579710
79	87	-7	0.9080459
83	84	0	0.9880952
89	96	-6	0.9270833
97	96	2	1.0104170
101	96	6	1.0520830
103	101	3	1.0198020
107	111	-3	0.9639640
109	125	-15	0.8720000
113	114	0	0.9912280
127	136	-8	0.9338235
131	119	13	1.1008400
137	123	15	1.1138210
139	127	13	1.0944880
149	154	-4	0.9675325
151	141	11	1.0709220
157	159	-1	0.9874214
163	166	-2	0.9819277
167	182	-14	0.9175824
173	180	-6	0.9611111
179	176	4	1.0170450
181	167	15	1.0838320
191	173	19	1.1040460
193	182	12	1.0604400
197	190	8	1.0368420
199	220	-20	0.9045454
211	207	5	1.0193240
223	247	-3	0.9028340
227	218	10	1.0412840
229	240	-10	0.9541667
233	214	20	1.0887850
239	239	1	1.0000000
241	260	-18	0.9269231
251	265	-13	0.9471698
257	285	-27	0.9017554
263	264	0	0.9962121
269	270	0	0.9962963
271	271	1	1.0000000
277	270	8	1.0259260
281	294	-12	0.9557823

Calcul de la valeur du produit des N premiers facteurs de la série $L(E_1, s=1)$ pour $N = 100, 200, ..., 2000$:

N	Produit des N premiers facteurs de $L(E_1, s=1)$
200	0.94163104866E-01
300	0.73705049394E-01
400	0.58528266479E-01
500	0.39583906975E-01
600	0.42974437832E-01
700	0.43799817834E-01
800	0.42725467760E-01
900	0.35836974154E-01
1000	0.35556224806E-01
1100	0.34067563088E-01
1200	0.31206499676E-01
1300	0.28226258520E-01
1400	0.26425916012E-01
1500	0.25259756212E-01
1600	0.26668610192E-01
1700	0.27976957136E-01
1800	0.27891529453E-01
1900	0.28634881094E-01
2000	0.29706753289E-01

Ces valeurs de $L(E_1, s=1)$ ne nous permettent pas de conclure la limite de cette série.
Pour une valeur plus précise de la limite de la série $L(E_1, s=1)$ il faut utiliser un ordinateur puissant et augmenter la valeur de *N*.

4.2 Courbe E_2 :

Calcul du discriminant :

$$\triangle(E_2) = -8682587$$

Calcul de la valeur de $L(E_2, 1)$ pour *N* = 100, 200, …, 1500

Listing des résultats :

```
I=     1 P =     2 NBR SOL=     5 TP=    -2 XLLL=.40000000000E+00
I=     2 P =     3 NBR SOL=     7 TP=    -3 XLLL=.42857142857E+00
I=     3 P =     5 NBR SOL=    10 TP=    -4 XLLL=.50000000000E+00
I=     4 P =     7 NBR SOL=    12 TP=    -4 XLLL=.58333333333E+00
I=     5 P =    11 NBR SOL=    14 TP=    -2 XLLL=.78571428571E+00
I=     6 P =    13 NBR SOL=    20 TP=    -6 XLLL=.65000000000E+00
I=     7 P =    17 NBR SOL=    25 TP=    -7 XLLL=.68000000000E+00
I=     8 P =    19 NBR SOL=    24 TP=    -4 XLLL=.79166666667E+00
I=     9 P =    23 NBR SOL=    32 TP=    -8 XLLL=.71875000000E+00
I=    10 P =    29 NBR SOL=    35 TP=    -5 XLLL=.82857142857E+00
```

```
I=    11 P =    31 NBR SOL=    40 TP=    -8 XLLL=.77500000000E+00
I=    12 P =    37 NBR SOL=    40 TP=    -2 XLLL=.92500000000E+00
I=    13 P =    41 NBR SOL=    50 TP=    -8 XLLL=.82000000000E+00
I=    14 P =    43 NBR SOL=    45 TP=    -1 XLLL=.95555555556E+00
I=    15 P =    47 NBR SOL=    50 TP=    -2 XLLL=.94000000000E+00
I=    16 P =    53 NBR SOL=    59 TP=    -5 XLLL=.89830508475E+00
I=    17 P =    59 NBR SOL=    67 TP=    -7 XLLL=.88059701493E+00
I=    18 P =    61 NBR SOL=    61 TP=     1 XLLL=.10000000000E+01
I=    19 P =    67 NBR SOL=    79 TP=   -11 XLLL=.84810126582E+00
I=    20 P =    71 NBR SOL=    75 TP=    -3 XLLL=.94666666667E+00
I=    21 P =    73 NBR SOL=    71 TP=     3 XLLL=.10281690141E+01
I=    22 P =    79 NBR SOL=    87 TP=    -7 XLLL=.90804597701E+00
I=    23 P =    83 NBR SOL=    81 TP=     3 XLLL=.10246913580E+01
I=    24 P =    89 NBR SOL=   101 TP=   -11 XLLL=.88118811881E+00
I=    25 P =    97 NBR SOL=    91 TP=     7 XLLL=.10659340659E+01
I=    26 P =   101 NBR SOL=   113 TP=   -11 XLLL=.89380530973E+00
I=    27 P =   103 NBR SOL=   104 TP=     0 XLLL=.99038461538E+00
I=    28 P =   107 NBR SOL=   110 TP=    -2 XLLL=.97272727273E+00
I=    29 P =   109 NBR SOL=   104 TP=     6 XLLL=.10480769231E+01
I=    30 P =   113 NBR SOL=   116 TP=    -2 XLLL=.97413793103E+00
I=    31 P =   127 NBR SOL=   131 TP=    -3 XLLL=.96946564885E+00
I=    32 P =   131 NBR SOL=   153 TP=   -21 XLLL=.85620915033E+00
I=    33 P =   137 NBR SOL=   150 TP=   -12 XLLL=.91333333333E+00
I=    34 P =   139 NBR SOL=   160 TP=   -20 XLLL=.86875000000E+00
I=    35 P =   149 NBR SOL=   144 TP=     6 XLLL=.10347222222E+01
I=    36 P =   151 NBR SOL=   167 TP=   -15 XLLL=.90419161677E+00
I=    37 P =   157 NBR SOL=   178 TP=   -20 XLLL=.88202247191E+00
I=    38 P =   163 NBR SOL=   175 TP=   -11 XLLL=.93142857143E+00
I=    39 P =   167 NBR SOL=   150 TP=    18 XLLL=.11133333333E+01
I=    40 P =   173 NBR SOL=   148 TP=    26 XLLL=.11689189189E+01
I=    41 P =   179 NBR SOL=   172 TP=     8 XLLL=.10406976744E+01
I=    42 P =   181 NBR SOL=   198 TP=   -16 XLLL=.91414141414E+00
I=    43 P =   191 NBR SOL=   216 TP=   -24 XLLL=.88425925926E+00
I=    44 P =   193 NBR SOL=   192 TP=     2 XLLL=.10052083333E+01
I=    45 P =   197 NBR SOL=   220 TP=   -22 XLLL=.89545454545E+00
I=    46 P =   199 NBR SOL=   210 TP=   -10 XLLL=.94761904762E+00
I=    47 P =   211 NBR SOL=   225 TP=   -13 XLLL=.93777777778E+00
I=    48 P =   223 NBR SOL=   248 TP=   -24 XLLL=.89919354839E+00
I=    49 P =   227 NBR SOL=   240 TP=   -12 XLLL=.94583333333E+00
I=    50 P =   229 NBR SOL=   224 TP=     6 XLLL=.10223214286E+01
I=    51 P =   233 NBR SOL=   256 TP=   -22 XLLL=.91015625000E+00
I=    52 P =   239 NBR SOL=   249 TP=    -9 XLLL=.95983935743E+00
I=    53 P =   241 NBR SOL=   240 TP=     2 XLLL=.10041666667E+01
I=    54 P =   251 NBR SOL=   230 TP=    22 XLLL=.10913043478E+01
I=    55 P =   257 NBR SOL=   267 TP=    -9 XLLL=.96254681648E+00
I=    56 P =   263 NBR SOL=   265 TP=    -1 XLLL=.99245283019E+00
I=    57 P =   269 NBR SOL=   284 TP=   -14 XLLL=.94718309859E+00
I=    58 P =   271 NBR SOL=   250 TP=    22 XLLL=.10840000000E+01
I=    59 P =   277 NBR SOL=   303 TP=   -25 XLLL=.91419141914E+00
I=    60 P =   281 NBR SOL=   286 TP=    -4 XLLL=.98251748252E+00
I=    61 P =   283 NBR SOL=   300 TP=   -16 XLLL=.94333333333E+00
I=    62 P =   293 NBR SOL=   304 TP=   -10 XLLL=.96381578947E+00
I=    63 P =   307 NBR SOL=   335 TP=   -27 XLLL=.91641791045E+00
I=    64 P =   311 NBR SOL=   318 TP=    -6 XLLL=.97798742138E+00
I=    65 P =   313 NBR SOL=   345 TP=   -31 XLLL=.90724637681E+00
I=    66 P =   317 NBR SOL=   288 TP=    30 XLLL=.11006944444E+01
I=    67 P =   331 NBR SOL=   330 TP=     2 XLLL=.10030303030E+01
I=    68 P =   337 NBR SOL=   318 TP=    20 XLLL=.10597484277E+01
I=    69 P =   347 NBR SOL=   342 TP=     6 XLLL=.10146198830E+01
I=    70 P =   349 NBR SOL=   348 TP=     2 XLLL=.10028735632E+01
I=    71 P =   353 NBR SOL=   340 TP=    14 XLLL=.10382352941E+01
```

```
I=    72 P =   359 NBR SOL=   380 TP=   -20 XLLL=.94473684211E+00
I=    73 P =   367 NBR SOL=   382 TP=   -14 XLLL=.96073298429E+00
I=    74 P =   373 NBR SOL=   388 TP=   -14 XLLL=.96134020619E+00
I=    75 P =   379 NBR SOL=   402 TP=   -22 XLLL=.94278606965E+00
I=    76 P =   383 NBR SOL=   386 TP=    -2 XLLL=.99222797927E+00
I=    77 P =   389 NBR SOL=   397 TP=    -7 XLLL=.97984886650E+00
I=    78 P =   397 NBR SOL=   390 TP=     8 XLLL=.10179487179E+01
I=    79 P =   401 NBR SOL=   412 TP=   -10 XLLL=.97330097087E+00
I=    80 P =   409 NBR SOL=   445 TP=   -35 XLLL=.91910112360E+00
I=    81 P =   419 NBR SOL=   429 TP=    -9 XLLL=.97668997669E+00
I=    82 P =   421 NBR SOL=   393 TP=    29 XLLL=.10712468193E+01
I=    83 P =   431 NBR SOL=   450 TP=   -18 XLLL=.95777777778E+00
I=    84 P =   433 NBR SOL=   420 TP=    14 XLLL=.10309523810E+01
I=    85 P =   439 NBR SOL=   415 TP=    25 XLLL=.10578313253E+01
I=    86 P =   443 NBR SOL=   466 TP=   -22 XLLL=.95064377682E+00
I=    87 P =   449 NBR SOL=   471 TP=   -21 XLLL=.95329087049E+00
I=    88 P =   457 NBR SOL=   448 TP=    10 XLLL=.10200892857E+01
I=    89 P =   461 NBR SOL=   461 TP=     1 XLLL=.10000000000E+01
I=    90 P =   463 NBR SOL=   494 TP=   -30 XLLL=.93724696356E+00
I=    91 P =   467 NBR SOL=   475 TP=    -7 XLLL=.98315789474E+00
I=    92 P =   479 NBR SOL=   468 TP=    12 XLLL=.10235042735E+01
I=    93 P =   487 NBR SOL=   517 TP=   -29 XLLL=.94197292070E+00
I=    94 P =   491 NBR SOL=   525 TP=   -33 XLLL=.93523809524E+00
I=    95 P =   499 NBR SOL=   493 TP=     7 XLLL=.10121703854E+01
I=    96 P =   503 NBR SOL=   515 TP=   -11 XLLL=.97669902913E+00
I=    97 P =   509 NBR SOL=   500 TP=    10 XLLL=.10180000000E+01
I=    98 P =   521 NBR SOL=   528 TP=    -6 XLLL=.98674242424E+00
I=    99 P =   523 NBR SOL=   563 TP=   -39 XLLL=.92895204263E+00
I=   100 P =   541 L(E,1) =.35289181386E-03
I=   200 P =  1223 L(E,1) =.21719451665E-03
I=   300 P =  1987 L(E,1) =.25379180541E-03
I=   400 P =  2741 L(E,1) =.14346628242E-03
I=   500 P =  3571 L(E,1) =.13363103059E-03
I=   600 P =  4409 L(E,1) =.14241873768E-03
I=   700 P =  5279 L(E,1) =.14103105620E-03
I=   800 P =  6133 L(E,1) =.15612517034E-03
I=   900 P =  6997 L(E,1) =.16767616650E-03
I=  1000 P =  7919 L(E,1) =.16088801169E-03
I=  1100 P =  8831 L(E,1) =.12923290358E-03
I=  1200 P =  9733 L(E,1) =.12441276455E-03
I=  1300 P = 10657 L(E,1) =.11313660623E-03
I=  1400 P = 11657 L(E,1) =.10875868066E-03
I=  1500 P = 12553 L(E,1) =.10372858578E-03
```

En prenant le produit de 1500 facteurs de la série de Dirichlet $L(E_2,1)$ de la courbe E_2, on a $L(E_2,1)=0$ aux 3 premières décimales. Ceci suggère fortement que cette série peut avoir un zéro en $s=1$ d'ordre 1 ou plus et que cette courbe est de rang $r>0$.

4.3 Courbe E_3 :

Courbe elliptique d'équation de Weierstrass :

$$E_3 : y^2 + y = x^3 - 79x + 342 \in \mathbb{Q}[x, y]$$

Calcul du discriminant :

$$\triangle(E_3) = -19047851$$

Calcul de la valeur de la série de Dirichlet $L(E_3,1)$ pour N = 100, 200, …, 1500

Listing des résultats :

```
I=    78 P =   397 NBR SOL=   411 TP=   -13 XLLL=.96593673966E+00
I=    79 P =   401 NBR SOL=   433 TP=   -31 XLLL=.92609699769E+00
I=    80 P =   409 NBR SOL=   384 TP=    26 XLLL=.10651041667E+01
I=    81 P =   419 NBR SOL=   450 TP=   -30 XLLL=.93111111111E+00
I=    82 P =   421 NBR SOL=   440 TP=   -18 XLLL=.95681818182E+00
I=    83 P =   431 NBR SOL=   417 TP=    15 XLLL=.10335731415E+01
I=    84 P =   433 NBR SOL=   432 TP=     2 XLLL=.10023148148E+01
I=    85 P =   439 NBR SOL=   426 TP=    14 XLLL=.10305164319E+01
I=    86 P =   443 NBR SOL=   432 TP=    12 XLLL=.10254629630E+01
I=    87 P =   449 NBR SOL=   440 TP=    10 XLLL=.10204545455E+01
I=    88 P =   457 NBR SOL=   446 TP=    12 XLLL=.10246636771E+01
I=    89 P =   461 NBR SOL=   422 TP=    40 XLLL=.10924170616E+01
I=    90 P =   463 NBR SOL=   456 TP=     8 XLLL=.10153508772E+01
I=    91 P =   467 NBR SOL=   491 TP=   -23 XLLL=.95112016293E+00
I=    92 P =   479 NBR SOL=   480 TP=     0 XLLL=.99791666667E+00
I=    93 P =   487 NBR SOL=   496 TP=    -8 XLLL=.98185483871E+00
I=    94 P =   491 NBR SOL=   487 TP=     5 XLLL=.10082135524E+01
I=    95 P =   499 NBR SOL=   511 TP=   -11 XLLL=.97651663405E+00
I=    96 P =   503 NBR SOL=   487 TP=    17 XLLL=.10328542094E+01
I=    97 P =   509 NBR SOL=   536 TP=   -26 XLLL=.94962686567E+00
I=    98 P =   521 NBR SOL=   492 TP=    30 XLLL=.10589430894E+01
I=    99 P =   523 NBR SOL=   560 TP=   -36 XLLL=.93392857143E+00
I=   100 P =   541 L(E,1) =.15718507253E-03
I=   200 P =  1223 L(E,1) =.69545251974E-04
I=   300 P =  1987 L(E,1) =.52407273009E-04
I=   400 P =  2741 L(E,1) =.44431135300E-04
I=   500 P =  3571 L(E,1) =.36878507081E-04
I=   600 P =  4409 L(E,1) =.39248325341E-04
I=   700 P =  5279 L(E,1) =.32073920173E-04
I=   800 P =  6133 L(E,1) =.27541900106E-04
I=   900 P =  6997 L(E,1) =.22655368285E-04
I=  1000 P =  7919 L(E,1) =.23840979680E-04
I=  1100 P =  8831 L(E,1) =.21846519042E-04
I=  1200 P =  9733 L(E,1) =.22130853760E-04
I=  1300 P = 10657 L(E,1) =.19951911125E-04
I=  1400 P = 11657 L(E,1) =.19680390553E-04
I=  1500 P = 12553 L(E,1) =.17321931987E-04
```

Le produit de 1500 facteurs de la série $L(E_3,1)$ de Dirichlet de la courbe E_3 est égal à zéro aux 4 premieres décimales ; ceci implique fortement que la série $L(E_3, s=1)$ tend vers 0 lorsque le nombre des facteurs *N* augmente. De ce faîte le zéro de cette série en $s=1$ est d'ordre $r \geq 1$.

Pour une valeur plus précise de r, il faut calculer les dérivées $\frac{dL}{ds}, \frac{d^2L}{ds^2}, etc \ldots$

Ces calculs ont été réalisés par un programme que j'ai écrit avec le langage FORTRAN :

Programme de calcul :

```
            PROGRAM SERIEL
!           CALL DECOMP
!           CALL DELTA
!           CALL NBRPREM
            CALL SOLUTIO
            STOP
            END
!-------------------------------------------------------------
            SUBROUTINE DECOMP
!           FACTEURS PREMIERS D'UN NOMBRE
            DIMENSION NPREM(5000)
            PRINT *,'NOMBRE A DECOMPOSER : '
            READ *,NBR
            OPEN (7,FILE='C:\FICHIER.ENT',STATUS='OLD')
            READ (7,100) (NPREM(I),I=1,5000)
      100 FORMAT (20I6)
            CLOSE (7)
            DO 20 K=1,5000
            IQUOT=NBR/NPREM(K)
            IREST=NBR-IQUOT*NPREM(K)
            IF (IREST.EQ.0) THEN
            PRINT *,NPREM(K)
            ENDIF
       20 CONTINUE
            RETURN
            END
!-------------------------------------------------------------
            SUBROUTINE NBRPREM
            DIMENSION NPREM(5000)
!           CALCUL DES 5000 PREMIERS NOMBRES PREMIERS
            NPREM(1)=2
            NPREM(2)=3
            PRINT *,'NOMBRE DE NBR PREMIERS VOULUS : < ou = 5000'
            READ *,NBR
            OPEN (7,FILE='C:\FICHIER.ENT',STATUS='NEW')
            DO 20 L=3,NBR
            I=L-1
            J=NPREM(I)+1
        15 KK=0
            DO 30 K=1,I
            NVAL=J/NPREM(K)
            NREST=NVAL*NPREM(K)
            IF (NREST.EQ.J) KK=KK+1
       30 CONTINUE
            IF (KK.EQ.0) GOTO 50
            J=J+1
            GOTO 15
```

```
 50 NPREM(L)=J
     IF (I.EQ.NBR) GOTO 60
     J=J+1
 20 CONTINUE
100 FORMAT(20I6)
 60 PRINT *,'FIN'
    PRINT *,(NPREM(II),II=1,NBR)
    WRITE (7,100) (NPREM(II),II=1,NBR)
    CLOSE (7)
    RETURN
    END
!---------------------------------------------------------------
    SUBROUTINE DELTA
!   REM CALCUL DE DESCRIMINANT
    INTEGER A1,A2,A3,A4,A6
    INTEGER*4 B2,B4,B6,B8
    INTEGER*4 DESCRI
    PRINT *,'DONNER LA VALEUR DE A1'
    READ *,A1
    PRINT *,'DONNER LA VALEUR DE A3'
    READ *,A3
    PRINT *,'DONNER LA VALEUR DE A2'
    READ *,A2
    PRINT *,'DONNER LA VALEUR DE A4'
    READ *,A4
    PRINT *,'DONNER LA VALEUR DE A6'
    READ *,A6
    B2=A1*A1+4*A2
    B4=2*A4+A1*A3
    B6=A3*A3+4*A6
    B8=B2*B6-B4*B4
    DESCRI=-B2*B2*B8-8*B4*B4*B4-27*B6*B6+9*B2*B4*B6
    PRINT *,'DESCRIMINANT = ',DESCRI
    RETURN
    END
!---------------------------------------------------------------
    SUBROUTINE SOLUTIO
    DIMENSION NPREM(5000)
!   CALCUL DU NOMBRE DE SOLUTIONS MODULO P
    INTEGER*4 NVAL,NQUOT,NREST,I,NBR
    INTEGER*4 NNX2,NNXQUOT,NNXREST,NNX3
    INTEGER*4 NNY2,NNYQUOT,NNYREST
    REAL*8 XLL,XLLL,XPR,XITP
    PRINT *,'ENTRER LE NOMBRE DE NBR PREM A TRAITER :'
    READ *,NBR
    OPEN (7,FILE='C:\FICHIER.ENT',STATUS='OLD')
    READ (7,100) (NPREM(I),I=1,NBR)
    CLOSE (7)
100 FORMAT (20I6)
    OPEN (8,FILE='C:\FICHIER.RES')
```

```
          I=0
          XLL=1.
       10 I=I+1
          JPR=NPREM(I)
          NSOL=1
          JMAX=JPR-1
          DO 20 NX=0,JMAX
          NNX2=NX*NX
          NNXQUOT=NNX2/JPR
          NNXREST=NNXQUOT*JPR
          NNX2=NNX2-NNXREST
          NNX3=NNX2*NX
          NNXQUOT=NNX3/JPR
          NNXREST=NNXQUOT*JPR
          NNX3=NNX3-NNXREST
          DO 30 NY=0,JMAX
          NNY2=NY*NY
          NNYQUOT=NNY2/JPR
          NNYREST=NNYQUOT*JPR
          NNY2=NNY2-NNYREST
!---------------------------------------------
!          NVAL=NNY2-48*NY-NNX3+8*NX+8
!---------------------------------------------
!          NVAL=NNY2+8*NX*NY+11*NY-NNX3-2*NNX2+3*NX
!          NVAL=NNY2+11*NY-NNX3-18*NNX2-41*NX
!---------------------------------------------
!          NVAL=NNY2-4*NX*NY+13*NY-NNX3+NX
!---------------------------------------------
!          NVAL=NNY2+40*NX*NY+4*NY-NNX3-15*NNX2+6*NX+4
!---------------------------------------------
!          NVAL=NNY2+4*NX*NY+4*NY-NNX3-15*NNX2+6*NX+4
!---------------------------------------------
!          NVAL=NNY2+NY-NNX3+7*NX-6
!---------------------------------------------
!          NVAL=NNY2-NNX3+NX
!---------------------------------------------
!          NVAL=NNY2-NNX3+25*NX
!---------------------------------------------
          NVAL=NNY2+NY-NNX3+79*NX-342
!---------------------------------------------
          NQUOT=NVAL/JPR
          NREST=NQUOT*JPR
          IF (NVAL.EQ.NREST) THEN
          NSOL=NSOL+1
          ENDIF
       30 CONTINUE
       20 CONTINUE
          ITP=1+JPR-NSOL
          XPR=JPR
          XITP=ITP
```

```
!---------------------------------
!
!Courbe : y2-48y=x3-8x-8
!
!            IF (JPR.EQ.2)      GOTO 50
!            IF (JPR.EQ.5)      GOTO 50
!            IF (JPR.EQ.5443)   GOTO 50
!---------------------------------
!
! Courbe : y2+8xy+11y=x3+2x2-3x
!            y2+11y=x3+18x2+41x
!
!           IF (JPR.EQ.8682567) GOTO 50
!
!---------------------------------
!Courbe : y2-4xy+13y=x3-x
!
!            IF (JPR.EQ.17)     GOTO 50
!            IF (JPR.EQ.59)     GOTO 50
!            IF (JPR.EQ.769)    GOTO 50
!
!---------------------------------
!
! Courbe : y2+40xy+4y=x3+15x2-6x-4
!
!            IF (JPR.EQ.2)      GOTO 50
!            IF (JPR.EQ.3)      GOTO 50
!            IF (JPR.EQ.5)      GOTO 50
!            IF (JPR.EQ.7)      GOTO 50
!            IF (JPR.EQ.7559)   GOTO 50
!
!
!---------------------------------
!
! Courbe : y2+4xy+4y=x3+15x2-6x-4
!
!            IF (JPR.EQ.2)      GOTO 50
!            IF (JPR.EQ.359)    GOTO 50
!
!---------------------------------
!
!Courbe : y2+y=x3-7x+6
!
!            IF (JPR.EQ.5077)   GOTO 50
!---------------------------------
!
!Courbe : y2=x3-x
!
!            IF (JPR.EQ.2)      GOTO 50
!---------------------------------
```

```
!
!
!Courbe : y2=x3+25x
!
!            IF (JPR.EQ.2)      GOTO 50
!            IF (JPR.EQ.5)      GOTO 50
!----------------------------------
!
!Courbe : y2+y=x3-79x+342
!
           IF (JPR.EQ.19047851)      GOTO 50
!----------------------------------
            XLLL=1./(1.-XITP/XPR+1./XPR)
            XLL=XLL*XLLL
            IF (I.EQ.NBR)  GOTO 80
            IF (I.LT.100)  GOTO 60
            IF (I.EQ.100)  GOTO 70
            IF (I.EQ.200)  GOTO 70
            IF (I.EQ.300)  GOTO 70
            IF (I.EQ.400)  GOTO 70
            IF (I.EQ.500)  GOTO 70
            IF (I.EQ.600)  GOTO 70
            IF (I.EQ.700)  GOTO 70
            IF (I.EQ.800)  GOTO 70
            IF (I.EQ.900)  GOTO 70
            IF (I.EQ.1000) GOTO 70
            IF (I.EQ.1100) GOTO 70
            IF (I.EQ.1200) GOTO 70
            IF (I.EQ.1300) GOTO 70
            IF (I.EQ.1400) GOTO 70
            IF (I.EQ.1500) GOTO 70
            IF (I.EQ.1600) GOTO 70
            IF (I.EQ.1700) GOTO 70
            IF (I.EQ.1800) GOTO 70
            IF (I.EQ.1900) GOTO 70
            IF (I.EQ.2000) GOTO 70
            IF (I.EQ.2100) GOTO 70
            IF (I.EQ.2200) GOTO 70
            IF (I.EQ.2300) GOTO 70
            IF (I.EQ.2400) GOTO 70
            IF (I.EQ.2500) GOTO 70
            IF (I.EQ.2600) GOTO 70
            IF (I.EQ.2700) GOTO 70
            IF (I.EQ.2800) GOTO 70
            IF (I.EQ.2900) GOTO 70
            IF (I.EQ.3000) GOTO 70
            IF (I.EQ.3100) GOTO 70
            IF (I.EQ.3200) GOTO 70
            IF (I.EQ.3300) GOTO 70
            IF (I.EQ.3400) GOTO 70
```

```
            IF (I.EQ.3500) GOTO 70
            GOTO 10
         50 XLLL=1./(1.-XITP/XPR)
            XLL=XLL*XLLL
           PRINT *,'I =',I,' P =',JPR,' NBR SOL =',NSOL,' TP = ',ITP
           IF (I.EQ.NBR) GOTO 80
           GOTO 10
!
         60 WRITE (8,200) I,JPR,NSOL,ITP,XLLL
        200 FORMAT ('I=',I6,' P =',I6,' NBR SOL=',I6,' TP=',I6,' XLLL=',E16.11)
            GOTO 10
!
         70 PRINT *,'JE SUIS AU FACTEUR NUMERO ',I
            WRITE (8,300) I,JPR,XLL
        300 FORMAT ('I=',I6,' P =',I6,' L(E,1) =',E16.11)
            GOTO 10
         80 PRINT *,'JE SUIS A LA FIN'
            WRITE (8,300) I,JPR,XLL
            CLOSE (8)
            RETURN
            END
```

Ce programme comporte 4 « subroutines » :

1. Subroutine DECOMP : c'est un programme qui calcule les diviseurs premiers d'un nombre donné.

2. Subroutine DELTA : c'est un programme de calcul du discriminant d'une courbe elliptique donnée par la forme de Weierstrass $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in \mathbb{Z}[x, y]$.

3. Subroutine NBRPREM : c'est un programme qui calcule et exhibe un nombre donné de nombres premiers.

4. Subroutine SOLUTIO : c'est un programme qui calcule les solutions d'une courbe elliptique E modulo un nombre premier p, le facteur de la série $L(E,s)$ relatif à ce nombre premier et la valeur du produit des N premiers facteurs de cette série.

Bibliographie :

[1] E. ARTIN : « *Algebraic Numbers and Algebraic Functions* ».
Gordon and Breach New York – London – Paris (1951).

[2] B. BIRCH, H. P. F. SWINNERTON-DYER :
1) « *Notes on elliptic curves* I ».
J. Reine Angew. Math. 212 (1963), 7-25.
2) « *Notes on elliptic curves* II ».
J. Reine Angew. Math. 218 (1965), 79-108.

[3] J.W.S. CASSELS : « *Diophantine equations with special reference to elliptic curves* ».
J. London Math Soc. (1966) 193-291.

[4] HARVEY COHN : « *A classical invitation to algebraic numbers and class fields* ».
Springer Verlag Berlin – New York (1978).

[5] R. HARTSHORNE : « *Algebraic Geometry* ».
Graduate Texts in Mathematics 52. Springer-Verlag 1977.

[6] H. HASSE : « *Number Theory* ».
Springer Verlag Berlin – New York (1980).

[7] S. IYANAGA : « *The theory of Numbers* ».
North-Holland Publishing Company - Amsterdam
American Elsevier Publishing Company – New York (1969).

[8] N. KOBLITZ : « *Introduction to elliptic curves and modular forms* ».
Graduate Texts in Mathematics 97 Springer-Verlag 1984.

[9] S. LANG :
1) « *Algebra* ».
Addison-Wesley 1965
2) « *Algebraic Numbers* ».
Addison-Wesley Publishing Company, New York – London – Paris (1963).
3) « *Elliptic curves : Diophantine analysis* »
Springer-Verlag Berlin New York (1978)

[10] B. MAZUR : « *Rational isogenies of prime degre* ».
Invent. Math. 44 (1978), pages 129-162.

[11] T. NAGELL :
« *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre* » Wid. Akad. Skrifter Oslo. (1935), Nr. 1.

[12] A. OGG : « *Modular forms and Dirichlet series* ».
Benjamin New York (1967).

[13] D. ROHRLICH : « *On L-Function of Elliptic curves and anti-cyclotomic towers* ».
Invent. Math. 75 (1984) 383-408.

[14] G. SHIMURA : « *Introduction to the arithmetic theory of automorphic functions* ».
Princeton University Press (1971).

[15] J.H. SILVERMAN : « *The arithmetic of elliptic curves* ».
Graduate Texts in Mathematics 106, Springer-Verlag, New York (1986).

[16] A WEIL : « *Dirichlet Series and Automorphic Forms* ».
Lecture Notes in Mathematic 189, Springer-Verlag, (1971).

[17] E. WEISS « *Algebraic Number Theory* ».
Mc Graw-Hill Book New York 1970.