République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Djilali BOUNAÂMA Khemis Miliana

Mémoire Présenté

Pour l'obtention de diplôme de

Master en Mathématiques

Spécialité : Mathématiques Appliquées et Traitement du sigual

Intitulé

Introduction aux courbes elliptiques

Réalisé par : **BENCHAA SOUAD**

Soutenu publiquement le :28 / 06 / 2016

devant les membres du jury :

Mr. O.Benniche	Université de Djilali BOUNAÂMA.	Président
Mr. B.Sadaoui	Université de Djilali BOUNAÂMA	Encadreur
Mr. M.bouderbala	Université de Djilali BOUNAÂMA	Examinateur
Mr. A.Krelifa	Université de Djilali BOUNAÂMA	Examinateur

Année Universitaire 2015/2016

Résumé

L'objectif de ce mémoire, est de donner une introduction générale sur les courbes elliptiques, et de rappeler quelques applications de ces courbes dans d'autres disciplines. Tout d'abord, on rappelle la définition d'une courbe elliptique, et les transformations qui réduisent son équation de **W**eierstrass, en suite on présente la structure de son groupe donne la construction de son groupe de **M**ordell **W**eil. Enfin, et comme des applications de ces courbes, on les utilise dans la factorisation d'un entier, et finalement, on explique la cryptographie en utilisant les courbes elliptiques.

Abstract

The objective of this thesis is to give a general introduction on elliptic curves , and to recall some applications of these curves in other disciplines. First, we recall the definition of an elliptic curve , and the transformations that reduce its Weierstrass equation , the suite presents its group structure gives the building its Mordell Weil. Finally, and as applications of these curves are used in the factorization of an integer, and finally , it is explained cryptography using elliptic curves

Dédicaces

Je dédie ce modeste travail :

A la prunelle de mes yeux et la joie de ma vie, ma Mère et mon Père, mon mari pour leur confiance,

amour, courage et surtout leurs conseils précieux durant toutes mes années d'études ;

A mes sœurs : Nadia, Salima, Rania et surtout mon frère AbdElhak ;

A mes oncles et leurs familles et ma tante Saida;

A tout l'entourage familial ;

A toutes mes copines qui se connaissent eux même sans citer leurs noms, sans oublier ma chère

copine zola qui a partagé avec moi le meilleur et le pire ;

A tout mes collègues ;

Et bien sur à moi-même.

souad

Remerciements

Avant tout

Nous remercions Dieu qui nous a donné la foi,

la volanté et le courage d'aller jusqu'au bout.

Nous profitons de cette occasion pour exprimer notre profonde gratitude et

Remerciements à Mr B.Saadaoui qui nous a donné la chance de travailler avec lui

et surtout ses conseils précieux durant toute la période du travail.

Nous remercions également les membres du jury d'avoir accepter l'évaluation de

notre travail.

Et aussi A Dr BENBACHIR et Mr boukabcha et Mr.Said Abd El Rezzak pour leurs

aides et leurs encouragements.

A mes enseignants qui nous ont suivis durant les années d'études, sans oublier l'effectif

du service de Département de Mathématiques et Informatique.

A tous ceux qui ont contribué de prés ou de loin à la réalisation de ce modeste

travail.

Notations et Abréviations

$\mathbf{F}_p$ =: Un corps fini à q éléments ;

$Ker\ f$ =: Le noyau de f;

$Im\ f$ =: L'image de f;

$\mathbb{Z}$ =: L'ensemble des nombres entiers ;

$\mathbb{Z}/n\mathbb{Z}$ =: Les classes résiduelles d'entiers modulo n ;

$a \equiv b[n]$ =: a congrus b modulo n ;

$(n, q) = 1$ =: n et q sont premiers entre eux ;

$a|b$ =: a est divise b ;

$PGCD(a; b)$ =: Le plus grand commun multiple de a et b.

mod =: est l'opération de modulo (reste de la division entière)

$\Bbbk^*$ =: L'ensemble des éléments inversibles de $\Bbbk$.

Table des matières

Introduction

La théorie des courbes elliptiques est une branche de Mathématiques, qui se situent de sur croîtau croisement de multiples branches : arithmétique, géométrie algébrique, représentations de groupes, analyse complexe, etc.

En général, une courbe elliptique est une courbe algébrique, munie entre autres propriétés d'une addition géométriquesur ses points. Parmi les applications des courbes elliptiques, elles interviennenten mécanique classique dans la description du mouvement des toupies ; en théorie des nombres dans la preuvedu dernier théorème de Fermat qui a été démontré par Andrew Wiles en 1995 ; encryptologie dans le problème de la factorisation des entiers ou pour fabriquer des codes performants.Contrairement à ce que son nompourrait laisser croire, l'ellipse n'est pas une courbe elliptique. Le nom des courbes elliptiques vienthistoriquement de leur association avecles intégrales elliptiques, elles-mêmesappelées ainsi car elles servent en particulier à calculer la longueur d'arcs d'ellipses.

Le mémoire est composé de quatre chapitres, le premier chapitre est consacré à présenter quelques préliminaires qui seront utiles tout au long de ce travail.

Dans le deuxième chapitre, on rappelle les définitions et les propriétés d'une courbe elliptique.

Le troisième chapitre, est consacré à la construction du groupe de Mordell- Weil $E(\Bbbk)$d'une courbe elliptique sur un corps $\Bbbk$.

Enfin, dans le quatrième et le dernier chapitre on donne quelques applications des courbes elliptiques.

Chapitre 1

Préliménaires

On regroupe dans ce chapitre quelque notions qui seront nécessaire pour la suite.

1.1 Groupes et anneaux

1.1.1 Groupes

Définition 1 *On appelle un groupe un couple formé par un ensemble G et d'une loi de composition $(x, y) \to xy$ sur G:*
•$\forall x, y; z \in G : (xy)\, z = x\,(yz)\,(associativité)$.
•$\exists 1 \in G$ *tel que* $\forall x \in G : x1 = 1x = x$ $(existence\ d'un\ élément\ neutre)$.
•$\forall x \in G, \exists x^{-1} \in G$ *tel que* $x^{-1}x = xx^{-1} = 1$ *(existence d'un élément inverse pour tout élément du groupe).*

Remarque 1 1)*Si la loi de groupe est commutative, le groupe est appelé groupe commutatif* $(ou\ abélien)$.
2)*Pour un groupe commutatif, on utilise la notation du loi* $(x, y) \to x + y$.
Dans cette notation, l'élément neutre est habituellement noté O *et l'inverse d'un élément* x *est noté* $(-x)$.

Exemple 1 *on définit dans* $\mathbb{Z}$ *une loi de composition interne* T *définit par*

$$aTb = a + b + ab$$

avec $a, b \in \mathbb{Z}$, $(\mathbb{Z} - \{-1\}, T)$ *est un groupe car :*

•*T est associative*

Soient $a, b, c \in \mathbb{Z}$

$$\begin{aligned}(aTb)\,Tc = yTc = y + c + yc \qquad & tq \qquad y = a + b + ab\\ = (a + b + ab) + c + (a + b + ab)\,c\end{aligned}$$

$$\begin{aligned}aT\,(bTc) = aTx = a + x + ax \qquad & tq \qquad x = b + c + bc\\ = a + (b + c + bc) + a\,(b + c + bc)\end{aligned}$$

donc : $(aTb)\,Tc = aT\,(bTc)$

•*L'existence de l'élément neutre*

On suppose que O *est l'élément neutre a loi* T

$$\forall a \in \mathbb{Z} :\ aTO = OTa = a$$

$$\begin{aligned}aTO = a &\Rightarrow a + O + aO = a\\ &\Rightarrow O\,(1 + a) = 0\\ &\Rightarrow O = 0.\end{aligned}$$

•*Tout élément de* $\mathbb{Z}$ *admet un symétrique ?*

supposons que x' *est l'élément symétrique de* x *donc :*

$$\begin{aligned}xTx' = 0 &\Rightarrow x + x' + xx' = 0\\ &\Rightarrow x' + xx' = -x\\ &\Rightarrow x' = \frac{-x}{1 + x}\end{aligned}$$

donc l'élément $x = -1$ *n'admet pas de symétrique donc*$(\mathbb{Z}, T)$ *n'est pas un groupe mais par contre* $((\mathbb{Z} - \{-1\}, T))$ *est un groupe.*

Applications surjectives

Définition 2 *Une application* $f : E \longrightarrow F$ *est surjective si tout élément de* F *possède au moins un anticédant*

$$f \text{ surjective } \Leftrightarrow \forall y \in F, \exists\,(au\ moins)\, x \in E,\ f(x) = y.$$

Exemple 2 *Soit* f *un application tq :*

$$\begin{aligned}f : \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longrightarrow f(x) = \frac{2x}{1 + 2x^2}\end{aligned}$$

1/ f est elle surjective

Suposon que $y = 2$, on a

$$\begin{aligned} y = f(x) &\Leftrightarrow 2 = f(x) \\ &\Leftrightarrow 2 = \frac{2x}{1+2x^2} \\ &\Leftrightarrow 2 + 2x^2 = 2x \\ &\Leftrightarrow 2x^2 - 2x + 2 = 0 \\ \Delta = 4 - 4\,(2)\,(2) &= -12 < 0. \end{aligned}$$

Donc l'équation n'admet pos de solution alors f n'est pas surjective.

homomorphisme de groupe

Définition 3 *Soit $(G, \bullet)$ et $(H, *)$ deux groupes, une application $f : G \longrightarrow H$ est appelée homomorphisme de groupes de G dans H si :*

$$\forall a, b \in G, \qquad f\,(a \bullet b) = f\,(a) * f\,(b) \tag{1.1}$$

Remarque 2 *Si dans la relation (1.1), nous prenons $b = 1$,*

$$\begin{aligned} f\,(a \bullet 1) &= f\,(a) * f\,(1) \\ f\,(a) &= f\,(a) * f\,(1) \\ \frac{f\,(a)}{f\,(a)} &= f\,(1) \\ 1 &= f\,(1) \end{aligned}$$

alors $f\,(1) = 1$.

Dans la définition, nous avons utilisé l'écriture multiplicative pour les groupes G et H. Si les groupes sont notés additivement, il faut bien sûr adapter la définition en conséquence. Par exemple, si le groupe G est noté additivement et le groupe H multiplicativement, alors la relation (1.1) devient

$$f\,(a + b) = f\,(a)\,f\,(b)$$

Exemple 3 *On a les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, .)$, alors l'application suivante est un homomorphisme de groupes*

1)

$$\begin{aligned} f : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^*, .) \\ x &\longrightarrow \exp x. \end{aligned}$$

On applique la définition

$$\forall x, y \in \mathbb{R}, \qquad f(x+y) = f(x).f(y)$$
$$\forall x, y \in \mathbb{R}, \qquad \exp(x+y) = \exp(x).\exp(y).$$

2)

$$g : (\mathbb{R}^*, .) \longrightarrow (\mathbb{R}, +)$$
$$x \longrightarrow \ln \mid x \mid .$$

On applique la définition

$$\forall x, y \in \mathbb{R}^*, \qquad g(x.y) = g(x) + g(y)$$
$$\forall x, y \in \mathbb{R}^*, \qquad \ln \mid x.y \mid = \ln \mid x \mid + \ln \mid y \mid .$$

Exemple 4 *Soient G le groupe additif $\mathbb{Z}$, H un groupe multiplicatif quelconque et a un élément de H.*
L'aplication

$$f : \mathbb{Z} \longrightarrow H$$
$$n \longrightarrow a^n$$

est un homomorphisme de $\mathbb{Z}$ dans H.
En effet,

$$f(n_1 + n_2) = a^{n_1+n_2} = a^{n_1}a^{n_2} = f(n_1)\, f(n_2).$$

Le noyau

Définition 4 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes. On appelle noyau de f l'ensemble*

$$\ker\ f = f^{-1}(\{h\}) = \{a \in G;\ f(a) = h\}$$

et l'image de f l'ensemble

$$\mathrm{Im}\ f = f(G) = \{f(a),\ a \in G\}.$$

1.1.2 Anneaux

Définition 5 *On appelle un anneau un ensemble* $\mathbb{k}$ *muni de deux lois de composition* $(x, y) \longmapsto xy$ *et* $(x, y) \mapsto x + y$ *sur l'ensemble* $\mathbb{k}$*.Tel que:*

- $(\mathbb{k}, +)$ *est un groupe commutatif;*
- *la loi de composition* $(x, y) \longmapsto xy$ *est associative et admet un élément neutre 1;*
- $\forall x, y, z \in \mathbb{k} : x(y + z) = xy + yz$ $(distributivité)$.

Remarque 3 *Si la loi de composition* $(x, y) \longmapsto xy$ *est commutative, alors l'anneau est dit commutatif.*

Exemple 5 $*$*L'ensemble des entiers muni des lois composition habituelles (adition et multiplication) forme un anneau commutatif.*

1.2 Corps finis

Définition 6 $\mathbb{k}$ *un anneau. On dit que* $\mathbb{k}$ *est un corps si tout élément non nul de* $\mathbb{k}$ *est inversible.*

Exemple 6 *Les anneaux* $\mathbb{Q}$ *et* $\mathbb{R}$ *sont des corps, appelés respectivement corps dse nombres rationnels et corps dse nombres réels*

Exemple 7 *Par contre, l'anneau* $\mathbb{Z}$ *n'est pas un corps car les seuls éléments non nuls qui sont inversibles sont 1 et -1.*

Définition 7 *Un corps fini est un corps commutatif dont le nombre d'éléments est fini.*

Exemple 8 *Si* p *un entier premier, alors* $\mathbb{Z}/p\mathbb{Z}$ *est un corps fini, notons* $\mathbf{F}_p$ *tel que :*

$$\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, ..., p - 1\}$$

Définition 8 *Soit* $\mathbb{k}$ *un corps. La caractéristique de* $\mathbb{k}$ *c'est le plus petit entier* p *tel que*

$$p.1 = 0.$$

1.3 Le plan projectif P_2

Définition 9 *soit $\Bbbk$ un corps, Le plan projectif $P_2(\Bbbk)$ est l'ensemble des points $P = (a, b, c)$ non nul dans $\Bbbk^3$ de sorte que deux points $P = (a, b, c)$ et $P^{'} = (a^{'}, b^{'}, c^{'})$ sont considérés comme étant des points équivalents s' il existe t appartient à $\Bbbk^*$ tel que $(a, b, c) = t(a^{'}, b^{'}, c^{'})$.*
a, b et c sont appelés les coordonnées homogènes du point P.

Plus généralement, nous définissons le *n-espace projectif* $P_n(\Bbbk)$ comme l'ensemble des classes d'équivalence des $(n+1)$

$$P_n(\Bbbk) = \frac{\{(a_0, a_1, ..., a_n) \in \Bbbk^{n+1}, \quad \text{tel que : } a_0, a_1, ..., a_n \text{ non tous nuls } \}}{\tilde{}},$$

où $(a_0, a_1, ..., a_n) \tilde{} (a'_0, a'_1, ..., a'_n)$ s'il existe $t \in \Bbbk^*$tel que

$$(a_0, a_1, ..., a_n) = t\,(a'_0, a'_1, ..., a'_n)$$

Définition 10 *Soit un corps $\Bbbk$. Le degré d'un terme d'un polynôme P de l'anneau $\Bbbk[X_1, ..., X_n]$ est la somme des exposants des variables X_i apparissant dans ce terme. Le degré du polynôme p est le plus grand de ses termes.*

Exemple 9 *Le polynôme $p(x, y, z) = 3x^3y + 4x^2y^2z - yz^2$ est un polynôme de degré 5.*

polynôme irréductible

Définition 11 *Soit un corps $\Bbbk$. Un polynôme $P \in \Bbbk[X_1, ..., X_n]$ est un polynôme homogène de degré d si chacun de ses termes est de degré d. De plus, P est dit **irréductible** s'il ne peut pas s'écrire comme un produit non trivial de deux polynôme de $\Bbbk[X_1, ..., X_n]$.*

Notation 1 *Si P est un polynôme homogène de degré d défini sur un corps $\Bbbk$ et à n variables, alors nous écrirons $P \in \Bbbk[X_1, ..., X_n]_d$.*

Définition 12 *Soit un corps $\Bbbk$. Une courbe E de $P_2(\Bbbk)$ est l'ensemble des points qui satisfait à*

$$P(x, y, z) = 0,$$

Notation 2 $E(\Bbbk) := \{(x, y, z) \in P_2(\Bbbk) : P(x, y, z) = 0\}$

où $P \in \Bbbk[X_1, ..., X_n]_d$est un polynôme homogène de degré $d \geq 1$.

$*$Si $d = 1$, alors E est appelée une droite.

$*$Si $d = 2$ E est dite une conique.

$*$Si $d = 3$ **une cubique**, Le nombre d est appelé le **degré** de la courbe.

Le plan usuel sur un corps $\Bbbk$, et noté $A_2(\Bbbk)$, est l'ensemble des point $(X, Y) \in \Bbbk^2$. Si nous introduisons les coordonnés x, y, z telles que $X = \frac{x}{z}$ et $Y = \frac{y}{z}$, alors à tout point (X, Y) de $A_2(\Bbbk)$ correspond le point (x, y, z) de $P_2(\Bbbk)$. Réciproquement, si $z \neq 0$, alors à tout point (x, y, z) de $P_2(\Bbbk)$ correspond le point (X, Y) de $A_2(\Bbbk)$. Dans le cas $z = 0$ on considere dans $A_2(\Bbbk)$, deux droites parallèles

$$L : aX + bY + c = 0 \qquad et \qquad L' : a'X + b'Y + c = 0$$

où $a' = ta$ et $b' = tb$. En coordonnées homogènes, c-à-d. dans $P_2(\mathbb{R})$, ces droites s'écrivent

$$L : ax + by + cz = 0 \qquad et \qquad L' : a'x + b'y + c'z = 0$$

L'intersection de ces droites a lieu en un point pour le quel $z = 0$. Un tel point est appelé **point à l'infini.**

courbe algébrique

Définition 13 *une* ***courbe algébrique*** *est un schéma de type fini sur un corps, dont les composantes irréductibles sont de dimension 1*

1.4 congrunce modulo n

Définition 14 *Soit n un entier naturel. Deux entiers relatifs a et b sont dits* ***congrus modulo*** *n si leur différence est divisible par n, c'est-à-dire*

$$a = b + kn \qquad k \in \mathbb{N}$$

et on notè :

$$a \equiv b[n] \quad ou \quad a \equiv b(modn).$$

les propriétés :

1/Pour tout entier a,

$$a \equiv a[n].$$

En effet :

$$a = a + 0n \Rightarrow a \equiv a[n]$$

2/pour tous entiers a et b,

$$a \equiv b[n] \Leftrightarrow b \equiv a[n].$$

En effet :

$$\begin{aligned} a = b + kn &\Leftrightarrow b = a + (-k)n \quad \text{tq } k \in \mathbb{Z} \\ &\Leftrightarrow b = a + k_1 n \\ &\Leftrightarrow b \equiv a[n]. \end{aligned}$$

3/pour tous entiers a, b et c,

$$si\ a \equiv b[n] \qquad et \qquad b \equiv c[n] \qquad alors \qquad a \equiv c[n].$$

En effet :

$$\begin{aligned} a = b + kn \quad &\text{et} \quad b = c + k_1 n \quad \text{tq } k, k_1 \in \mathbb{Z} \\ &\Rightarrow b = a + (-k)n \quad \text{et} \quad b = c + k_1 n \\ &\Rightarrow b = a + (-k)n = c + k_1 n \\ &\Rightarrow a - c = (k + k_1)\, n \\ &\Rightarrow a = c + (k + k_1)\, n \\ &\Rightarrow a = c + k_2 n \\ &\Rightarrow a \equiv c[n]. \end{aligned}$$

4/Si $a_1 \equiv b_1\ (n)$ et $a_2 \equiv b_2(n)$, alors

$$a_1 + a_2 \equiv b_1 + b_2[n] \qquad \text{et} \qquad a_1 a_2 \equiv b_1 b_2[n],$$

car

$$a_1 = b_1 + k_1 n \quad \text{et} \quad a_2 = b_2 + k_2 n \qquad \text{tq} \quad k_1, k_2 \in \mathbb{Z}$$

donc on a

$$(a_1 - b_1) = k_1 n, \qquad (a_2 - b_2) = k_2 n$$

$$\begin{aligned} (a_1 - b_1) + (a_2 - b_2) &= kn \\ (a_1 + a_2) - (b_1 + b_2) &= kn \\ (a_1 + a_2) &= (b_1 + b_2) + kn \\ a_1 + a_2 &\equiv b_1 + b_2[n] \end{aligned}$$

Pour $a_1a_2 \equiv b_1b_2[n]$ on a et

$$(a_1 - b_1) = k_1 n \qquad \text{et} \qquad (a_2 - b_2) = k_2 n.$$

On en tire

$$a_1 = b_1 + k_1 n, \qquad a_2 = b_2 + k_2 n.$$

D'où

$$a_1 a_2 = b_1 b_2 + n\left(k_1 b_2 + k_2 b_1 + k_1 k_2 n\right).$$

On en déduit que

$$a_1 a_2 \equiv b_1 b_2[n]$$

Diviseur

Définition 15 *Si les termes a et b d'une division sont des nombres naturels non nuls, alors b est un* ***diviseur entier*** *de a si et seulement si le reste de cette division est nul.*

Définition 16 *un* ***diviseur premier*** *est un diviseur entier qu'est un* ***nombre premier.***

Exemple 10 *Dans l'opération* $12 \div 4 = 3$*, le nombre* 4 *est le diviseur.*
L'ensemble des diviseurs de 60*, noté div*60*, est*

$$\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}.$$

L'ensemble des diviseurs premiers de 60 *est* $\{2, 3, 5\}$*.*

Décomposition d'un nombre en facteurs premiers

Définition 17 *On appelle un décomposition d'un nombre en facteurs premiers la formule*

$$x = \prod_{i=1}^{r} P_i^{\alpha_i}$$

telle que P_i *parcorue l'ensemble des nombre premier et* α_i *des entier tq* $\alpha_i \geq 0$*.*

Propriété : La décomposition d'un nombre en facteurs premiers est unique.

Exemple 11 $50 = 2 * 5 * 5 = 2 * 5^2$.
$100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$.

diviseur non trivial

Définition 18 *un diviseur non trivial d'un entier naturel n est un* ***entier naturel*** *diviseur de n mais distinct de n et de 1 (qui sont ses diviseurs triviaux).*

Exemple 12 *Les diviseurs non triviaux de 30 sont $2, 3, 5, 6, 10$ et 15.*

Chapitre 2

Quelque notions sur les courbes elliptiques

Dans ce chapitre, on va introduire quelques notions des courbes elliptiques et donner quelques exemples et quelques résultats

2.1 Structure d'une courbe elliptique

2.1.1 Courbe elliptique

Définition 19 *Une courbe elliptique est une paire* (E, O_∞), *où* E *est une cubique irréductible non singulière et* $O_\infty \in E$. *On dit que la courbe elliptique* E *est définie sur un corps* $\Bbbk$ *si* E *est une courbe sur* $\Bbbk$ *et si* $O_\infty \in E(\Bbbk)$.

Remarque 4 *Le point "**non singulière** " signifie que la propriété suivante est satisfaite :*
$*$*si* $P = (X, Y, Z) \in \Bbbk^3$, *vérifie l'équation*

$$E : F(x, y, z) = 0 \tag{2.1}$$

alors

$$\left.\frac{\partial F}{\partial x}\right|_P \neq 0 \quad ou \quad \left.\frac{\partial F}{\partial y}\right|_P \neq 0 \quad ou \quad \left.\frac{\partial F}{\partial z}\right|_P \neq 0$$

$*$*si* P *vérifie l'équation (2.1), on dit que* P *est un point sur la courbe. La condition "courbe **non singulière**" de la définition affirme que si* $F(X, Y, Z) = 0$,*avec* $(X, Y, Z) \in \Bbbk^3$,*alors le*

vecteur

$$(\frac{\partial F}{\partial x}(X,Y,Z), \frac{\partial F}{\partial y}(X,Y,Z), \frac{\partial F}{\partial z}(X,Y,Z))$$

n'est pas le vecteur nul. En d'autres termes, on peut définir une tangente à la courbe au point (X,Y,Z).

Exemple 13

►On prend $\Bbbk = \mathbb{R}$, on pose :

$$E_1 : y^2 = x^3 + x \qquad \text{et} \qquad E_2 : y^2 = x^3 + x^2.$$

Les courbes E_1 et E_2 sont bien définies sur $\mathbb{R}$ puisque tous les coefficients sont réels.
La courbe E_1est **non singulière**, car :

$$\left(\frac{\partial F}{\partial x}(x,y), \frac{\partial F}{\partial y}(x,y)\right) = (0,0) \Leftrightarrow \begin{cases} 3x^2 + 1 = 0 \\ 2y = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x^2 = -\frac{1}{3} \\ y = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x^2 = \frac{i^2}{3} \\ y = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = \pm\frac{i}{\sqrt{3}} \\ y = 0 \end{cases}$$

or les points $(\pm i/\sqrt{3}, 0)$ ne sont pas sur la courbe et donc la courbe E_1est **non singulière**.
Pour la courbe E_2 est **non singulière**, car :

$$\left(\frac{\partial F}{\partial x}(x,y), \frac{\partial F}{\partial y}(x,y)\right) = (0,0) \Leftrightarrow \begin{cases} 3x^2 + 2x = 0 \\ 2y = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x(3x+2) = 0 \\ 2y = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 0 \\ y = 0 \end{cases} \vee \begin{cases} 3x + 2 = 0 \\ y = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = \frac{-2}{3} \\ y = 0 \end{cases}$$

le point $(0,0)$ est un point sur la courbe et on vérifie aisément que $\frac{\partial F}{\partial x}(0,0) = \frac{\partial F}{\partial y}(0,0) = 0$. On dit alors que le point $(0,0)$ est un point singulier.

La courbe E_2 est **non singulière**. E_2 possède un point singulier (un point double en $(0,0)$).

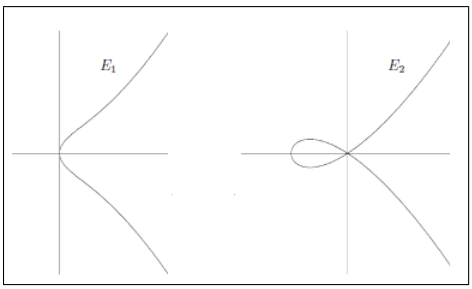


FIG : 1.1 – Graphes des courbes E1 et E2 sur $\mathbb{R}$.

2.1.2 Équations de Weierstrass

Définition 20 *une courbe elliptique sur* $\Bbbk$*, définie comme l'ensemble des solutions du plan projectif* $P_2(\Bbbk)$ *de l'équation de Weierstrass suivante :*

$$E : F(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

où les coefficients a_1, a_2, a_3, a_4 *et* a_6 *sont dans* $\Bbbk$*.*

pour alléger les notations, nous allons écrire l'équation de Weierstrass avec coordonnées non homogènes : $X = x/z$ et $Y = y/z$,

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2.2}$$

2.2 Transformation de l'équation de Weierstrass

Soit $\Bbbk$ un corps de caractéristique $\Bbbk \neq 2, 3$, il'ya des transformation qui rendrent l'équation a la courbe elliptique (2.2) , plus simplifiée.

Proposition 1 *Soit E une courbe elliptique. On peut se ramener une équation de E, dite forme simplifiée de Weierstrass :*
1/Si car$(\Bbbk) \neq 2$*, on a*

$$E' : Y^2 = X^3 + \frac{b_2}{4}X^2 + \frac{b_4}{2}X + \frac{b_6}{4}$$

2/Si car$(\Bbbk) \neq 3$*, on a*

$$E" : y^2 = x'^3 + B'x' + C'$$

Preuve. On a l'équation de Weierstrass :

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2.3}$$

1/ Supposons que car($\Bbbk$) $\neq 2$, le changement lineaires de variables $(X, Y) \to \left(X, Y + \frac{a_1}{2}X + \frac{a_3}{2}\right)$ transforme l'équation(2.3) :

$$(Y + \frac{a_1}{2}X + \frac{a_3}{2})^2 = Y^2 + a_1XY + a_3Y + \frac{a_1a_3}{2}X + \frac{a_1^2}{4}X^2 + \frac{a_3^2}{4}$$

on ajoute la valeur $(\frac{a_1a_3}{2}X + \frac{a_1^2}{4}X^2 + \frac{a_3^2}{4})$ dans la formule (2.3) ensuite on l'enleve.

$$\begin{aligned} Y^2 + a_1XY + a_3Y + \frac{a_1a_3}{2}X + \frac{a_1^2}{4}X^2 + \frac{a_3^2}{4} &= X^3 + a_2X^2 + a_4X + a_6 + \frac{a_1a_3}{2}X + \frac{a_1^2}{4}X^2 + \frac{a_3^2}{4} \\ (Y + \frac{a_1}{2}X + \frac{a_3}{2})^2 &= X^3 + (a_2 + \frac{a_1^2}{4})X^2 + (a_4 + \frac{a_1a_3}{2})X + (a_6 + \frac{a_3^2}{4}) \\ &= X^3 + (\frac{4a_2 + a_1^2}{4})X^2 + (\frac{2a_4 + a_1a_3}{2})X + (\frac{4a_6 + a_3^2}{4}) \end{aligned}$$

On pose $b_2 = (4a_2 + a_1^2)$, $b_4 = (2a_4 + a_1a_3)$ et $b_6 = (4a_6 + a_3^2)$ et on définit la courbe E' sur $\Bbbk$ par :

$$E' : Y^2 = X^3 + \frac{b_2}{4}X^2 + \frac{b_4}{2}X + \frac{b_6}{4}$$

donc on a

$$E' : y^2 = x^3 + Ax^2 + Bx + C \tag{2.4}$$

2/Supposons que car($\Bbbk$) $\neq 3$, on pose $x' = \left(x + \frac{A}{3}\right)$ tq $A = (\frac{4a_2 + a_1^2}{4})$

$$\begin{aligned} x'^3 = \left(x + \frac{A}{3}\right)^3 &= x^3 + x^2\frac{A}{3} + x^2\frac{A}{3} + x\frac{A^2}{9} + x^2\frac{A}{3} + \frac{A^2}{9} + \frac{A^2}{9}x + \frac{A^3}{27} \\ &= x^3 + Ax^2 + \frac{2}{9}A^2x + \frac{3A^2 + A^3}{27} \end{aligned}$$

on ajoute la valeur $(\frac{2}{9}A^2x + \frac{3A^2+A^3}{27})$ dans la formule (2.4) ensuite on l'enleve.

$$\begin{aligned}
y^2 + \frac{2}{9}A^2x + \frac{3A^2+A^3}{27} &= x^3 + Ax^2 + Bx + C + \frac{2}{9}A^2x + \frac{3A^2+A^3}{27} \\
y^2 &= x^3 + Ax^2 + \frac{2}{9}A^2x + \frac{3A^2+A^3}{27} + Bx + C - \frac{2}{9}A^2x - \frac{3A^2+A^3}{27} \\
y^2 &= x'^3 + Bx + C - \frac{2}{9}A^2x - \frac{3A^2+A^3}{27} \\
y^2 &= x'^3 + (B - \frac{2}{9}A^2)((x + \frac{A}{3}) - \frac{A}{3}) + C - \frac{3A^2+A^3}{27} \\
y^2 &= x'^3 + (B - \frac{2}{9}A^2)x' - (B - \frac{2}{9}A^2)\frac{A}{3} + C - \frac{3A^2+A^3}{27} \\
y^2 &= x'^3 + (B - \frac{2}{9}A^2)x' - \frac{BA}{3} + \frac{2A^3}{27} + C - \frac{3A^2+A^3}{27} \\
y^2 &= x'^3 + (B - \frac{2}{9}A^2)x' + \left[C - \frac{3A^2+3A^3}{27} - \frac{BA}{3}\right] \\
y^2 &= x'^3 + A'x' + C'
\end{aligned}$$

On pose $A' = (B - \frac{2}{9}A^2)$, $C' = (C - \frac{3A^2+3A^3}{27} - \frac{BA}{3})$ et on définit la courbe $E^{"}$ sur $\Bbbk$ par :

$$E" : y^2 = x'^3 + A'x' + C'$$

Remarque 5 *Il existe d'autres formes de l'équation d'une courbes elliptique; par exemple :*

$$\begin{aligned}
E_1 &: Y^2 = X\,(X - \lambda)\,(X - \lambda) \\
E_2 &: Y^2 = (X - e_1)\,(X - e_2)\,(X - e_3)
\end{aligned}$$

l'hypothèse $\prec$ **non − singulière** $\succ$ *implique les conditions :* $A \neq 0, 1$, *et* $e_j \neq e_i$ *pour* $i, j = 1, 2, 3$.

Proposition 2 *Sur les cubiques de Weierstrass E le point à l'infini* $O_\infty = (\infty, \infty) = (0, 1, 0)$ *est un point non singulier sur E.*

Preuve. Soit une cubique de Weierstrass d'équation

$$E : F(X, Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in \mathbb{R}\,[X, Y] \tag{2.5}$$

Dans le plan Projectif $P_2(\mathbb{R})$, l'équation (2.5)devient :

$$E : F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in P_2(\mathbb{R})$$

on a les dérivées partielles :

$$F'_X = \frac{\partial F}{\partial X} = a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2 - a_6Z^3$$
$$F'_Y = \frac{\partial F}{\partial Y} = 2YZ + a_1XZ + a_3Z^2$$
$$F'_Z = \frac{\partial F}{\partial Z} = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2$$

Les coordonnées du point O_E satisfont cette équation : $F(O_E) = 0$. Il en résulte que ce point est sur la cubique E. La valeur $F'_Z(0,1,0) = 1 \neq 0$ implique que le point $O_E = (0,1,0) = (\infty, \infty)$ est un point non singulier sur E .

2.3 Invariants d'une courbe elliptique

Les coeffécients b_i de l'équation d'une courbe elliptique E permettent de défini deux invariants de cette courbes :

Définition 21 *Soit* $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ *une courbe définie sur* $\Bbbk$. *On pose :*

$b_2 = a_1^2 + 4a_2$ $\qquad$ $b_4 = a_1a_3 + 2a_4$

$b_6 = a_3^2 + 4a_6$ $\qquad$ $b_8 = a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$

$$\begin{aligned}\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ &= -\left(a_1^2 + 4a_2\right)^2\left(a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\right) - 8\left(a_1a_3 + 2a_4\right)^3 - 27\left(a_3^2 + 4a_6\right)^2 \\ &+ 9\left(a_1^2 + 4a_2\right)\left(a_1a_3 + 2a_4\right)\left(a_3^2 + 4a_6\right).\end{aligned}$$

Le nombre $\Delta = \Delta(E)$ *est appelé le discriminant de* E.

Proposition 3 [4] *un courbe est une courbe elliptique si et seulement si on a* $\Delta \neq 0$.

Définition 22 *L'invariant modulaire d'une courbes elliptique* E *est la fraction rationnelle*

$$j(E) = \frac{C_4^3}{\Delta(E)}.$$

Définition 23 *Soit un polynôme*

$$f(x) = x^n + a_1x^{n-1} + ... + a_n, \qquad \text{de degré } n \succ 1$$

et sa factorisation

$$f(x) = \prod_{1 \leq i \leq n} (x - \theta_i), \quad \theta_i \in \mathbb{R} \tag{2.6}$$

alors le discriminant de f est égal à :

$$disc(f) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

L'une des méthodes de calcul de ce discriminant utilise la définition du Résultant de 2 polynômes.

Soit deux polynômes de l'anneau $\mathbb{R}[x]$:

$$\begin{aligned} f(x) &= a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n, \qquad \textit{de degré } n \succ 1 \ ; \\ g(x) &= b_0 x^m + b_1 x^{m-1} + ... + b_{m-1} x + b_m, \quad \textit{de degré } m \succ 1 \ ; \end{aligned}$$

Définition 24 *Résultant de deux polynômes f et g est le déterminant d'ordre $n+m$:*

$$\mathrm{Re}\, s(f,g) = \begin{vmatrix} a_0 & a_1 & . & . & . & a_n & 0 & . & . & 0 \\ 0 & a_0 & a_1 & . & . & . & a_n & 0 & . & 0 \\ 0 & 0 & a_0 & . & . & . & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & .a_0 & . & . & a_{n-1} & a_n \\ b_0 & b_1 & . & . & . & . & b_m & 0 & . & 0 \\ 0 & b_0 & . & . & . & . & . & b_0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & . & . & b_{m-1} & b_m \end{vmatrix}$$

formé de n lignes $(a_0.....a_n)$ et m colonne $(b_0.....b_m)$ de diagonale principale formée de m termes a_0 et n termes b_m et les termes manquants sont remplacés par des zéros.

Exemple 14 *$f(x) = 2x^3 + 3x^2 + 4$ et $g(x) = 3x^4 - 5x3 + 8x^2 - 6x - 3$ le Résultant $\mathrm{Re}\, s(f,g)$ est donc le déterminant d'une matrice carrée d'ordre $3+4=7$ de lignes $(a_0, a_1, a_2, a_3) = (2, 3, 0, 4)$ et $(b_0, b_1, b_2, b_3, b_4) = (3, -5, 8, -6, -3)$*

$$\operatorname{Re} s(f,g) = \begin{vmatrix} 2 & 3 & 0 & 4 & 0 & 0 & 0 \\ 0 & 2 & 3 & 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 & 3 & 0 & 4 \\ 3 & -5 & 8 & -6 & -3 & 0 & 0 \\ 0 & 3 & -5 & 8 & -6 & -3 & 0 \\ 0 & 0 & 3 & -5 & 8 & -6 & -3 \end{vmatrix}$$

Définition 25 *Le discriminant d'un polynôme $f(x)$ de degré $n > 1$*

$$f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n$$

est

$$disc(f) = (-1)^{\frac{n(n-1)}{2}} \operatorname{Re} s(f, f'). \tag{2.7}$$

Proposition 4 *soit $E : y^2 = x^3 + Bx + C$ une courbe définie sur $\Bbbk$. Le discriminant de E est $\Delta(E) = 16\ disc(f)$ tq $f = x^3 + Ax^2 + Bx + C$*

$$\Delta(E) = -16(4B^3 + 27C^2)$$

Preuve. On à $f = x^3 + Bx + C$ et sa dérivée

$$f'(x) = 3x^2 + B$$

et donc

$$\begin{aligned}
\Delta(E) &= (-1)^{\frac{3(3-1)}{2}} \operatorname{Re} s(f, f') \\
&= (-1)^{\frac{6}{2}} \operatorname{Re} s(f, f') \\
&= (-1)^3 \operatorname{Re} s(f, f') \\
&= -1 \operatorname{Re} s(f, f') \\
&= -\det \begin{pmatrix} 1 & 0 & B & C & 0 \\ 0 & 1 & 0 & B & C \\ 3 & 0 & B & 0 & 0 \\ 0 & 3 & 0 & B & 0 \\ 0 & 0 & 3 & 0 & B \end{pmatrix} \\
&= -\left(\det \begin{pmatrix} 1 & 0 & B & C \\ 0 & B & 0 & 0 \\ 3 & 0 & B & 0 \\ 0 & 3 & 0 & B \end{pmatrix} + B \det \begin{pmatrix} 0 & 1 & B & C \\ 3 & 0 & 0 & 0 \\ 0 & 3 & B & 0 \\ 0 & 0 & 0 & B \end{pmatrix} + C \det \begin{pmatrix} 0 & 1 & 0 & C \\ 3 & 0 & B & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & B \end{pmatrix} \right) \\
&= \vdots \\
&= -4B^3 - 27C^2
\end{aligned}$$

Proposition 5 *soit $E : y^2 = x^3 + Ax^2 + Bx + C$ une courbe définie sur $\Bbbk$. Le discriminant de E est*

$$\Delta(E) = -4A^3C + 18ABC - 4B^3 - 27C^2$$

Preuve. On a $f = x^3 + Ax^2 + Bx + C$ et sa dérivée

$$f'(x) = 3x^2 + 2Ax + B$$

et donc

$$\begin{aligned}
\Delta(E) &= (-1)^{\frac{3(3-1)}{2}} \operatorname{Re} s(f, f') \\
&= -\operatorname{Re} s(f, f') \\
&= -\det \begin{pmatrix} 1 & A & B & C & 0 \\ 0 & 1 & A & B & C \\ 3 & 2A & B & 0 & 0 \\ 0 & 3 & 2A & B & 0 \\ 0 & 0 & 3 & 2A & B \end{pmatrix}
\end{aligned}$$

$$
\begin{aligned}
&= -\left(\begin{array}{l}
\det\begin{pmatrix} 1 & A & B & C \\ 2A & B & 0 & 0 \\ 3 & 2A & B & 0 \\ 0 & 3 & 2A & B \end{pmatrix} + A\det\begin{pmatrix} 0 & A & B & C \\ 3 & B & 0 & 0 \\ 0 & 2A & B & 0 \\ 0 & 3 & 2A & B \end{pmatrix} \\
+B\det\begin{pmatrix} 0 & 1 & B & C \\ 3 & 2A & 0 & 0 \\ 0 & 3 & B & 0 \\ 0 & 0 & 2A & B \end{pmatrix} + C\det\begin{pmatrix} 0 & 1 & A & C \\ 3 & 2A & B & 0 \\ 0 & 3 & 2A & 0 \\ 0 & 0 & 3 & B \end{pmatrix}
\end{array}\right) \\
&= -\left(\begin{array}{l}
\det\begin{pmatrix} B & 0 & 0 \\ 2A & B & 0 \\ 3 & 2A & B \end{pmatrix} + A\det\begin{pmatrix} 2A & 0 & 0 \\ 3 & B & 0 \\ 0 & 2A & B \end{pmatrix} + B\det\begin{pmatrix} 2A & B & 0 \\ 3 & 2A & B \\ 0 & 3 & 2A \end{pmatrix} \\
+B\det\begin{pmatrix} 2A & B & 0 \\ 3 & 2A & 0 \\ 0 & 3 & B \end{pmatrix} + \ldots + C\det\begin{pmatrix} 3 & 2A & B \\ 0 & 3 & 2A \\ 0 & 0 & 3 \end{pmatrix}
\end{array}\right) \\
&= \vdots \\
&= -4A^3C + 18ABC - 4B^3 - 27C^2
\end{aligned}
$$

Exemple 15 $*E_1/\mathbb{R} : y^2 = x^3 + x$, *on a* $\Delta(E_1) = -4 \times 16 = 64 \neq 0$, *est une courbe elliptique.*

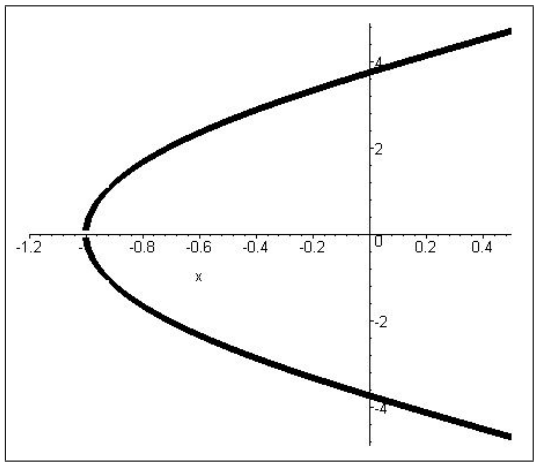
Exemple 16 $*E_2/\mathbb{R} : y^2 = x^3 + x^2$, *on a* $\Delta(E_1) = 0 \times 16 = 0$, *n'est pas une courbe elliptique.*

2.3.1 Représentation graphique

On prend $\mathbb{k} = \mathbb{R}$

Exemple 17 ▶*Soit* $E_1/\mathbb{k}$ *définie par*

$$E_1 : Y^2 = (X^2 + X + 14)(X + 1) = X^3 + 2X^2 + 15X + 14.$$



$FIG : 1.2 - Graphe\ de\ courbe\ E_1\ sur\ \mathbb{R}$

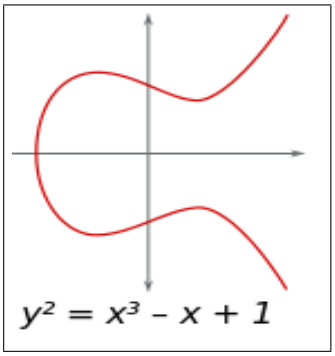
Est une courbe elliptique car $\Delta(E) = -4A^3C + 18ABC - 4B^3 - 27C^2$

$$\begin{aligned}\Delta(E) &= \left[-4 \times (2)^3 \times 14\right] + \left[18 \times (2) \times 15 \times 14\right] - \left[4 \times (15)^3\right] - \left[27 \times (14)^2\right] \\ &= -11680 \neq 0.\end{aligned}$$

◄

Exemple 18 ►*Soit* $E_2/\mathbb{k}$ *définie par*

$$E2 : \quad Y^2 = X^3 - X + 1$$



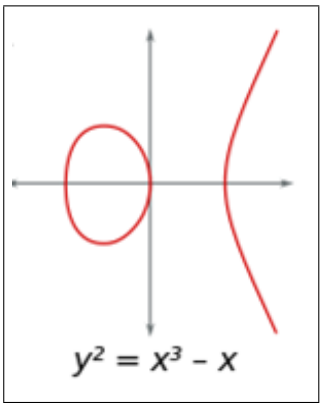
$FIG : 1.3 - Graphe\ de\ courbe\ E_2\ sur\ \mathbb{R}$

Est une courbe elliptique car $\Delta(E) = -16(4B^3 + 27C^2)$

$$\begin{aligned}\Delta(E) &= -16(4 \times (-1)^3 + 27(1)^2) \\ &= -16(-4 + 27) \\ &= -16(23) = -368 \neq 0.\end{aligned}$$

◄

Exemple 19 ▶*Soit* $E_3/\mathbb{k}$ *définie par*



$FIG : 1.3 - Graphe\ de\ courbe\ E3\ sur\ \mathbb{R}$

Est une courbe elliptique car $\Delta(E) = -16(4B^3 + 27C^2)$

$$\begin{aligned}\Delta(E) &= -16(4 \times (-1)^3) \\ &= -16(-4) \\ &= 64 \neq 0.\end{aligned}$$

Chapitre 3

Groupe de Mordell Weil d'une courbe

La loi de groupe abélien sur une courbe elliptique est déterminée par une propriété géométrique des sécantes qui coupent la courbe en 3 points distincts, soit en un point double et un point simple, soit en deux points distincts et un point à l'infini.

3.1 Structure de groupe $E(\Bbbk)$

3.1.1 Points rationnels

Dans cette partie, on considère une courbe elliptique E définie sur $\Bbbk$ par :

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{3.1}$$

Définition 26 *L'ensemble des points $\Bbbk$-rationnels de E, noté $E(\Bbbk)$ est :*

$$E(\Bbbk) = \left\{(X,Y) \in \Bbbk^2 \mid Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6\right\} \cup \{O_E\}$$

Exemple 20 *Soit E la courbe elliptique définie sur $\mathbb{Q}$ par*

$$E : Y^2 = X^3 - 6X + 4$$

L'ensemble des points $\mathbb{Q}$ rationnels de E

$$E(\Bbbk) = \{O_E, (-1,3), (-1,-3), (2,-3), (2,0), (1,-1), ...\}.$$

3.1.2 Introduction de la loi de groupe

Une courbe elliptique est un cas particulier de courbe algébrique, munie entre autres propriétés d'une addition géométrique sur ses points. En somme, il s'agit, pour deux points P et Q donnés de la courbe, de tracer la droite définie par ces deux points, et de considérer le troisième point appartenant à cette droite et à la courbe, qu'on appellera $P * Q$. En ayant choisi une origine O_E sur la courbe qui sera l'élément neutre de la loi de groupe, et qui peut être un point "à l'infini", $P + Q$ sera le troisième point d'intersection de la courbe et de la droite définie par les points $O_E = O$ et $P * Q$.

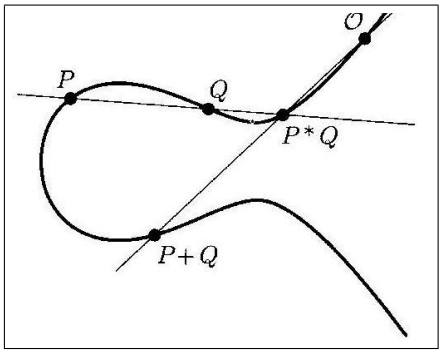


FIG : 2.1 – *Graphe de la loi de group sur les courbs elliptiques*

Définition 27 *On définit une loi de groupe abélien* $\oplus$ *sur* $E(\Bbbk)$ *de la façon suivante (il faudrait vérifier à posteriori qu'il s'agit bien d'une loi de groupe commutatif) :*
♦O_∞ *est l'élément neutre*

$$(x_1, y_1) \oplus O_\infty = O_\infty \oplus (x_1, y_1) = (x_1, y_1) \qquad \forall\, (x_1, y_1) \in E(\Bbbk)$$

♦*L'oposé de* (x_1, y_1) *est* $\ominus (x_1, y_1) = (x_1, \tilde{y}_1) = (x_1, -y_1 - a_1 x_1 - a_3)$.
♦*Soient* P *et* Q *deux points de* $E(\Bbbk) \setminus \{O_\infty\}$, *la droite passant par* P *et* Q *"**recoupe**" la courbe* E *en un troisiéme point* $P * Q \in E(\Bbbk)$ *qui est l'oposé de* $P \oplus Q$.

−*Si* $P = Q$, *on considére la droite tangente en* P *à la courbe* E *au lieu de la droite* (PQ).

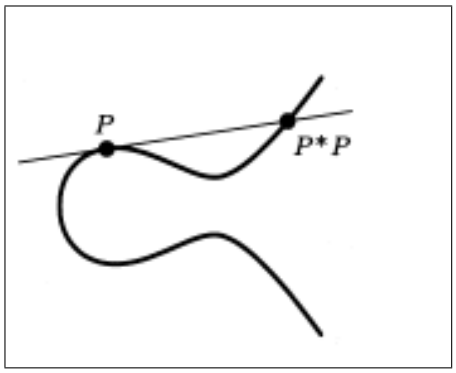


FIG : 2.2 – Graphe de courb dans le cas $P = Q$

L'addition de P et Q

−Si $P \neq Q$, La droite passant par P et Q a pour équation $y = \lambda x + \mu$ avec

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \qquad et \qquad \mu = y_1 - \lambda x_1$$

L'intersection de la droite (PQ) avec la courbe de weierstras E est donnée par :

$$\begin{aligned}
(\lambda x + \mu)^2 + a_1 x(\lambda x + \mu) + a_3(\lambda x + \mu) &= x^3 + a_2 x^2 + a_4 x + a_6 \\
(\lambda x + \mu)^2 + (a_1 x + a_3)(\lambda x + \mu) &= x^3 + a_2 x^2 + a_4 x + a_6 \\
\lambda^2 x^2 + \mu^2 + 2\lambda x\mu + a_1\lambda x^2 + a_1 x\mu + a_3\lambda x + a_3\mu &= x^3 + a_2 x^2 + a_4 x + a_6
\end{aligned}$$

ce qui donne l'équation suivante :

$$x^3 + a_2 x^2 + a_4 x + a_6 - \lambda^2 x^2 - \mu^2 - 2\lambda x\mu - a_1\lambda x^2 - a_1 x\mu - a_3\lambda x - a_3\mu = 0$$

Et donc :

$$x^3 + \left(a_2 - \lambda^2 - a_1\lambda\right)x^2 + \left(a_4 - 2\lambda\mu - a_1\mu - a_3\lambda\right)x + \left(a_6 - \mu^2 - a_3\mu\right) = 0 \qquad (3.2)$$

Les trois solutions de notre système est les coordonnées des points P, Q et **l'oposé** de $P \oplus Q$ $= (x_3, y_3) = P * Q$ tq $P \oplus Q = (x_3, \tilde{y}_3)$du coefficient de degré 2, l'équation(3.2) peut donc être écrite de la manière suivante :

$$(x - x_1)(x - x_2)(x - x_3) = 0.$$

Ce qui donne aprés développement :

$$x^3 - x_1 x^2 - x_2 x^2 - x_3 x^2 + x_1 x_2 x + x_1 x_3 x + x_2 x_3 x - x_1 x_2 x_3 = 0$$

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 = 0 \tag{3.3}$$

En égalisant les coefficients de (3.2) et (3.3), on obtient :

$$\begin{aligned} -(x_1 + x_2 + x_3) &= a_2 - \lambda^2 - a_1\lambda \\ -x_1 - x_2 - x_3 &= a_2 - \lambda^2 - a_1\lambda \\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \end{aligned}$$

donc on à les coordonnées de point $P * Q = (x_3, y_3)$

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = \lambda x_3 + \mu \end{cases}.$$

En remplaçant μ par sa valeur, on obtient :

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = \lambda x_3 + y_1 - \lambda x_1 \end{cases}$$

$$\Rightarrow \begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = \lambda(x_3 - x_1) + y_1 \end{cases}$$

et on à l'oposé de (x_1, y_1) est $\ominus(x_1, y_1) = (x_1, -(y_1 + a_1x_3 + a_3))$, donc

$$P \oplus Q = (x_3, \tilde{y}_3) \Rightarrow \begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ \tilde{y}_3 = -(\lambda(x_3 - x_1) + y_1) \end{cases}$$

$$P \oplus Q = (x_3, \tilde{y}_3) \Rightarrow \begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ \tilde{y}_3 = -(\lambda(x_3 - x_1) - (y_1 + a_1x_3 + a_3)) \end{cases}$$

$$P \oplus Q = (x_3, \tilde{y}_3) \Rightarrow \begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ \tilde{y}_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3 \end{cases}$$

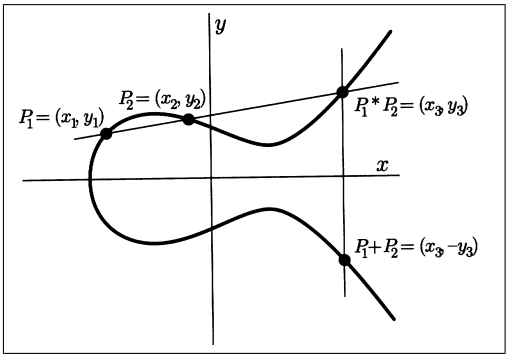


FIG : 2.3 – *Règle de la sécante tangente dans le cas* $P \neq Q$

Doublement de P

– Supposons maintenant que $P = Q = (x_1, y_1)$ et $y_1 \neq 0$. La droite tangente à la courbe E au point P a pour équation $y = \lambda x + \mu$ avec $\mu = y_1 - \lambda x_1$ et :

$$\begin{aligned}\lambda &= -\frac{\frac{\partial f}{\partial x}(x_1, y_1)}{\frac{\partial f}{\partial y}(x_1, y_1)} \\ &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}\end{aligned}$$

tq f équation de Weierstrass .

L'intersection de la droite avec la courbe de Weierstras E est donnée par :

$$(\lambda x + \mu)^2 + (a_1x + a_3)(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6$$

ce qui donne l'équation suivante :

$$x^3 + \left(a_2 - \lambda^2 - a_1\lambda\right)x^2 + (a_4 - 2\lambda\mu - a_1\mu - a_3\lambda)\,x + \left(a_6 - \mu^2 - a_3\mu\right) = 0$$

On connait une racine double (à savoir x_1) de cette équation, on en déduit la derniére solution, le calcul est ensuite le même qu'au paragraphe précédent. On obtient :

$$P \oplus P = (x_3, \tilde{y}_3) \Rightarrow \begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - 2x_1 \\ \tilde{y}_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3. \end{cases}$$

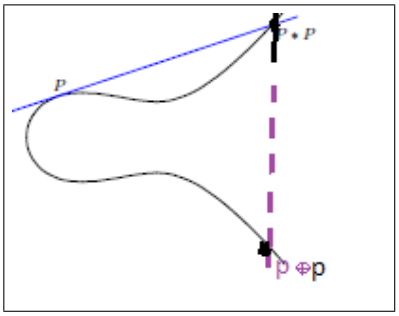


FIG : 2.4 – Règle de la sécante tangente dans le cas $P = Q$.

Si $y_1 = 0$:

La tangente en P à la courbe E est verticale et ne coupe E qu'au point P. Le point P est alors un point d'ordre 2 et on a $2P = O_E$, donc

$$P \oplus Q = P \oplus P = 2P = O_E$$

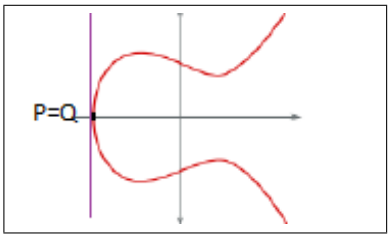


FIG : 2.5 – Règle de la sécante tangente dans le cas $P = Q$ et $y_1 = 0$.

Proposition 6 *Soit E est une courbe elliptique définie sur un corp $\mathbb{k}$. Pour tous points P_1,P_2, Q_1et Q_2 de E, nous avons :*

$$(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2)$$

Théorème 1 *Soit un corps $\mathbb{k}$. Soit E est une courbe elliptique définie sur $\mathbb{k}$. Soient P et Q deux points de cette courbe. Alors l'opération*

$$P + Q = O_E * (P * Q)$$

définit une structure de groupe commutatif ayant $O_E = O$ comme élément neutre.

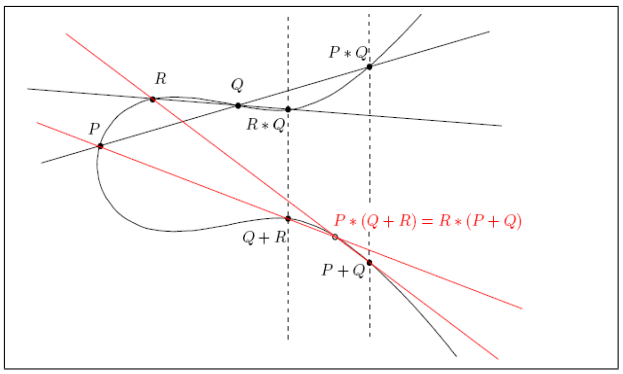


FIG : 2.6 – Graphe de L'associativité de la loi de groupe

Preuve. géométrique :

1/ La loi + est bien interne puisque $P + Q$ est l'intersection d'une droite et de la courbe, c'est-à-dire un point de la courbe.

2/ La loi + est associative voir(FIG : 2.6). En effet, si P, Q et R sont trois points de la courbe,

on a :

$$\begin{aligned} P*(Q+R) &= P*(O*(Q*R)) \\ &= ((P*Q)*Q)*(O*(Q*R)) \quad \text{car} \quad P=(P*Q)*Q \\ &= ((P*Q)*O)*(Q*(Q*R) \\ &= ((P*Q)*O)*R \qquad \text{car } (Q*(Q*R)=R \\ &= (O*(P*Q))*R \quad \text{voir la figure précédent} \\ &= (P+Q)*R \end{aligned}$$

donc on a : $P*(Q+R)=(P+Q)*R$

En appliquant O_E sur les deux membres de l'égalité, nous trouvons

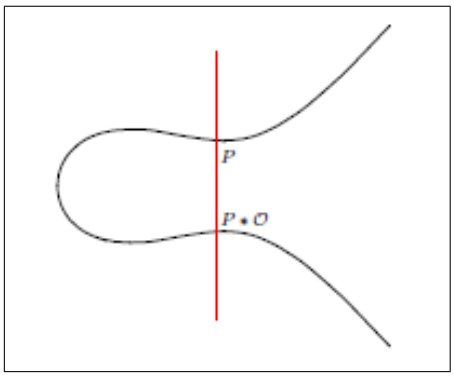
$$\begin{aligned} O_E *(P*(Q+R)) &= O_E *((P+Q)*R) \\ P+(Q+R) &= (P+Q)+R \qquad \text{car} \quad P+R=O_E *(P*R) \end{aligned}$$

3/L'éléement O_E est le neutre pour la loi $+$ (voir $FIG:2.7$). En effet :

$$P+O_E = O_E *(P*O_E)=P$$

et

$$O_E + P = O_E *(O_E *P)=P$$



$FIG:2.7-$ L'élément neutre de la loi de group.

4/Tout point P posséde un inverse pour la loi $+$. Vérifions que le point

$$-P=(O_E *O_E)*P$$

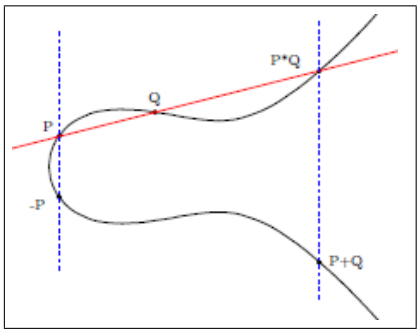
est bien l'inverse de P :

$$\begin{aligned}
P + (-P) &= O_E * (P * ((O_E * O_E) * P)) \\
&= O_E * (O_E * O_E) \quad \text{car } O_E * (P * O_E) = P \\
&= O_E + O_E = O_E \\
(-P) + P &= O_E * (((O_E * O_E) * P) * P) \\
&= O_E * (O_E * O_E) \\
&= O_E + O_E = O_E
\end{aligned}$$

5/Enfin la loi $+$ est commutative. Si P et Q sont deux points de la courbe :

$$P + Q = O_E * (P * Q) = (O_E * P) * Q = Q + P.$$

Les propriétés de la loi de groupe sur une courbe elliptique sont représentées sur la ($FIG : 2.8$)



$FIG : 2.8 -$ *La loi de groupe* $+$ *sur une courbe elliptique*

Chapitre 4

Quelques applications

Dans ce chapitre, on donne quelques applications des courbes elliptiques.

4.1 Théorème de Fermat

Proposition 7 (***petit théorème de fermat***)
Soit p un nombre premier. Tout entier a satisfait :

$$a^p \equiv a \,(\text{mod } p)$$

de plus si a n'est pas divisible par p alors

$$a^{p-1} \equiv 1 \,(\text{mod } p)\,.$$

Preuve. Considérons d'abord le cas ou p ne divise pas a, alors $a \in F_p^*$.
Par conséquent, nous avons

$$a^p \equiv a \,(\text{mod } p)$$
$$a^p = a + kp$$

donc on a

$$\begin{aligned} a^p &= a + kp \\ a^p - a &= kp \\ a\left(a^{p-1} - 1\right) &= kp \\ \left(a^{p-1} - 1\right) &= kp \qquad (\text{ car } p \text{ ne divise pas } a \text{ }) \\ a^{p-1} &= 1 + kp \\ a^{p-1} &\equiv 1 \,(\text{mod } p)\,. \end{aligned}$$

Si p divise a alors $a \equiv 0 \,(\text{mod } p)$, donc c'est trivial.

Ce théorème (**Fermat**) permet d'introduire la notion de nombres pseudo premiers.

Définition 28 *Un nombre est dit pseudo premier en base b est un nombre composé impair n qui se divise pas par b et tel que :*

$$a^{p-1} \equiv 1 \,(\text{mod } p)\,.$$

Théorème 2 (***Théorème d'Euler***)
Si p un nombre impair alors pour tout nombre x premier avec p,on a :

$$x^{\frac{(p-1)}{2}} \equiv 1 \,(\text{mod } p)\,.$$

Preuve. On a $x^{p-1} \equiv 1 \,(\text{mod } p)$.
Donc $x^{\frac{(p-1)}{2}}$ est une racine de l'équation suivante dans le corps F_p

$$X^2 - 1 = 0$$

car si on pose

$$x^{(p-1)^{\frac{2}{2}}} = X^2$$

donc on a

$$X^2 - 1 = 0$$

$$\begin{aligned} x^{(p-1)^{\frac{2}{2}}} - 1 &= 0 \\ x^{(p-1)^{\frac{2}{2}}} &= 1 \\ \sqrt{x^{(p-1)^{\frac{2}{2}}}} &= \sqrt{1} \\ x^{(p-1)^{\frac{1}{2}}} &= \pm 1 \\ x^{\frac{(p-1)}{2}} &= \pm 1. \end{aligned}$$

D'ou

$$x^{\frac{(p-1)}{2}} \equiv 1 \,(\text{mod } p) \text{ ou } x^{\frac{(p-1)}{2}} \equiv -1 \,(\text{mod } p)\,.$$

Montrons que l'ensemble des carrés de F_p^* coïncide avec les $x \in F_p^*$ tels que :

$$x^{\frac{(p-1)}{2}} = 1$$

Si x est un carré de F_p^*,

$$\begin{aligned} x = y^2 \text{ alors } & x^{(p-1)} = y^{(p-1)^2} \\ \Rightarrow & x^{\frac{(p-1)}{2}} = y^{\frac{(p-1)}{2}^2} \\ \Rightarrow & x^{\frac{(p-1)}{2}} = y^{(p-1)^{\frac{2}{2}}} \\ \Rightarrow & x^{\frac{(p-1)}{2}} = y^{(p-1)} = 1. \end{aligned}$$

Montrons que seuls les carrés de F_p^* sont tels que :

$$x^{\frac{(p-1)}{2}} = 1.$$

Tout d'abord ,il y a exactement $(p-1)/2$ carrés dans F_p^*. En effet,

$$a^2 = b^2 \Leftrightarrow a = b \text{ ou } a = -b.$$

De plus l'application

$$\begin{aligned} f: \quad F_p^* &\longrightarrow \{1, -1\} \\ x &\longrightarrow x^{\frac{(p-1)}{2}} \end{aligned} \tag{4.1}$$

est surjective. Et est un homomorphisme de groupe car :

$$x^{\frac{(p-1)}{2}} = \exp((p-1)/2(\ln x))$$

si on applique

$$\forall x, y \in F_p^*, \qquad f\,(x.y) = f\,(x) + f\,(y) \tag{4.2}$$

on va donne

$$\forall x, y \in F_p^*, \quad \exp((p-1)/2(\ln(x.y))) = \exp((p-1)/2(\ln(x) + \ln(y)))$$

donc on a la formule suivant si on applique

$$\forall x, y \in F_p^*, \qquad f\,(x+y) = f\,(x)\,.f\,(y) \tag{4.3}$$

$$\forall x, y \in F_p^*, \ \exp((p-1)/2(\ln(x)).\exp((p-1)/2(\ln(y))$$

donc est un homomorphisme de groupe. donc le noyau contient $(p-1)/2$ éléments car

$$\ker f \simeq F_p^* / \operatorname{Im} f$$

donc

$$| \ker f | = | F_p^* / \operatorname{Im} f | = (p-1)/2.$$

4.2 Factorisation d'un entier par les courbes elliptiques

4.2.1 Méthode $p-1$ de Pollard

Elle a été présentée par **J. M. Pollard en 1974**. Soit n un entier composé. Cette méthode probabiliste permet de déterminer les *diviseurs premiers* p de n, pour lesquels toute les *facteurs premiers* de $p-1$ sont inférieurs à un certain entier $A << n$. cela sinifie que $A!$ est un multiple de $p-1$.

Principe

Soit p un diviseur premier de n tel que les diviseurs premiers de $p-1$ soient inférieurs ou egaux a un certain entier A, avec des exposants pas trop grands.

Choisissons un entier a tel que $1 < a < n$.

On peut supposer que a est premier avec n, donc on a

$$\begin{aligned} a^{A!} \pmod{n} &= a^{k_1(p-1)} \pmod{n} \\ &= \left(a^{k_1} \pmod{n}\right)^{p-1} \pmod{n} \\ &= \left(a^{k_1} \pmod{n}\right)^{p-1} + k_2 n \quad \text{car} \quad a'^p = a' + kp' \text{ donc } a' = \left(a^{k_1} \pmod{n}\right)^{p-1} \end{aligned}$$

avec $k_1, k_2 \in \mathbb{Z}$. Et donc, d'après le **petit théorème de Fermat**

$$a^{A!} \pmod{n} = \left(a^{k_1} \pmod{n}\right)^{p-1} \pmod{n}$$
$$a^{A!} = \left(a^{k_1} \pmod{n}\right)^{p-1}$$
$$\textit{donc}$$
$$a^{A!} \equiv 1 \pmod{p}$$

et comme a est premier avec n . L'entier p est donc un facteur de $a^{A!}-1$. On choisir au hasard un nombre a, et de calculer $A!\,(\text{mod } n)$.

Si l'on a $pgcd\left(a^{A!}-1,n\right)\neq 1$, ce qui est pratiquement presque toujours le cas, on obtient un facteur non trivial de n , qui est un multiple de p, ce qui permet souvent d'obtenir p.

Algorithme $p-1$ de Pollard

1) On choisit un entier naturel A disons plus petit que 10^6.

2) On choisit un entier a tel que $1<a<n$ (par exemple $a=2$ ou $a=3$).

3) On calcule le $pgcd$ de a et n

$$pgcd\,(a,n)\,.$$

Si l'on a $pgcd(a,n)\neq 1$, on obtient un diviseur non trivial de n et l'algorithme est terminé.

4) Si l'on a $pgcd(a,n)=1$, on calcule $a^{A!}$ modulo n, puis l'entier

$$d=pgcd\left(a^{A!}-1,n\right).$$

Si l'on a $1<d<n$, alors d est un diviseur non trivial de n. Si $d=1$, on reprend à la première étape avec un plus grand entier A. Si $d=n$, on retourne a la première étape avec un plus petit entier A ou à la deuxième avec un autre entier a.

Exemple 21 *On a $n=1403$, Appliquent la Méthode $p-1$ de Pollard*

on prend $A=2$ *et évaluer*

$$2^{A!}\,(\text{mod } \textit{1403}) \quad \textit{pour} \quad A=2,3,4,...,$$

et on calcule

$$pgcd\left(2^{A!}-1,1403\right).$$

$pgcd\left(2^{2!}-1,1403\right)=1$ *donc est un facteur trivial, passer à la prochaine étape .*
$*Si$ $A=3$,
$2^{3!}=64$,

$$pgcd\left(2^{3!}-1,1403\right)=1$$

donc est un facteur trivial, passer à la prochaine étape .

$*Si\ A = 4,$
$2^{4!} = 142,$

$$pgcd\left(2^{4!} - 1, 1403\right) = 1$$

donc est un facteur trivial, passer à la prochaine étape .
$*Si\ A = 5,$
$2^{5!} = 794,$

$$pgcd\left(2^{5!} - 1, 1403\right) = 61$$

et nous truvons

$$1403 = 61 \times 23$$

donc l'algorithme s'arrète là .
61 *est un diviseur non triviale*

4.2.2 Factorisation par courbes elliptiques

Etape 1 : *choix d'une courbe elliptique*

On choisir une équation

$$y^2 = x^3 + ax + b\ définit\ une\ courbe\ elliptique$$

vérifiant

$$4a^3 + 27b^2 \neq 0$$

sur n'importe quel corps fini $\mathbf{F}_p$, pour cela il suffit de vérifier que

$$pgcd\left(4a^3 + 27b^2, n\right) = 1.$$

donc est premier avec n et premier avec p et est inversible dans $\mathbb{Z}/p\mathbb{Z}$. Tel que p un diviseur premier de n .

Etape 2 : *choix d'un point sur la courbe elliptique*

On choisit $P(x, y)$ sur la courbe elliptique E modulo n.

Etape 3 : *choix d'un entier auxiliaire*

On choisit A un entier pas très grand, mais qui est produit de petits facteurs premiers à des exposants déjà élevés.

Par exemple, $A = 2^{10}3^85^6$.

Etape 4 : *calcul sur les courbes elliptiques*

On calcule les coordonnées du point AP, en utilisant

$$x_3 = \left(-\frac{\frac{\partial f}{\partial x}(x_1, y_1)}{\frac{\partial f}{\partial y}(x_1, y_1)} \right)^2 - 2x_1$$
$$y_3 = \left(\lambda = -\frac{\frac{\partial f}{\partial x}(x_1, y_1)}{\frac{\partial f}{\partial y}(x_1, y_1)} \right)(x_1 - x_3) - y_1,$$

les calculs s'effectuant modulo n.

Il faut que le dénominateur d soit premier avec n. Si d n'est pas premier avec n, $pgcd(d, n)$ donne un diviseur premier de n.

4.3 Les crypto systèmes basés sur les courbes elliptiques

la cryptographie est de proposer des méthodes pour coder facilement de l'information de telle sorte que le décodage soit difficile si l'on ne possède pas la signature d'autentification adéquate comme dans la méthode **RSA** qui est un système de codage à clé publique de taille inferieure et utilise les courbes elliptiques.

4.3.1 La cryptographie à clé publique « le RSA »

La méthode de cryptographie **RSA** a été inventé en 1977 par Ron **R**ivest, Adi **S**hamir et Len **A**dleman .

Principe de fonctionnement :

Si **Bob** souhaite recevoir des messages en utilisant le **RSA** , il procède de la façon suivante :

∗**Création des clés :** **Bob** crée 4 nombres p, q, e et d :

1/ p et q sont deux grands nombres premiers distincts .

2/ On pose $n = pq$.

3/$z = (p-1)(q-1)$, e est un entier premier avec z tq :

$$1 < e < z.$$

4/ $(d \times e) \bmod z = 1$, On peut trouver d à partir de e, p et q, en utilisant l'algorithme d'Euclide.

5/ Distribution des clés :

♦$K_{pub} = (e, n)$ constitue la clé publique de **Bob.**

♦$K_{pri} = (d, n)$constitue sa clé privé.

∗**Envoi du message codé :**

Alice veut envoyer un message codé à *Bob*. Elle le représente sous forme d'un plusieurs entiers M (message en clair) compris entre 0 et $n - 1$.

Alice possède la clé publique K_{pub} de **Bob** .

Alice calcule $C = M^e \,(\text{mod } n)$, tq $C =$ message encrypté.

∗**Réception de message codé :**

Bob reçoit C et il le calcule grâce à sa clé privée

$$M = C^d \,(\text{mod } n)\,.$$

Il a donc reconstitué le message initial.

Exemple 22 ***Exemple 23*** *On a 2 nombres premiers p et q, tq $p = 11$, $q = 5$.*
donc on calcul n

$$n = pq = 11 \times 5 = 55.$$

On calcul

$$\begin{aligned} z &= (p-1)(q-1) \\ &= (11-1)\,(5-1) \\ &= 10 \times 4 \\ &= 40. \end{aligned}$$

On choisir e un entier premier avec z tq :

$$1 < e < z.$$

Donc $e = 7$,on calcul d à partir de $(d \times e) \bmod z = 1$, on a

$$\begin{aligned} (d \times e) \bmod z &= 1 \\ (d \times 7) \bmod 40 &= \boxed{1}, \end{aligned}$$

1/

$$\begin{aligned} 40x + 7y &= 1 \\ 40 &= 5\,(7) + 5 \\ 7 &= 1\,(5) + 2 \\ 5 &= 2\,(2) + \boxed{1} \end{aligned}$$

donc on a le reste $= 1$.

2/

$$\begin{aligned} 1 &= 5 - 2\,(2) \\ 1 &= 5 - 2\,(7 - 1\,(5)) \\ 1 &= 3\,(5) - 2\,(7) \\ 1 &= 3\,(40 - 5\,(7)) - 2\,(7) \\ 1 &= 3\,(40) - 17\,(7) \\ 1 &= 3\,(40) + \boxed{(-17)}\,(7) \end{aligned}$$

donc $d = 40 - 17 = 23$.

On a maintenant nos clés :

- *La clé publique est* $(e, n) = (7, 40)$ *(=clé d'encryptage).*
- *La clé privée est* $(d, n) = (23, 40)$ *(=clé de décryptage).*

Exemple 24 *crée* 2 *nombres* $p = 29$, $q = 37$,

On calcul $n = pq = 29 \times 37 = 1073$. *On calcul* z

$$z = (p - 1)(q - 1) = (29 - 1)(37 - 1) = 1008.$$

On prend $e = 71$.

On choisit tel que

$$71 \times d \bmod 1008 = 1$$

On trouve $d = 1079$.

On a maintenant nos clés :

- *La clé publique est* $(e, n) = (71, 1073)$ *(=clé d'encryptage).*
- *La clé privée est* $(d, n) = (1079, 1073)$ *(=clé de décryptage).*

On va encrypter le message 'HELLO' tq $M = 7269767679$. *Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que* n, n *comporte* 4 *chiffres, on va donc découper notre message en blocs de* 3 *chiffres :*

$$726\ 976\ 767\ 900$$

(on complète avec des zéros). Ensuite on encrypte chacun de ces blocs :

$$726^{71} \bmod 1073 = 436.$$

$$976^{71} \bmod 1073 = 822.$$

$$767^{71} \bmod 1073 = 825.$$

$$900^{71} \bmod 1073 = 552.$$

Le message encrypté est 436 822 *825* 552. *On peut le décrypter avec d :*

$$436^{1079} \bmod 1073 = 726.$$

$$822^{1079} \bmod 1073 = 976.$$

$$825^{1079} \bmod 1073 = 767.$$

$$552^{1079} \bmod 1073 = 900.$$

C'est à dire la suite de chiffre 726 976 767 900.
On retrouve notre message en clair 7269767679 *: 'HELLO'.*

4.3.2 L'échange de clés par les courbe elliptiques : schéma Diffie-Hellman

On a deux personnes **Alice** et **Bob** se mettent d'accord ensemble et publiquement sur une courbe elliptique E, c'est-à-dire qu'ils choisissent un corps fini $\Bbbk$ (par exemple, $\mathbb{Z}/p\mathbb{Z}$) et une courbe elliptique

$$y^2 = x^3 + ax^2 + b.$$

Ils choisissent aussi ensemble, et toujours publiquement, un point P situé sur la courbe.

Et pour constitue clé secrète il faut appliquent le schéma **Diffie-Hellman** qui procède de la façon suivante :

1/ Données publiques : E une courbe elliptique sur un corps fini $\mathbf{F}_p$ et un point $P \in E(\mathbf{F}_p)$ d'ordre suffisamment grand.

2/ Choix secret d'**Alice** : un entier a.

3/ Choix secret de **Bob** : un entier b.

4/ **Alice** envoie $P_a = aP$ à **Bob**.

5/ **Bob** calcule $P_b = bP$et l'envoie à **Alice.**

6/ **Alice** calcule $aP_b = abP$et **Bob** calcule $bP_a = abP$. La clé commune est une certaine fonction du même point abP.

Définition 29 *On appelle problème de Diffie-Hellman le problème suivant :*
étant donné P, aP et bP dans $E(\mathbf{F}p)$, trouver abP.

Exemple 25 *$E : y^2 = x^3 + ax^2 + b \pmod{17}$, une courbe elliptique sur un corps fini $\mathbf{F}_p$, $P = (5,1)$, $n = 19$.*
1/ On calcule $2P = P + P$ tq :

$$\lambda = \frac{(3x_P^2 + 2)}{2y_P} = \frac{(3(5^2) + 2)}{2(1)} = 77 \times 2^{-1} \equiv 9 \times 9 \equiv 13 \pmod{17}.$$
$$x_{2P} = \lambda^2 - 2x_P = 13^2 - 2(5) = 16 - 10 = 6 \equiv 6 \pmod{17}.$$
$$y_{2P} = \lambda(x_P - x_{2P}) - y_P = 13(5-6) - 1 = -13 - 1 = -14 \equiv 3 \pmod{17}.$$

Donc $2P = (6,3), 3P = (10,6), 4P = (3,1), 5P = (9,16), 6P = (16,13), 7P = (6,0), 8P = (13,7), 9P = (7,6), 10P = (7,11), 11P = (13,10), 12P = (0,11), 13P = (16,4), 14P = (9,1), 15P = (3,16), 16P = (10,11), 17P = (6,14), 18P = (5,16), 19P = (O_E)$.
*2/**Alice** elle est choisir un entier $a = 3$.*
*3/ **Bob** elle est choisir un entier $b = 9$.*
*4/ **Alice** calcule $P_3 = 3P = (10,6)$ et envoie à **Bob**.*
*5/ **Bob** calcule $P_9 = 9P = (7,6)$ et l'envoie à **Alice.***
*6/ **Alice** calcule $3P_9 = 3(9P) = 27P = 8P = (13,7)$ car $27 - 19 = 8$ et **Bob** calcule $9P_3 = 9(3P) = 27P = 8P = (13,7)$. Ce point de la courbe elliptique constitue leur clé secrète.*

Conclusion

dans ce mémoire nous avons abordé une notion générales sur la structure des courbes elliptiques comme étant un domaine de recherche trés vaste puisqu'il n'est pas resté sur les domaines des mathématiques ordinaires, et ne rester pas restrin sur l'algèbre ou de la géométrie, or il a pris un chemin trés utile envers d'autres domaines et encours d'améliorer le monde des technologies jusqu'a ce jour par le developpement des méthodes de cryptographie, les domaines de rebotique et les systèmes CAO dans l'industrie. on ne savait pas ou va ce domaine mais ce qu'on sait c'est que ce dernier va bien servire monde au future comme c'set le cas avec les autres branche des mathématques.

Bibliographie

[1] **Neal Koblitz :** Introduction to elliptic and moduler forms.

[2] **Peter L . Montgomery :** Speeding the pollard and elliptic curve method of factirisation.

[3] **Jean –Marc Couveignes, François Morain :** Théorie algorithmique des nombres.

[4] **Marc Joye :** Introduction élémentaire à la théorie des courbes elliptiques.

[5] **Serge Vaudenay, Jean Monnerat :** Factorisation de Grands Nombres à l'Aide de Courbes Elliptiques.

[6] **JOHANNES BUCHMANN :** La factorisation des grands nombres.

[7] **Abderrahmane NITAJ :** INTRODUCTION AUX COURBES ELLIPTIQUES.

[8] **Jean-Guillaume Dumas :** Factorisation d'entiers, cryptographie.

[9] **Alain Kraus :** Cours de cryptographie MM067 - 2012/13.