N° d'ordre :11/2012-M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET
DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
≪ HOUARI BOUMEDIENNE ≫
FACULTE DE MATHEMATIQUES

MEMOIRE
Présenté pour l'obtention du diplôme de MAGISTER
En : Mathématiques
Spécialité : Algèbre et Théorie des nombres
Par : Saadallah Fatiha

Sujet

LES COURBES ELLIPTIQUES ET LOGARITHME DISCRET

Soutenu publiquement le 27/11/2012, devant le jury composé de :

Mr-S.Rezaoui, Maitre de conférences à l' U.S.T.H.B Président.

Mlle- A. Laoudi, Maitre de conférences/A à l'U.S.T.H.B Directeur de MEMOIRE.

Mlle- F.Mamache, Maitre de conférences /A à l'U.S.T.H.B Examinateur.

Mr- D.Bahloul, Maitre de conférences /A à l'U.S.T.H.B Examinateur.

Remerciements

Je tiens à remercier monsieur S.Rezaoui Maitre de conférences à l' USTHB, d'avoir accepter de présider le jury de cette thèse.
J'adresse ma gratitude et ma profonde reconnaissance à madame Aini Laoudi, qui a accepté de rapporter ma thèse et m'avoir suivi tout au long de ce travail.
Je remercie également Messieurs :
Mlle- F.Mamache Maitre de conférences à l' USTHB.
Mr- D.Bahloul Maitre de conférences à l' USTHB.
de bien vouloir être membres du jury.
Je tiens aussi à remercier tous ceux qui m'ont aidé pour la réalisation de cette thèse.

Table des matières

Introduction

L'objet principale de ce mémoire est d'étudier quelques propriétés des courbes elliptiques sur les corps finis et leurs utilisations dans la résolution du logarithme discret. Il existe de nombreux ouvrages traitant les courbes elliptiques comme : Joseph H.Silverman (The arithmetic of elliptic curves) ; A.W.Knapp (Elliptic curves) ; J.W.Cassels (Introduction to the arithmetic theory of automorphic functions) ; Schoof.R (Elliptic curves over finite fields) ; R.I.Shafarevich (Basic algebric geometry) ; R.ed.Hartshorne (Algebraic geometry) etc...

Ainsi notre mémoire est organisée en trois chapitres :

Le premier chapitre est consacré à des rappels et notions nécessaires sur les extentions finis, les corps finis et les espaces algébriques pour la compréhension de notre mémoire. Dans le deuxième chapitre nous étudions les courbes elliptiques dans le cas général et les corps finis.

Dans le dernier chapitre on définira le logarithme discret dans le cas de courbes elliptiques et nous présentons des méthodes qui permettent de résoudre le problème du logarithme discret ; d'autre part à l'algorithme de Schoof, est une méthode de comptage de points d'une courbe elliptique définie sur un corps fini.

La thèse s'achève par une conclusion sur l'ensemble de travail réalisé et des perspectives de recherche.

Chapitre 1

Péliminaires

Dans ce chapitre, on se propose de faire quelques rappels sur des notions dont on aura besoin par la suite. Pour plus de précision on poura consulter [1] et [5].

1.1 Extensions de corps

Généralités :

Définition 1.1. *Si K et L sont des corps, on appelle morphisme de corps tout morphisme d'anneaux $f : K \longrightarrow L$ un tel morphisme est injectif et aussi appelé extension de K.*
Le degré de l'extension, noté $[L : K]$ est la dimension de L comme espace vectoriel sur K.

Définition 1.2. *Soit k et K deux corps, on dit que K est une extension de k si k est un sous-corps de K ; c'est une extension finie de k si le k-espace vectoriel K est de dimension finie. Le degré de l'extension est alors la dimension du k-espace vectoriel K.*

Proposition 1.1. *Si L est une extension finie de K de degré n et K une extension finie de k de degré m, L est une extension finie de k de degré nm.*

Proposition 1.2.

1. *Si K est un corps de caractéristique nulle, alors il existe une unique extension*

$$f : \mathbb{Q} \longrightarrow K$$

2. *Si K est un corps de caractéristique $p > 0$, alors il existe une unique extension*

$$f : \mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}} \longrightarrow K$$

Définition 1.3. *On dit que k est un corps de caractéristique 0 si f est injectif. On dit que k est un corps de caractéristique p si $Ker(f) = p\mathbb{Z}$.*

Définition 1.4. *L'extension K/k est finie si la dimension de K comme k-espace vectoriel est finie. Dans ce cas, on note : $[K : k] = dim_k K$.*

Exemple 1.1.

1. *Comme $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dim 2 alors $\mathbb{C}$ est une extension finie ; $\mathbb{C}/\mathbb{R}$ est une extension finie et on a $[\mathbb{C} : \mathbb{R}] = 2$*

2. *Si K est un corps, l'extension $K \subset K(X)$ n'est pas finie car $K(X)$ contient la famille libre infinie des X^n pour $n \in \mathbb{N}$.*

Théorème 1.1. [1]
Soit $j : E \longrightarrow F$ et $k : F \longrightarrow G$ deux extensions de corps, alors :
$(koj) : E \longrightarrow G$ est une extension finie si et seulement si $j : E \longrightarrow F$ et $k : F \longrightarrow G$ sont finies et l'on a alors la relation :

$$[F : E][G : F] = [G : E]$$

Définition 1.5. *Soit $j : E \longrightarrow F$ une extension de corps. Un élément $x \in F$ est dit algébrique sur E s'il existe un polynôme non nul $P \in E[X]$ tel que $P(x) = 0$. Dans le cas contraire, on dit que x est transcendant*

Exemple 1.2.

1. *Si $K = \mathbb{Q}$, le nombre $\sqrt{2}$ est algébrique, mais e et π sont transcendants.*
2. *$\mathbb{R}$ est une extension transcendante sur $\mathbb{Q}$.*
3. *$\mathbb{C}$ est algébrique sur $\mathbb{R}$.*

Extensions algébriques :

Définition 1.6. *Soit L/K une extension. Un élément x de L est dit algébrique sur K s'il existe un polynôme $P \in K[X]$, qui ne soit pas le polynôme nul, tel que $P(x) = 0$. Sinon on dit que x est transcendant sur K. L'extension L/K est dite algébrique (on dit aussi que L est algébrique sur K)si tout élément de L est algébrique sur K.*

Proposition 1.3. *L/K une extension et $x \in L$ alors :*
x est algébrique sur $K \Longleftrightarrow K[x]$ est K-espace vectoriel de dimension finie.

Exemple 1.3. *$\mathbb{C}/\mathbb{Q}$ une extension, $P(x) = x^2 + 1 \in Q[X]$.*

i racine de P, donc i algèbrique sur $\mathbb{Q}$

1.2 Corps finis

Caractéristique d'un corps fini :

Soit K un corps fini d'élément unité 1 et $\varphi_K : \mathbb{Z} \longrightarrow K$ le morphisme de groupes défini par :

$$n \in \mathbb{Z} : \varphi(n) = n.1$$

Le corps K étant fini, l'application φ ne peut être injective, elle n'est pas non plus identiquement nulle.
Son noyau est donc un sous-groupe non trivial de $\mathbb{Z}$, de la forme $p\mathbb{Z}$ avec $p \geqslant 2$.
Comme K est intègre, le noyau de φ_K est un idéal premier de $\mathbb{Z}$, c'est à dire que l'on a $Ker\varphi_K = \{0\}$ où $Ker\varphi_K = p\mathbb{Z}$, p étant un nombre premier.
Ce nombre p est appelé la caractéristique du corps K.

Définition 1.7. *Soient K un corps et $\varphi_K : \mathbb{Z} \longrightarrow K$ comme précédemment*

1. *Si $ker\varphi_K = \{0\}$, on dit que le corps K est de caractéristique 0 (au parfois infinie) ou d'exposant caractéristique 1.*

2. *Si $ker\varphi_K = p\mathbb{Z}$, où p est un nombre premier, on dit que K est de caratéristique P ou d'exposant caratéristique p.*

Exemple 1.4. *Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0 si p est un nombre premier, le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est de caractéristique p.*

Définition 1.8. *Un corps K est dit premier s'il n'a pas de sous corps autre que lui même (c'est-à-dire il n'est extension que de lui même).*

Théorème 1.2. *Soit K un corps fini à q éléments, de caractéristiques p.*

1. *Si n est la dimension de l'espace vectoriel K sur $\mathbb{F}_p$, on a $q = p^n$.*
2. *Tout $x \in K^*$ vérifie $x^{q-1} = 1$, ce qui implique $x^{-1} = x^{q-2}$.*
3. *Tout $x \in K$ vérifie $x^q = x$.*
4. *Dans l'anneau $K[X]$, on a l'égalité*

$$X^{q-1} - 1 = \prod_{a \in K^*}(X - a)$$

5. *Soit a un élément primitif de K. La famille*

$$B = \{1, a, a^2, ..., a^{n-1}\}$$

Est une base de l'espace vectoriel K sur $\mathbb{F}_p$, c'est-à-dire que tout élément $x \in K$ s'écrit d'une façon unique

$$x = R(a), \text{ avec } R \in \mathbb{F}_p[X]^{(n)}$$

Théorème 1.3. *Soit $\mathbb{F}$ un corps fini de caractéristique p, alors $\mathbb{F}$ est un $\mathbb{F}_p$ espace vectoriel de dimension finie (disons n). Donc : $|\mathbb{F}| = p^n$ où $|\mathbb{F}|$ désigne le cardinal de $\mathbb{F}$.*

Demonstration :
$\mathbb{F}$ est un $\mathbb{F}_p$ espace vectoriel et par hypothèse, $\mathbb{F}$ est fini donc la dimension de $\mathbb{F}$ en tant que $\mathbb{F}_p$ espace vectoriel est forcement finie. D'où $\sharp(\mathbb{F}) = (\sharp(\mathbb{F}))^n = p^n$.

Proposition 1.4. *Soit K un corps fini de caractéristique p :*

1. $\forall (x, y) \in K^2, (x+y)^p = x^p + y^p$
2. $\forall (x, y) \in K^2, \forall i \geq 2, (x+y)^{p^i} = x^{p^i} + y^{p^i}$
3. $\mathbb{F}_p = \{x \in K / x = x^p\}$
4. *Soit $Q \in K[X]$; on a l'équivalence :*

$$(Q \in \mathbb{F}_p[X]) \Longleftrightarrow ([Q(X)]^p = Q(x^p))$$

preuve :

1. On développe $(x+y)^p$ par la formule du binôme de Newton ; puis on remarque que pour tout entier $k = 1, ..., p-1$ le coefficient binomial C_K^p est divisible par p. Donc est nul dans $\mathbb{F}_p$.
2. Par recurence sur i d'aprés la question précédente.
3. Le groupe $\mathbb{F}_p^*$ est d'ordre $p-1$, tout élément $x \in \mathbb{F}_p^*$ vérifie donc $x^{p-1} = 1$ d'où $x^p = x$. Cette relation vérifiée par 0 ; donc :

$$\mathbb{F}_p \subset \{x \in K / x = x^p\}.$$

   Réciproquement :
   le polynôme $x^p - x$ possédant au plus p racines dans K ; on a l'inégalité :

$$\sharp\{x \in K / x = x^p\} \leq p$$

   d'où l'égalité $\mathbb{F}_p = \{x \in K / x = x^p\}$.
4. Soit $Q(x) = a_0 + a_1 x + ... + a_n x^n$; d'après 1 on a :

$$\begin{aligned}[Q(x)]^p &= a_0^p + a_1^p x^p + ... + a_n^p (x^p)^n \\ &= a_0 + a_1 x^p + ... + a_n (x^p)^n \\ &= Q(x^p)\end{aligned}$$

Corps algébriquement clôs, clôture algébrique :

Définition 1.9.

1. *Un corps commutatif L est algébriquement clôs si et seulement si tout polynôme à coefficients dans L a au moins une racine dans L.*
2. *Une clôture algébrique d'un corps commutatif K est une extension algébrique qui est algébriquement clôse.*

Exemple 1.5.

1. *Le corps des nombres complexes $\mathbb{C}$ est algébriquement clôs.*
2. *Les corps des rationnes $\mathbb{Q}$ et des réels $\mathbb{R}$ ne sont pas algébriquement clôs.*

Définition 1.10. *Soit $k \subset K$ une extension de corps et soit $P \in k[X]$ non constant. On dit que P est scindé dans $K[x]$, ou sur K si P se décompose dans $K[x]$ comme produit de facteurs du premier degré c-à-d :*

$$P = C(X - \alpha_1) \times (X - \alpha_2)...(X - \alpha_d)$$

avec $d = degP$; C est le coefficient dominant de P et les α_i sont dans K.

Lemme 1.1. *Si K est algébriquement clôs, tout $P \in K[X]$ non constant est scindé.*

Démonstration :

Par récurence sur $d = degP$.

Pour $d = 1$ c'est clair, supposons $d \geq 2$; et l'assertion établie en degré $< d$. Soit $P \in K[X]$ de degré d ; comme K est algébriquement clôs, P possède dans K au moins une racine α donc se factorise en $P = (X - \alpha)Q$ avec $Q \in K[X]$ de degré $d - 1$.

Par hypothèse de récurence , Q est scindé dans $K[X]$ et donc il en est de même de P.

1.3 Espaces algébriques

Les notions utilisées se trouvent dans des ouvrages de géometries algébriques [6], [8] et [10].

1.3.1 Espaces affines

Soit K un corps commutatif, et $\overline{K}$ sa clôture algébrique.

Définition 1.11. *On appelle espace affine de dimension n sur un corps commutatif K, l'ensemble des n-uplets d'éléments a_i de $\overline{K}$, noté $\mathbb{A}^n(\overline{K})$ où :*

$$\mathbb{A}^n(\overline{K}) = \{a = (a_1, a_2, ..., a_n); a_i \in \overline{K}\}$$

Les points K-rationnels de $\mathbb{A}^n$ sont les points de l'ensemble :

$$\mathbb{A}^n(K) = \{(x_1, ..., x_n) \in \mathbb{A}^n; x_i \in K\}.$$

Soit $\overline{K}[X] = \overline{K}[X_1, ..., X_n]$ l'anneau des polynômes à n variables et à coefficient dans $\overline{K}$ et $I \subset \overline{K}[X]$ un idéal; comme $\overline{K}[X_1, ..., X_n]$ est noetherien alors :
$I =< f_1, f_2, ..., f_k >$. On associe à I un sous-ensemble de $\mathbb{A}^n$ en posant :

$$V(I) = \{p = (a_1, ..., a_n) \in \mathbb{A}^n(\overline{K}) : f(p) = 0; \forall f \in I\}$$

Exemple 1.6.

1. *Si $n = 1$ alors : $\mathbb{A}^1(\overline{K})$ est la droite affine.*

2. *Si $n = 2$; $\mathbb{A}^2(\overline{K}) = \{(x, y) \in \overline{K^2}\}$ est le plan affine.*

Définition 1.12. *Un ensemble algébrique affine est un ensemble de la forme $V(I)$; où I est un idéal de $\overline{K}[X]$*

Exemple 1.7.

1. *Soient V_1 et V_2 deux ensembles*

   (a) $V_1 = \{(x, y) \in \mathbb{A}^2 / x^3 - y^3 = 1\} = V(x^3 - y^3 - 1)$.

(b) $V_2 = \{(x, y) \in \mathbb{A}^n / x^n + y^n = 1\} = V(x^n + y^n - 1)$.

donc : V_1 *et* V_2 *sont des ensembles algébriques.*

2. *Soient* $f(x) = x^2 - 1 \in \mathbb{C}[X]$ *et* $I =< f >$ *; alors :* $V(I) = \{-1, 1\}$.

3. *Soient* $K = \mathbb{F}_7, f(x) = x^2 - 1 \in \overline{K}[X]$ *; et* $I =< f >$ *alors :* $V(I) = \{1, 6\}$.

Définition 1.13. *Une courbe plane affine* C *est un ensemble de points* $P = (x, y) \in \mathbb{A}^2$ *dont les coordonnées vérifient une équation de la forme* $f(x, y) = 0$ *où* f *est un polynôme non constant de* $\overline{K}[x, y]$*, qu'on note* $C = V(f)$ *et le degré de* C *est le degré de* f.

$$C = V(f) = \{(x, y) \in \mathbb{A}^2 / f(x, y) = 0\}.$$

L'idéal de C *est donné par :*

$$I(C) = \{g \in \overline{K}[x, y] : g(P) = 0, \forall P \in C\}$$

La courbe $C = V(f)$ est définie sur K si $I(C)$ est engendré par des polynômes à coefficients dans K, dans ce cas on note C/K. Si C est définie sur K, l'ensemble des points K-rationnels de C est :

$$C(K) = C \bigcap \mathbb{A}^2(K).$$

Pour toute extension L de K contenue dans $\overline{K}$, l'ensemble des points L-rationnels de C est :

$$C(L) = C \bigcap \mathbb{A}^2(L).$$

À toute courbe plane affine C/K, on associe les idéaux $I(C/K) \subset K[x, y]$ et $I(C) \subset \overline{K}[x, y]$. Ils vérifient :

$$\begin{aligned} I(C/K) &= \{g \in K[x, y] : g(P) = 0; \forall P \in C\} \\ &= I(C) \bigcap K[x, y]. \end{aligned}$$

La courbe C est définie sur K si et seulement si :

$$I(C) = I(C/K)\overline{K}[x, y]$$

Définition 1.14. *Une courbe plane affine $C = V(f)$ est dite irréductible sur K lorsque son idéal $I(C/K) \subset K[x, y]$ est premier, lorsque C est irréductible sur $\overline{K}$, on dit qu'elle est absolument irréductible .*
Et plus généralement on appelle variété affine un ensemble algébrique affine V dont l'idéal associe $I(V) \subset \overline{K}[x_1, ..., x_n]$ est premier.

Définition 1.15. *Une courbe plane affine $C = V(f)$ est dite non-singulière en $P = (x_P, y_P) \in C$ si les dérivées partielles $\frac{\partial f}{\partial x}(x_P, y_P)$ et $\frac{\partial f}{\partial y}(x_P, y_P)$ ne sont pas simultanément nulles. On dit qu'une courbe est lisse si elle est non-singulière en chacun de ces points.*

Exemple 1.8. *:*
Etudions les courbes suivantes dans $\mathbb{R}$

1. *Soit $V_1 : y^2 = x^3 + x$; $V_1 \subset A^2(\mathbb{R})$.*

   Un point singulier de V_1 doit satisfaire :

   $\frac{\partial f(x,y)}{\partial x} = 3x^2 + 1 = 0$ *; pas de solution dans $\mathbb{R}$.*

   $\frac{\partial f(x,y)}{\partial y} = 2y = 0 \Longrightarrow y = 0.$

   qui n'a pas de solutions dans $\mathbb{R}$; donc V_1 est lisse.

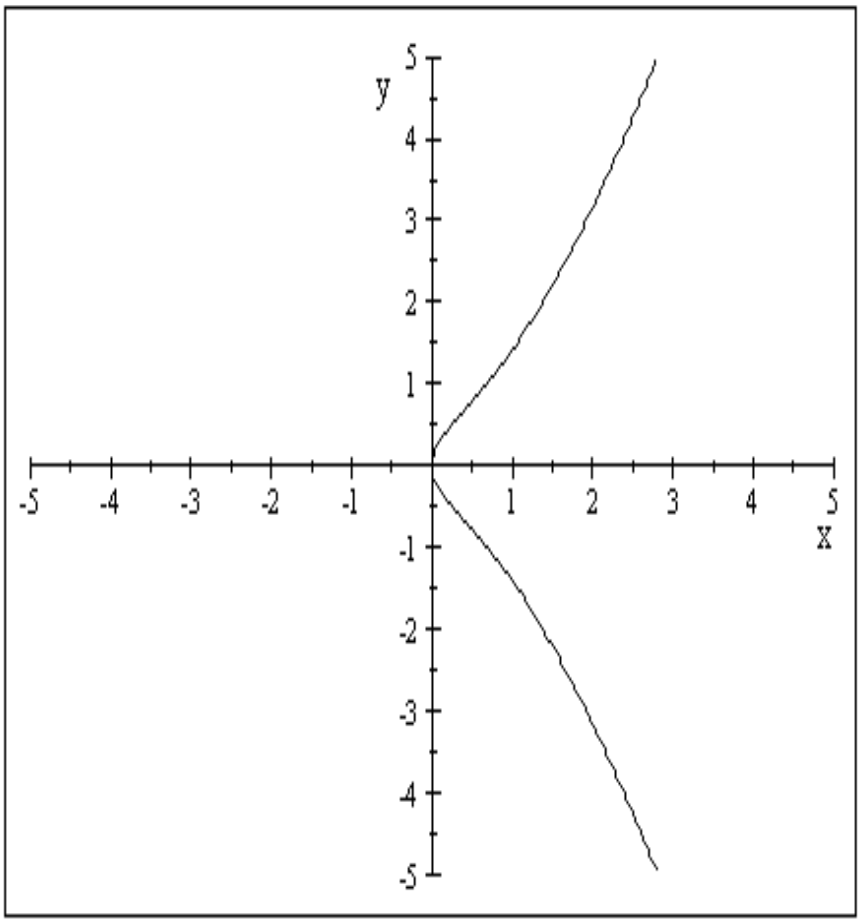

FIG. 1.1 – $E : y^2 = x^3 + x$

Soit $V_2 : y^2 = x^3 + x^2$ *;* $V_2 \subset \mathbb{A}^2(\mathbb{R})$.

Un point singulier de V_2 *doit satisfaire :*

$\frac{\partial f(x,y)}{\partial x} = 3x^2 + 2x = 0 \Longrightarrow x = 0$ *ou* $x = \frac{-2}{3}$.

$\frac{\partial f(x,y)}{\partial y} = 2y = 0 \Longrightarrow y = 0$.

Comme $(0,0) \in V_2$ *et* $(\frac{-2}{3}, 0) \notin V_2$ *; donc* V_2 *possède un unique point singulier* $(0,0)$.

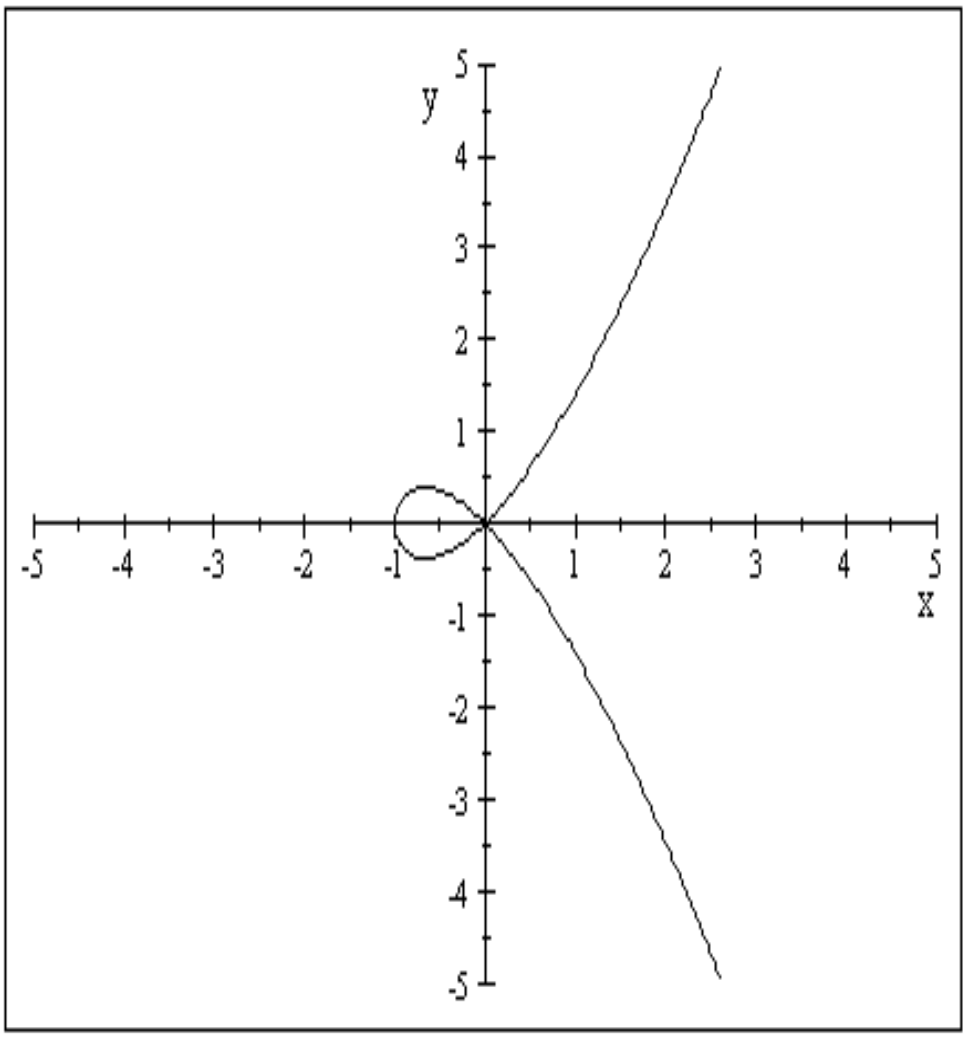

FIG. 1.2 – $E : y^2 = x^3 + x^2$

1.3.2 Espaces projectifs

Soit K un corps commutatif, et $\overline{K}$ sa clôture algébrique.

Définition 1.16. *Un espace projectif de dimension n sur K, noté $\mathbb{P}^n(K)$; est l'ensemble des classes d'équivalences de $(n+1)$ uplets $(a_1, ..., a_n)$ d'éléments de K, non tous nuls par la relation d'équivalence R :*

$$(x_1, ..., x_{n+1}) \ R \ (y_1, ..., y_{n+1}) \Longleftrightarrow \lambda \in \overline{K^*}/x_i = \lambda y_i \text{ ; pour } i = 0, ..., n+1.$$

Définition 1.17. *L'espace quotient de $\mathbb{A}^{N+1}(K) - \{(0, ..., 0)\}/R$ est l'espace projectif $\mathbb{P}^n(K)$ c.à.d :*

$$\mathbb{P}^n(K) = \{\mathbb{A}^{N+1}(K) - \{(0, ..., 0)\}/R\}.$$

Un élément de $\mathbb{P}^n(K)$ est appelé un point, si $P = (x_0 : x_1 : ... : x_n) \in \mathbb{P}^n(K)$.

Définition 1.18. *Soit $d \in \mathbb{N}$; un polynôme $f \in \overline{K}[x] = \overline{K}[x_0, ..., x_n]$ est dit homogène de degré d si :*

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n) \text{ ; pour tout } \lambda \in \overline{K}.$$

Un idéal de $\overline{K}[X]$ est dit homogène s'il est engendré par des polynômes homogènes .
Soit I un idéal homogène de $\overline{K}[X]$, notons $V(I)$ l'ensemble :

$$V(I) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ ; pour tout polynôme homogène } f\} \subset \mathbb{P}^n.$$

Un ensemble algébrique projectif est un ensemble de la forme $V(I)$; où I est un idéal homogène.

Définition 1.19. *Une courbe plane projective C est un ensemble de points*
$P = (X : Y : Z)$ de $\mathbb{P}^2$ dont les coordonnées homogènes vérifient une équation de la forme : $F(X, Y, Z) = 0$ où F est un polynôme homogène non constant de $\overline{K}[x, y, z]$; on note $C = V(F)$.
Si C est une courbe plane projective, l'idéal (homogène) de C est l'ensemble :

$$I(C) = \{g \text{ polynôme homogène de } \overline{K}[x, y, z] \text{ tel que pour tout ; } P = (x_P : y_P : z_P) \in C, \text{ on a : } g(x_P, y_P, z_P) = 0\}.$$

Remarque 1.1. *Une courbe de $\mathbb{P}^2(K)$ est l'ensemble des points (x, y, z) qui vérifient : $F(x, y, z) = 0$, où F est un polynôme de degré d, d est le degré de la courbe.*
On dit que cette courbe irréductible si F n'est pas produit de deux polynômes de degrés inférieurs à d.

Définition 1.20. *Un ensemble algébrique V est dit défini sur K si $I(V)$ peut être engendré par des polynômes homogènes à coefficients dans K. On le note alors V/K. Soit V un ensemble algébrique défini sur K ; on définit les points K-rationnels de V par :*

$$K(V) = V \bigcap \mathbb{P}^n(K).$$

Exemple 1.9.

(a) $\mathbb{P}^1(\mathbb{R})$ *est un cercle : c'est la droite réelle à laquelle on a ajouté un point à l'infini.*

(b) $\mathbb{P}^1(\mathbb{C})$ *est la sphère de Riemann, c'est le plan complexe auquel on a ajouté un point à l'infini, le même pour toutes les directions.*

(c) $\mathbb{P}^2(\mathbb{R})$ *est le plan projectif réel.*

Chapitre 2

Les courbes elliptiques

Dans ce chapitre, on rappelle quelque resultats sur les courbes elliptiques.
Pour plus de précision on poura consulter [3] ;[5] ou [6].

2.1 Définitions et préliminaires

Définition 2.1. *Une courbe elliptique est le couple (E, O_E) où E est une courbe plane projective lisse de genre 1 munie d'un point sur K-rationnel.*

Proposition 2.1. *Une courbe elliptique E définie sur K est une courbe lisse donnée par une équation de Weierstrass du type :*

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

où les coefficients a_1, a_2, a_3, a_4 et a_6 sont dans K et $\Delta \neq 0$ où Δ est le discriminant de la courbe est calculée par les équations suivantes :

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$
$$b_2 = a_1^2 + 4a_2.$$
$$b_4 = 2a_4 + a_1a_3.$$
$$b_6 = a_3^2 + 4a_6.$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Une courbe donnée par une telle équation est dite lisse si le système suivant n'admet pas de solution

$$\begin{cases} a_1y = 3x^2 + 2a_2x + a_4\,; \\ \\ 2y + a_1x + a_3 = 0\,; \end{cases}$$

Autrement dit : si les dérivées partielles en x et en y de
$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ *ne s'annulent pas en même temps.*

Une courbe elliptique E définie sur K est une courbe lisse donnée par une équation de Weierstrass définie sur K à laquelle on rajoute un point à l'infini noté O_E

$$E = \{(x,y) \in \overline{K^2}/y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O_E\}.$$

Si la caractéristique de K est differente de 2 ou 3 alors en faisant les deux changements de variables successifs :
$y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$, *ensuite* $(x,y) \longrightarrow (\frac{x-3b_2}{36}; \frac{y}{216})$ *dans E où, nous obtenons :*

$E : y^2 = x^3 - 27c_4x - 54c_6$ *avec :*

$$c_4 = b_2^2 - 24b_4.$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Définition 2.2. *On appelle j-invariant de la courbe elliptique E la quantité*

$$j(E) = \frac{c_4^3}{\Delta}.$$

Nous pouvons toujours travailler avec les courbes elliptiques de la forme :

$$E : y^2 = x^3 + Ax + B$$

Donc :

$$\Delta = -16(4A^3 + 27B^2).$$

Théorème 2.1. *Soit E une courbe donnée par une équation de Weierstrass. Alors E est non singulière ou lisse si et seulement si $\Delta \neq 0$.*

Démonstration :

$\Longleftarrow$)Supposons par l'absurde que E soit singulière en un point $P_0 = (x_0, y_0)$. Par le changement de variables $(x,y) \longrightarrow (x - x_0, y - y_0)$ nous nous ramenons au point $(0,0)$; où $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$.
alors on a : $a_6 = f(0,0)$; $a_4 = \frac{\partial f}{\partial x}(0,0) = 0$; $a_3 = \frac{\partial f}{\partial y}(0,0) = 0$ donc l'équation de la courbe E est :
$E : f(x,y) = y^2 + a_1xy - x^3 - a_2x^2 = 0$ *le discriminant est nul ce qui contre dit l'hypothèse.*

Il reste à montrer que le point infini 0_E est non singulier on a :
$0_E = (0,1,0)$ *et* $f(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$
$\frac{\partial f}{\partial z}(0,1,0) = y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2$; $\frac{\partial f}{\partial z}(0,1,0) = 1 \neq 0$ *donc c'est un point non singulier.*
$\Longrightarrow$ *Supposons que* $p \neq 2,3$ *; E la courbe donnée par l'équation de Weierstrass* $E : y^2 = x^3 + a_4x + a_6$. *Si la courbe est singulière en un point* $P_0(x_0,y_0)$ *cela signifie que* $2y_0 = 0 \Longrightarrow y_0 = 0$ *et* $3x_0^2 + a_4 = 0 \Longrightarrow x_0^2 = \frac{-a_4}{3} = 0$ $P_0 \in E$ *par conséquent* $y_0^2 = 0 = x_0^3 + a_4x_0 + a_6 = \frac{2}{3}a_4x_0 + a_6 \Longrightarrow x_0^2 = \frac{9a_6^2}{4a_4^2} = \frac{-a_4}{3} \Longrightarrow \triangle = 0.$

■

Le graphe d'une courbe elliptique peut prendre deux formes :

1. *Si le discriminant est positif, il présente deux composantes. Ce cas qui correspond au fait que le polynôme cubique* $x^3 + ax + b$ *a exactement trois racines réelles distinctes, elles donnent les abscisses des trois points de la courbe elliptique sur l'axe des* x.

Exemple 2.1. *Soit* $E : y^2 = x^3 - x$ *une courbe elliptique .*
On a $\triangle = -16(4a^3 + 27b)$ *;* $\triangle = 16 > 0$
donc le polynôme $x^3 - x$ *a exactement trois racines réelles distinctes.*
$x^3 - x = x(x-1)(x+1)$.

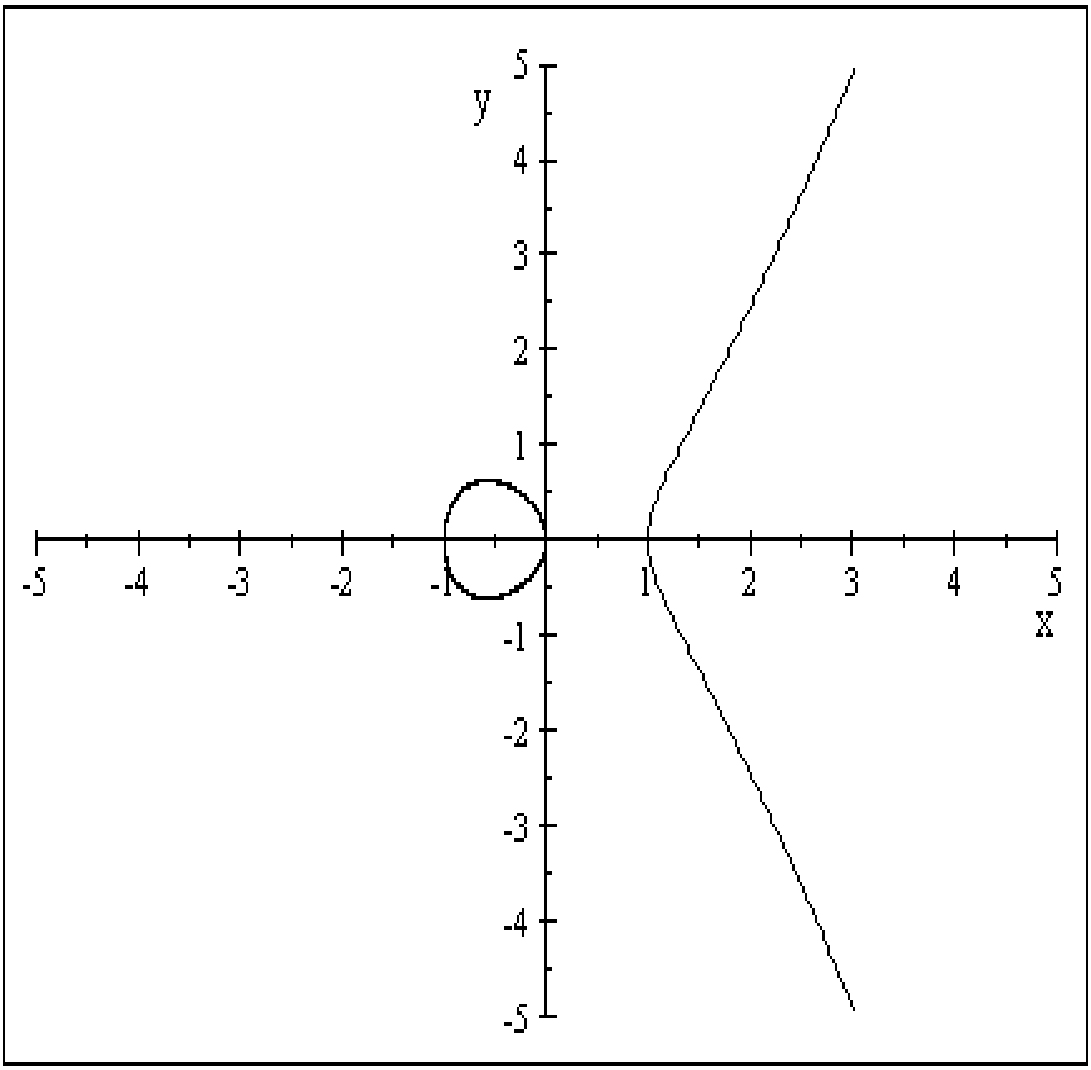

FIG. 2.1 – $E : y^2 = x^3 - x$

2. *Si le discriminent est négatif, il présente une seule composante. Ce cas correspond au fait que le polynôme cubique x^3+ax+b a exactement une racine réelle ; elle donne l'abscisse du point de la courbe elliptique sur l'axe des x.*

Exemple 2.2. *Soit E : $y^2 = x^3 - x + 1$ une courbe elliptique.*
On a $\triangle = -368 < 0$; donc le polynôme $x^3 - x + 1$ a exactement une racine réelle.

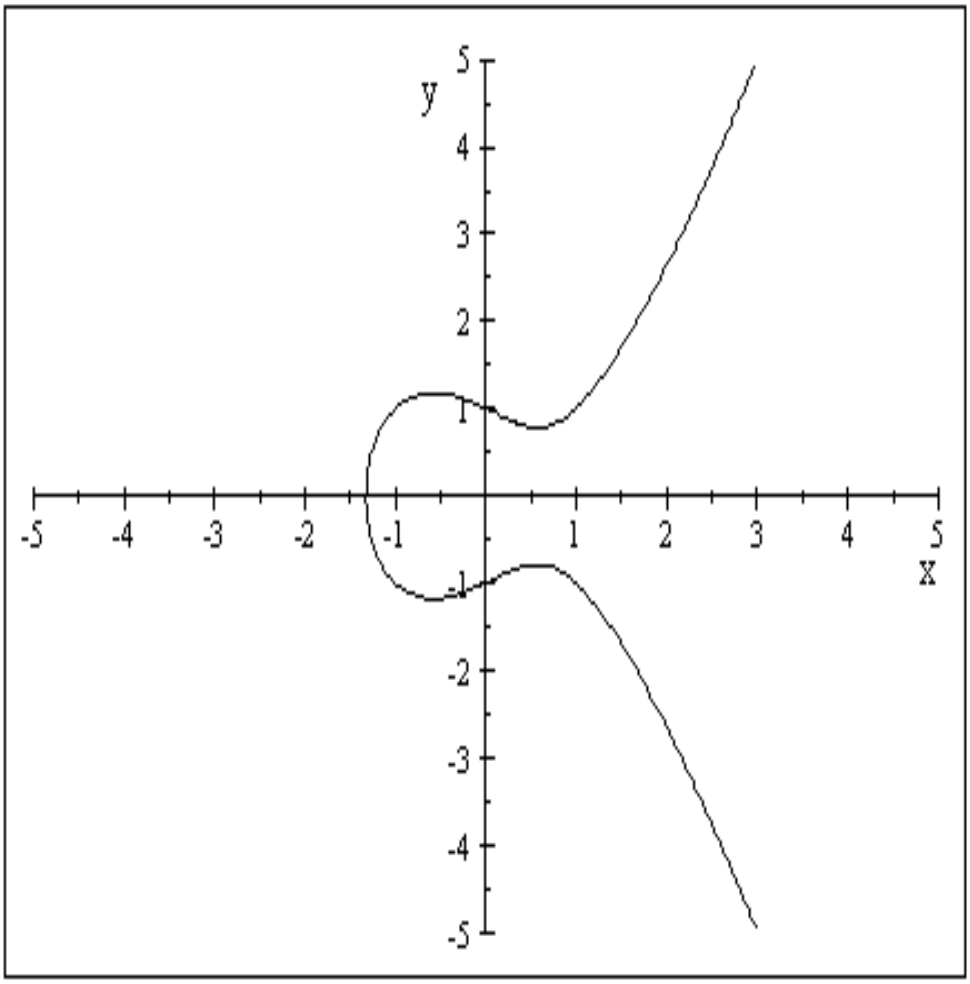

FIG. 2.2 – $E : y^2 = x^3 - x + 1$

K un corps de caractéristique p. E une courbe donnée par une équation de Weierstrass (1) définie sur K alors :

1. *Si $p \neq 2$ et $p \neq 3$:*
   $E : y^2 = x^3 + a_4x + a_6$.
   $\Delta = -16(4a_4^3 + 27a_6^2)$ *et* $j(E) = 1728(4a_4^3/(4a_4^3 + 27a_6^2))$.
2. *Si $p = 2$ et $j(E) \neq 0$:*
   $E : y^2 + xy = x^3 + a_2x^2 + a_6$; $\Delta = a_6$ *et* $j(E) = \frac{1}{a_6}$.
3. *Si $p = 2$ et $j(E) = 0$:*
   $E : y^2 + a_3y = x^3 + a_4x + a_6$; $\Delta = a_3^4$.
4. *Si $p = 3$ et $j(E) \neq 0$:*
   $E : y^2 = x^3 + a_2x^2 + a_6$; $\Delta = -a_2^3a_6$ *et* $j(E) = \frac{-a_2^3}{a_6}$.
5. *Si $p = 3$ et $j(E) = 0$:*
   $E : y^2 = x^3 + a_4x + a_6$; $\Delta = -a_4^3$.

Définition 2.3. *l'ensemble $E(K)$ des points d'une courbe elliptique E définie sur un corps K est donné par :*
$E(K) = \{(x, y, z) \in \mathbb{P}^2(K), y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\} \cup \{0_E\}$
un seul point correspond à $z = 0$, il s'agit de $0_E = (0, 1, 0)$ appelé point à l'infini

2.2 Loi de groupe

Proposition 2.2. *L'ensemble $E(K)$ des points rationnels d'une courbe elliptique E, muni de la loi de composition déterminée par la règle géométrique de trois points colinéaires de la courbe E est un groupe abélien qui vérifie les propriétés suivantes :*

1. *la loi est interne, $\forall P, Q \in E : P + Q \in E$.*
2. *Pour tout point $P = (x_p, y_p)$ de $E(K)$:*

$$P + 0_E = 0_E + P = P.$$

3. *la commutativité de la loi $\forall P, Q \in E : P + Q = Q + P$.*
4. *l'associativité : $\forall P, Q, R \in E : (P + Q) + R = P + (Q + R)$.*

L'addition de deux points est mieux expliquée géométriquement. Soient $P = (x_1, y_1)$ *et* $Q = (x_2, y_2)$ *deux points distincts d'une courbe elliptique* E*, alors la somme* R *de* P *et de* Q *est définie de la manière suivante :*

On commence par tracer une droite passant par les points P *et* Q*, cette droite coupe la courbe elliptique en un troisième point. Enfin* $R = P + Q$ *est le symétrique de ce point par rapport à l'axe des* x*.*

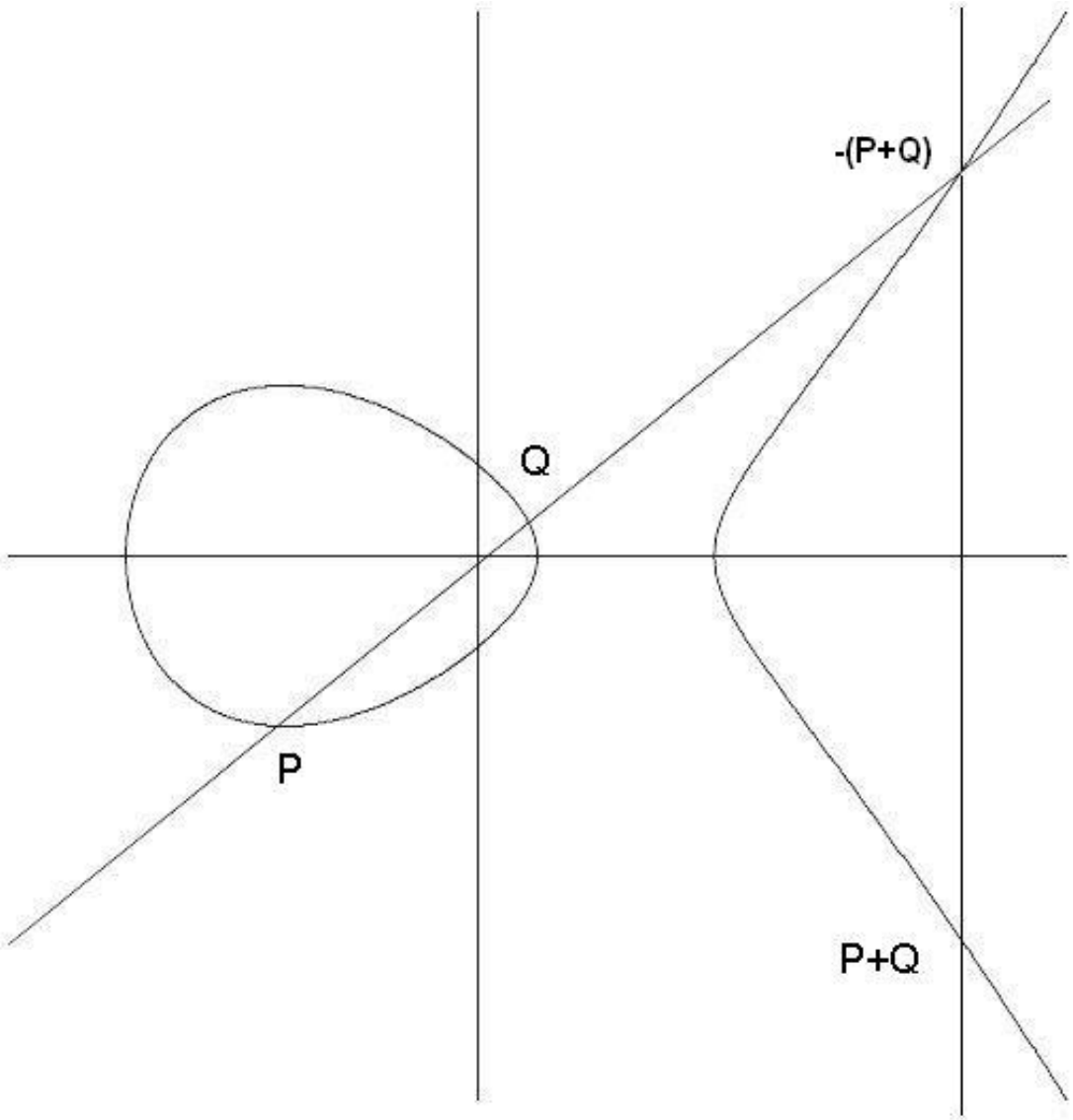

FIG. 2.3 – Addition de deux points sur $\mathbb{R}$

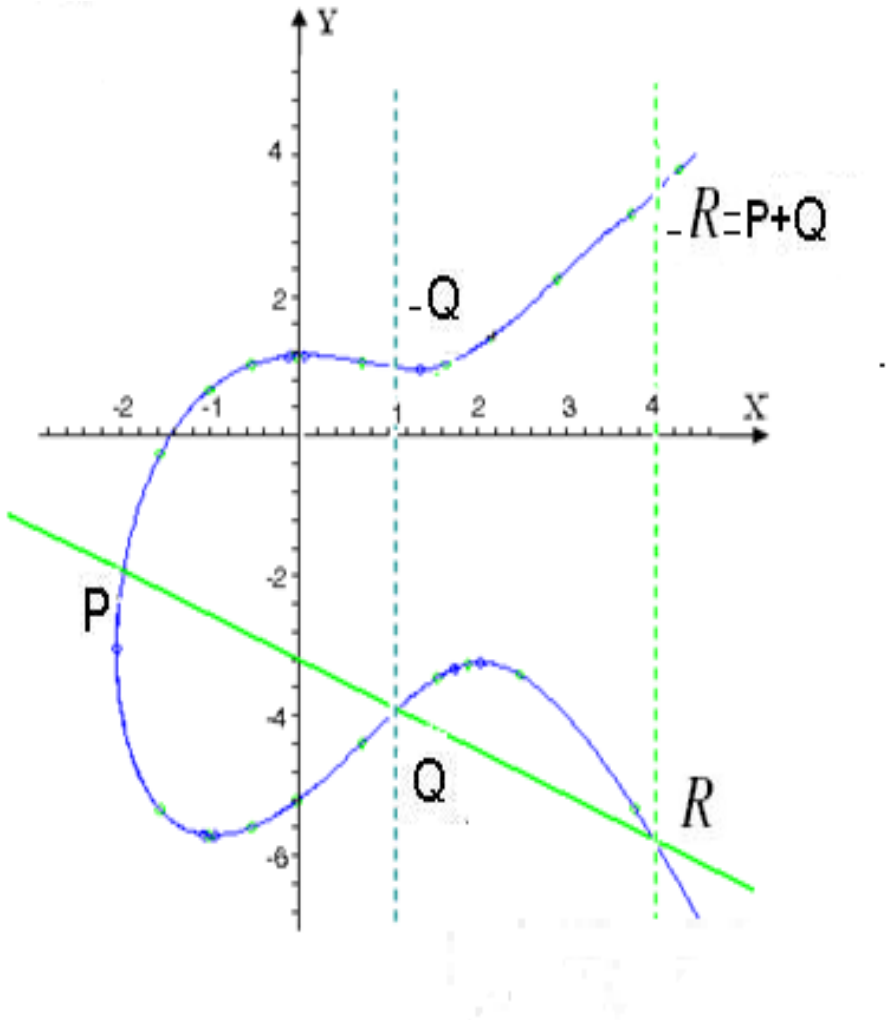

FIG. 2.4 – Addition de deux points sur $\mathbb{R}$

Le double $R = 2P$ de P est défini de la manière suivante :
On commence par tracer la tangente au point P. Cette droite coupe la courbe en un deuxième point dont on prend le symétrique par rapport à l'axe des x.

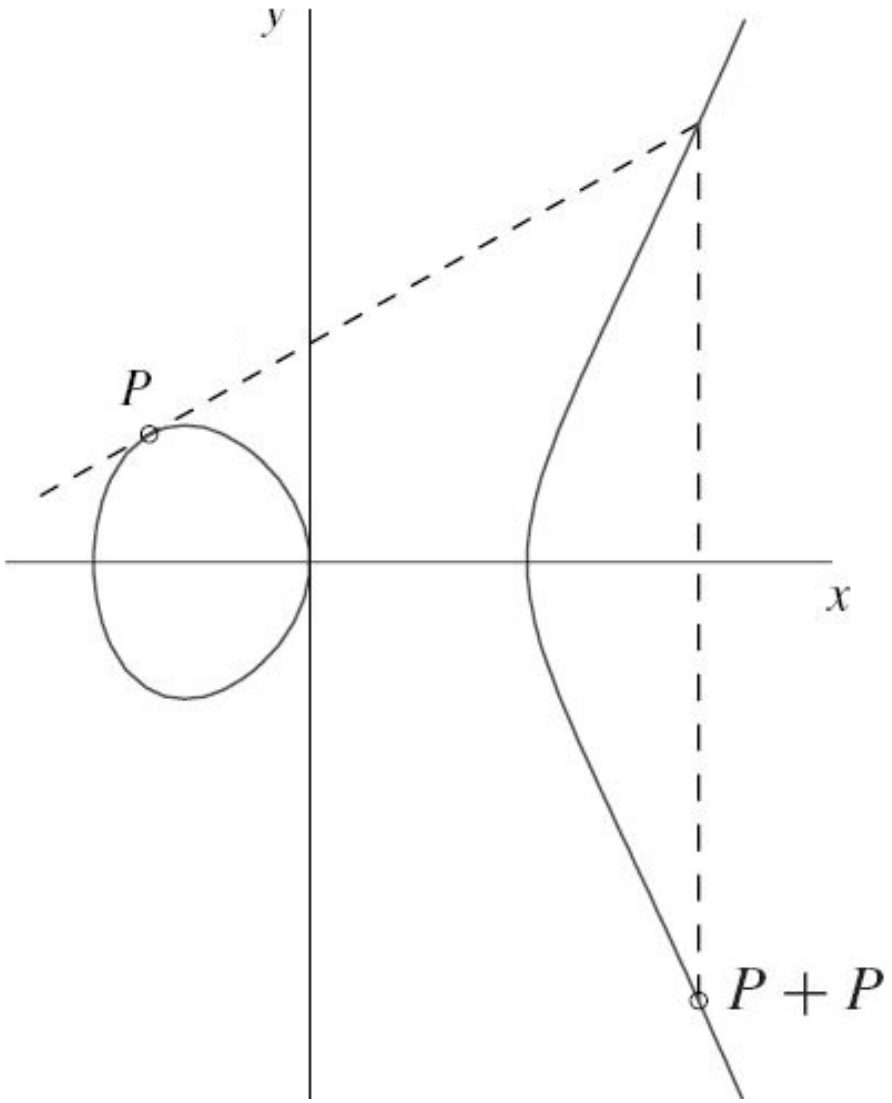

FIG. 2.5 – Doublement de point sur $\mathbb{R}$

Formules explicites :
L'inverse d'un point $P = (x_P, y_P)$ *:*

le point $-P = (x, y)$ *est l'intersection de la courbe* E *par la parallèle à oy passant par* P *l'équation de cette parallèle passant par* P *est :* $x = x_p$
L'ordonnée de $-P$ *est racine de l'équation :*

$$y^2 + a_1 x_p y + a_3 y = x_p^3 + a_2 x_p^2 + a_4 x_p + a_6. \ldots\ldots (1)$$

et comme cette équation en y *du* $2^{\text{ème}}$ *degré elle admet 2 racines distincts* y_p *et* y *leur somme est égal à :*

$$y + y_p = -(a_1 x_p + a_3)$$

donc

$$y = -y_p - a_1 x_p - a_3$$

Alors l'inverse $-P$ *du point* P *est :*

$$-P = (x, -y_p - a_1 x_p - a_3)$$

Addition des points $P = (x_P, y_P)$ ***et*** $Q = (x_q, y_q)$ *:*

1^{er} ***cas :***
Si $x_P = x_q$ *et* $y_q = -a_1 x_P - y_P - a_3$
Dans ce cas, la droite sécante qui joint les deux points est verticale, donc le troisième point d'intersection de cette sécante avec la courbe est le point à l'infini c'est-à-dire : $P + Q = 0_E$.
$2^{\text{ème}}$ ***cas :***

Notons $R = (x, y)$ *la somme de* P *et de* Q*, supposons que* $y_q \neq -a_1 x_p - y_p - a_3$.

1. *Si* $x_p \neq x_q$ *posons :* $\lambda = \frac{y_q - y_p}{x_q - x_p}$ *et* $\gamma = y_p - \lambda x_p$.
   La droite qui passe par les points P *et* Q *a pour équation* $y = \lambda x + \gamma$*. (le nombre* λ *est bien sa pente). On peut calculer l'intersection de cette droite avec* E*, on trouve trois solutions : les points* $P = (x_p, y_p)$*,* $Q = (x_q, y_q)$ *et un troisième point* $R = (x_R, y_R)$ *tel que :*

$$x_R = -a_2 + \lambda^2 + a_1\lambda - x_p - x_q.$$
$$y_R = -(\lambda + a_1)x_R - \gamma - a_3.$$

2. *Si* $x_p = x_q$ *alors* $p = q$
   L'addition de P *et de* Q *revient alors à doubler le point* P.

Doublement du point $p = (x_p, y_p)$ ***:***

La formule vue ci-dessus reste valable si ce n'est que maintenant λ *représente le coefficient angulaire de la tangente à la courbe en* P *:*

$\lambda = \frac{\partial y}{\partial x}|_p = \frac{\frac{\partial f}{\partial x}(x_p,y_p)}{\frac{\partial f}{\partial y}(x_p,y_p)} = \frac{3x_p^2+2a_2x_p+a_4-a_1y_p}{2y_p+a_1x_p+a_3}$. *et* $\gamma = y_p - \lambda x_p$ *donc :*

$$2P = (x^{'}, y^{'}) = (-a_2 + \lambda - 2x + a_1\lambda, -(\lambda x + \gamma) - a_1x^{'} - a_3)$$

Exemple 2.3. *Soit* $E : y^2 = x^3+x+1$ *une courbe définie sur* $\mathbb{F}_{23}$. *E est une courbe elliptique car on a :* $\Delta = -16(4a_4^3 + 27a_6^2) = -16(31) \neq 0$ *donc la courbe bien définie. Les seules points de cette courbe sont :*

$(0,1); (0,22); (1,7); (1,16); (3,10); (3,13); (4,0); (5,4); (5,19); (6,4); (6,19);$
$(7,11); (7,12); (9,7); (9,16); (11,3); (11,20); (12,4); (12,19); (13,7); (13,16);$
$(17,3); (17,20); (18,3); (18,20); (19,5); (19,18)$ *; plus le point à l'infini* 0_E.

1- Prenons $P = (18,20)$ *et* $Q = (17,3)$. *Calculons* $R = P + Q$ *:*
On a $\lambda = 17 \in \mathbb{F}_{23}, \gamma = 13 \in \mathbb{F}_{23}, x_R = 1 \in \mathbb{F}_{23}$ *et* $y_R = 16 \in \mathbb{F}_{23}$.

Donc $R = (1,16) \in \mathbb{F}_{23}$.

2- Maintenant, calculons $R = 2P$ *avec* $P = (6,4)$
$\lambda = 5 \in \mathbb{F}_{23}, \gamma = 20 \in \mathbb{F}_{23}, x_R = 13 \in \mathbb{F}_{23}$ *et* $y_R = 7 \in \mathbb{F}_{23}$,
d'où $2(6,4) = (13,7) \in \mathbb{F}_{23}$.

Exemple 2.4. *Soit* E *une courbe elliptique définie sur* $\mathbb{F}_5$ *par* $E : y^2 = x^3 - 1$.
On a $E(\mathbb{F}_5) = \{0, (1,0), (3,1), (0,2), (0,3), (3,4)\}$.
On prend $P = (3,1)$, $Q = (0,3)$ *et on calcule* $R = P + Q$ *;*
$\lambda = 1 \in \mathbb{F}_5, \gamma = x_R = 3 \in \mathbb{F}_5$ *et* $y_R = 4 \in \mathbb{F}_5$,
d'où $R = (3,4) \in \mathbb{F}_5$.

Les points d'ordre 2 et 3 *:*

1. *Soit E une courbe elliptique $E : y^2 = x^3+a_2x^2+a_4x+a_6$. Cherchons les points $P = (x, y)$ tel que $P \neq 0$ et $2P = 0$.*
   On a : $2P = 0 \Longleftrightarrow 2P - P = -P \Longleftrightarrow P = -P$
   c.à.d $(x, y) = (x, -y - a_1x - a_3)$ et comme $a_1 = a_3 = 0$ alors $(x, y) = (x, -y)$.
   On a $y = -y \Longrightarrow 2y = 0 \Longrightarrow y = 0 \Longrightarrow x^3 + a_2x^2 + a_4x + a_6 = 0$.
   Dans $\overline{K}$ il y a trois racines de ce polynôme, donc il y a trois point d'ordre 2.

   Exemple 2.5. *1- Soit E_1 une courbe elliptique tel que $E_1 : y^2 = x^3 - x$.*
   Déterminons le nombre de points d'ordre 2 dans $E(\mathbb{R})$?
   On a $\Delta = 16 \times 4 \neq 0$, donc E_1 est bien une courbe elliptique dans $\mathbb{R}$, P est d'ordre 2 $\Longleftrightarrow y = 0 \Longleftrightarrow x^3 - x = 0 \Longleftrightarrow x(x^2 - 1) = 0 \Longleftrightarrow x(x - 1)(x + 1) = 0$.
   D'où le polynôme $f(x) = x^3 - x$ admet trois racines réelles.
   donc $E(\mathbb{R})$ a trois points d'ordre 2 sont : (0,0) ; (-1,0) ; (1,0).

   2- Soit $E_2 : y^2 = x^3 + 1$ une courbe elliptique.
   Combien de points d'ordre 2 dans $E(\mathbb{R})$ et $E(\mathbb{C})$?
   On a $\Delta = -4 \times 27 \neq 0$, donc E_2 est bien une courbe elliptique P est d'ordre 2
   $x^3 + 1 = 0 \Longleftrightarrow (x + 1)(x^2 - x + 1) = 0$
   Le polynôme $g(x) = x^3 + 1$ admet une seule racine réelle, donc $E(\mathbb{R})$ a un seul point d'ordre 2 est $(-1, 0)$; et $E(\mathbb{C})$ a trois points d'ordre 2 sont $(-1, 0); (\frac{1+i\sqrt{3}}{2}, 0); (\frac{1-i\sqrt{3}}{2}, 0)$

2. *Soit $E : y^2 = x^3 + ax^2 + bx + c$ une courbe elliptique.*
   $P = (x, y)$ est un point d'ordre 3 $\Longleftrightarrow 3P = 0 \Longleftrightarrow 3P - P = -P \Longleftrightarrow 2P = -P$. on a :$-P = (x, -y)$ et

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

   et comme $x(2P) = x(-P) = x(P)$ donc :

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x$$

   C'est-à-dire : $3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$
   On pose $\Psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$; donc P est un point d'ordre $3 \Longleftrightarrow \Psi_3(x) = 0$, le polynôme Ψ_3 a au plus 4 racines.

2.3 Algorithme de base d'addition, l'opposé et doublement

On se propose de donner quelques algorithmes qui permettent le calcul de l'addition ,l'opposé et doublement de points :

1. Addition basique de deux points :

Entrées : $P = (x_p, y_p)$ *et* $Q = (x_q, y_q)$ *qui appartiennent à* $E(\mathbb{F})$ *et* $a_1, a_2, a_3 \in E(\mathbb{F})$
Sorties : $R = P + Q = (x_R, y_R) \in E(\mathbb{F})$.
Début
$\lambda \longleftarrow \frac{y_q - y_p}{x_q - x_p}$;
$\gamma \longleftarrow y_p - \lambda x_p$;
$x_R \longleftarrow -a_2 + \lambda^2 - x_p - x_q + a_1\lambda$;
$y_R \longleftarrow -(\lambda + a_1)x_R - \gamma - a_3$;
retourner (x_R, y_R);
Fin

2. Doublement basique d'un point :

Entrées : $P = (x, y) \in E(\mathbb{F})$ *et* $a_1, a_2, a_3, a_4 \in E(\mathbb{F})$
Sorties : $2P = (x', y') \in E(\mathbb{F})$.
Début
$\lambda \longleftarrow \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$;
$\gamma \longleftarrow y - \lambda x$;
$x' \longleftarrow -a_2 + \lambda - 2x + a_1\lambda$;
$y' \longleftarrow -(\lambda x + \gamma) - a_1x' - a_3$;
retourner (x', y') ;
Fin

3. L'opposé d'un point :

Entrées : $P = (x, y) \in E(\mathbb{F})$ *et* $a_1, a_3 \in E(\mathbb{F})$
Sorties : $-P = (x', y') \in E(\mathbb{F})$.
Début
$x' \longleftarrow x$;
$y' \longleftarrow -y - a_1x - a_3$;
retourner (x', y');
Fin

4. Addition propre de base :

Entrées : $P = (x_1, y_1)$ *et* $Q = (x_2, y_2)$ *qui appartiennent à* $E(\mathbb{F})$
et $a_1, a_2, a_3, a_4 \in E(\mathbb{F})$.
Sorties : $R = P + Q = (x_3, y_3) \in E(\mathbb{F})$.
Début
Si $(P = \infty)$ *alors*
retourner Q *;*
Fin si

Si $(Q = \infty)$ *alors*
retourner P *;*
Fin si

Si $P =$ *négation* (Q) *alors*
retourner ∞ *;*
Fin si

Si $P \neq Q$ *alors*
$\lambda \longleftarrow \frac{y_2 - y_1}{x_2 - x_1}$;
$\gamma \longleftarrow y_1 - \lambda x_1$ *;*
$x_3 \longleftarrow -a_2 + \lambda^2 - x_1 - x_2 + a_1\lambda$;
$y_3 \longleftarrow -(\lambda + a_1)x_R - \gamma - a_3$;
Sinon
$\lambda \longleftarrow \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$;
$\gamma \longleftarrow y_1 - \lambda x_1$ *;*
$x_3 \longleftarrow -a_2 + \lambda - 2x_1 + a_1\lambda$;
$y_3 \longleftarrow -(\lambda x_1 + \gamma) - a_1x_3 - a_3$;
Fin si
Fin

2.4 L'accouplement de Weil

Définition 2.4. *Soit un corps K et soit n un nombre entier qui n'est pas divisible par la caractéristique de K. On pose :*

$$\mu_n(\overline{K}) = \{x \in \overline{K}/x^n = 1\}.$$

Le groupe des racines $n^{ième}$ de l'unité dans $\overline{K}$, puisque la caractéristique de K ne divise pas n, l'équation $x^n = 1$ n'a pas de racines multiples, ainsi μ_n est cyclique d'ordre n.
Un générateur ζ de μ_n est appelé une racine primitive $n^{ième}$ de l'unité.

Corollaire 2.1. *Le groupe $E(K)$ de Mordell-Weil est isomorphe au produit directe de deux groupes abéliens :*

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

T(E) est le groupe de torsion de E qui est fini, $\mathbb{Z}^r = r$ copies du groupe additif abélien $\mathbb{Z}$.
avec l'entier $r \geq 0$ est le rang de la courbe elliptique E.

preuve *:* [4]

Théorème 2.2. ([3].$P83$) *Soit E une courbe elliptique définie sur un corps K et soit n un entier positif tel que la caractéristique de K ne divise pas n. Alors il existe une application :*

$$e_n : E[n] \times E[n] \longrightarrow \mu_n(\overline{K})$$

appelé l'accouplement de Weil, qui satisfait les propriétés suivantes :

1. *e_n est bilinéaire c'est-à-dire :*
   $\bullet e_n(s_1 + s_2, T) = e_n(s_1, T)e_n(s_2, T)$
   $\bullet e_n(s, T_1 + T_2) = e_n(s, T_1)e_n(s, T_2)$
   pour tous $s, s_1, s_2, T, T_1, T_2 \in E[n]$

2. *$e_n(T, T) = 1$ pour tout $T \in E[n]$.*

3. *$e_n(s, T) = e_n(T, s)^{-1}$ pour tout $s, T \in E[n]$; c'est-à-dire e_n est antisymétrique.*

4. *e_n est non dégénéré, c'est-à-dire que si $e_n(s, T) = 1$ pour tout $T \in E[n]$ alors $s = 0$ et si $e_n(s, T) = 1$ pour tout $s \in E[n]$ alors $T = 0$.*

preuve : *[6]*

Corollaire 2.2. *Soit $\{T_1, T_2\}$ une base de $E[n]$. Alors $e_n(T_1, T_2)$ est une racine primitive $n^{ième}$ de l'unité.*

preuve :
Posons $\zeta = e_n(T_1, T_2)$ avec $\zeta^d = 1$. Alors $e_n(T_1, dT_2) = 1$ par la linéarité de la deuxième composante. De plus $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$.
Soit $S \in E[n]$; alors $S = aT_1 + bT_2$ où a, b sont des entiers. Ainsi

$$e_n(S, dT_2) = e_n(T_1, T_2)^a e_n(T_2, T_2)^b = 1$$

Puisque ceci est vrai pour tout $S \in E[n]$; alors $dT_2 = 0$. Comme $dT_2 = 0$ si et seulement si $n \mid d$ (puisque T_2 est d'ordre n) ; ceci implique que ζest une racine primitive $n^{ième}$ de l'unité.

Théorème 2.3 (Mordel-Weil)**.** *Les groupes de Mordel-Weil $E(K)$des courbes elliptiques E sont de type fini.*

preuve*[11]*

2.5 Courbes elliptiques sur un corps fini

En cryptographie on s'intéresse surtout aux courbes elliptiques sur des corps fini. En particulier, il est crucial de savoir calculer $\sharp E(\mathbb{F}_q)$ pour E une courbe elliptique définie sur $\mathbb{F}_q$. Nous rappellons le théorème de Hasse.

Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$, avec $q = p^r$ pour un nombre premier p.
On fixe une clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Théorème 2.4. ([2]*P.*375) *Si E est une courbe elliptique définie sur $\mathbb{F}_q$ alors il existe des entiers d_1 et d_2 tels que*

$$E(\mathbb{F}_q) \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \bigoplus \frac{\mathbb{Z}}{d_2\mathbb{Z}}$$

avec $d_1 \mid d_2$.

Définition 2.5. *Soit E une courbe elliptique définie sur un corps K. Soit n un nombre entier positif, on pose :*

$$E[n] = \{p \in E(\overline{K})/np = 0\}$$

où $\overline{K}$ est une clôture algébrique de K.

Théorème 2.5. ([3]*P.*76) *Soit E une courbe elliptique définie sur un corps K de caractéristique p et n un entier positif non nul.*

1. *Si la caractéristique de K est nulle ou ne divise pas n alors :*

$$E[n] \cong \tfrac{\mathbb{Z}}{n\mathbb{Z}} \bigoplus \tfrac{\mathbb{Z}}{n\mathbb{Z}}$$

2. *Si la caractéristique de K est $p > 0$ et $p \mid n$; écrivons $n = p^r n'$ avec $p \nmid n'$ alors :*

$$E[n] \cong \tfrac{\mathbb{Z}}{n'\mathbb{Z}} \bigoplus \tfrac{\mathbb{Z}}{n'\mathbb{Z}} \text{ ou } E[n] \cong \tfrac{\mathbb{Z}}{n\mathbb{Z}} \bigoplus \tfrac{\mathbb{Z}}{n'\mathbb{Z}}$$

En particulier $E[p] \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$ ou $E[p] = \{0\}$.

Définition 2.6. *Soit E une courbe elliptique définie sur un corps K de caractéristique p. On dit que E est une courbe elliptique supersingulière si $E[p] = \{0\}$.*

Endomorphisme de Frobenius :

Définition 2.7. *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique p. Alors l'endomorphisme de Frobenius de E est défini par :*

$$\begin{aligned} \Phi_q : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ p &\longmapsto 0_E \qquad si \quad p = 0_E. \\ (x,y) &\longmapsto (x^q, y^q) \qquad si \quad p = (x,y). \end{aligned}$$

Lemme 2.1. *Soit $(x,y) \in E(\overline{\mathbb{F}}_q)$:*

1- $\Phi_q(x,y) \in E(\overline{\mathbb{F}}_q)$.

2- $(x,y) \in E(\mathbb{F}_q)$ *si et seulement si* $\Phi_q(x,y) = (x,y)$.

3- Φ_q *est un endomorphisme.*

preuve :

1. *Soient n, p tel que $q = p^n$ ou p est premier et n un entier. La caractéristique de $\mathbb{F}_q$ est p. Nous avons donc : $(a+b)^q = a^q + b^q$ pour $a, b \in \overline{\mathbb{F}}_q$ de plus $a^q = a$ pour tout $a \in \mathbb{F}_q$ on a : $(x,y) \in \overline{\mathbb{F}}_q \Longleftrightarrow E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathbb{F}_q$.*
   n'on élève les deux nombres de cette égalité à les puissances q, nous obtenons :
   $(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6$
   donc : $(x^q, y^q) \in E(\mathbb{F}_q) \Longrightarrow \Phi_q(x,y) \in E(\mathbb{F}_q)$.
2. *On a :* $(x,y) \in E(\mathbb{F}_q) \Longleftrightarrow x \in E(\mathbb{F}_q)$ *et* $y \in E(\mathbb{F}_q) \Longleftrightarrow \Phi_q(x) = x^q = x$ *et* $\Phi_q(y) = y^q = y \Longleftrightarrow \Phi_q(x,y) = (x^q, y^q) = (x,y)$.

Pour la preuve du point 3, le lecteur se référera à [3]$P.48-49$.

Théorème 2.6 (Hasse, 1933)**.** *[5] Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, le cardinal du groupe $E(\mathbb{F}_q)$ est noté $\sharp E(\mathbb{F}_q)$. Alors :*
$|q+1-\sharp E(\mathbb{F}_q)| \leq 2\sqrt{q}$. *Pour ce qui suit, posons* $a = q+1-\sharp E(\mathbb{F}_q)$

Démonstration :[6]

Théorème 2.7. *Soit E une courbe elliptique sur $\mathbb{F}_q$. Alors :*

$$\Phi_q^2 - a\Phi_q + q = o$$

En tant qu'endomorphisme de E et a est le seul nombre entier qui satisfait cette équation. Autrement dit, pour $(x, y) \in E(\overline{\mathbb{F}}_q)$; nous avons :

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = 0$$

Démonstration :[3]$pp.95 - 96$

Proposition 2.3. *Soit q une puissance d'un nombre premier impair et $q \equiv 2 \pmod 3$. Soit $b \in \mathbb{F}_q^*$; alors la courbe elliptique $E : y^2 = x^3 + b$ est supersingulière.*

preuve :
Soit $\Psi : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$ l'omomorphisme défini par $\Psi(x) = x^3$. Puisque $q-1$ n'est pas un multiple de 3 il n'y a pas d'élément d'ordre 3 dans $\mathbb{F}_q^*$; et donc le noyau de Ψ est trivial.
Ainsi Ψ est injective et surjective puisque l'application va d'un groupe fini dans lui -même.
En particulier, tout élément de $\mathbb{F}_q$ a une racine cubique unique dans $\mathbb{F}_q$.
Pour chaque $y \in \mathbb{F}_q$ il existe exactement un $x \in \mathbb{F}_q$ tel que $(x, y) \in E$. En fait x est l'unique racine cubique de $y^2 - b$; puisqu'il y a q valeurs de y possibles, nous trouvons q points finis.
Il faut encore rajouter le point à l'infini 0_E ; ainsi $\sharp E(\mathbb{F}_q) = q + 1$.
Donc E est supersingulière.([3]p.121)

Théorème 2.8. *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de cardinalité $q + 1 - a$. Alors la cardinalité de $E(\mathbb{F}_{q^n})$ avec $n \in \mathbb{N}^*$ est égal à $q^n + 1 - \alpha^n - \beta^n$ ou α et β sont les racines complexes du polynôme $x^2 - ax + q$.*

Supposons $\sharp E(\mathbb{F}_q)$ connu ; alors il existe un moyen simple de calculer $\sharp E(\mathbb{F}_{q^n})$. On pose $a = q + 1 - \sharp E(\mathbb{F}_q)$; soient α et β les deux racines complexes du polynôme :

$x^2 - ax + q = (x - \alpha)(x - \beta)$. La formule est :

$$\forall n \geq 1 : \sharp E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Exemple 2.6.

1. *Soit E une courbe elliptique $E : y^2 = x^3 + 2$ définie sur $E(\mathbb{F}_{7^2})$*

   $E(\mathbb{F}_7) = \{0; (0,3); (0,4); (3,1); (3,6); (5,1); (5,6); (6,1); (6,6)\}$

   d'où $\sharp E(\mathbb{F}_7) = 9$ *;* $a = -1$
   $E(\mathbb{F}_{7^2}) = 7^2 + 1 - (\alpha^2 + \beta^2)$ *avec :* $x^2 + x + 7 = (x - \alpha)(x - \beta)$

   $\Delta = -27 \Longrightarrow \sqrt{\Delta} = i3\sqrt{3}$ *donc* $\sharp E(\mathbb{F}_{7^2}) = 63$.
2. $E : y^2 = x^3 + x + 1$ *une courbe elliptique définie sur* $\mathbb{F}_5$ *; on calcul* $\sharp E(\mathbb{F}_{5^3})$

   $E(\mathbb{F}_5) = \{0; (0,1); (0,4); (2,1); (2,4); (3,1); (4,2); (4,3); (3,4)\}$ *;* $\sharp E(\mathbb{F}_5) = 9$

   d'où $a = -3$ *et* $\sqrt{\Delta} = i\sqrt{11}$ *donc :* $\sharp E(\mathbb{F}_{5^3}) = 108$

Proposition 2.4. *Soit E une courbe elliptique définie sur un corps fini. Alors E est une courbe supersingulière si et seulement si* $a \equiv 0 \pmod{p}$ *c'est-à-dire*
$\sharp E(\mathbb{F}_q) \equiv 1 \pmod{p}$ *or* $a = q + 1 - \sharp E(\mathbb{F}_q)$
si $q = p \geq 5$*, E est supersingulière si et seulement si* $\sharp E(\mathbb{F}_q) = p + 1$.

preuve :[3]$p.121$

Chapitre 3

Le problème du logarithme discret

Dans ce chapitre ; nous allons traiter le problème du logarithme discret et des méthodes qui permettent de résoudre ce dernier. Nous parlerons plus précisement des algorithmes de Baby Step, Giant Step et MOV ; l'algorithme MOV ramène le problème au cas du logarithme discret dans $\mathbb{F}_{p^m}^*$ pour un certain nombre premier et nous allons voir que dans le cas des courbes supersingulières et à anomalies comment nous pouvons résoudre le problème du logarithme discret.

3.1 Problème du logarithme discret

Commençons par définir le problème du logarithme discret dans un groupe G quelconque.

Définition 3.1. *Soient G un groupe et $g \in G$. Le problème du logarithme discret dans G en base g est de trouver un entier x tel que*

$$g^x = y$$

pour $y \in G$ donné.
Dans le cas où $G = E$ est une courbe elliptique, le problème du logarithme discret en base $P \in E$ est de trouver un entier x tel que

$$Q = xP$$

pour $Q \in E$ donné, si un tel x existe.
Soit G un groupe (noté additivement)cyclique fini d'ordre N engendré par un élément p.
Le problème du logarithme discret sur les courbes elliptiques (noté ECDLP ; Elliptic Curve Discrete Logarithm Problem), consiste à trouver un nombre entier k étant donné le point P

et le point $Q = kP$ *où*

$$kP = P + P + P + ... + P; \quad k\ fois$$

Les algorithmes disponibles pour le cas des courbes elliptiques sont les analogues de la méthode de Shanks et celle de Pollard.

Le problème du logarithme discret y sont difficiles à résoudre, et aucun algorithme sous -exponentiel n'y est disponible.

on pose $N_q = \sharp E(\mathbb{F}_q)$; donc le problème du logarithme discret elliptique est le suivant :

Définition 3.2. *Etant donné une courbe elliptique* E *définie sur le corps fini* $\mathbb{F}_q$*, un point* $P \in E(\mathbb{F}_q)$ *d'ordre* n *et un point* $Q \in < p >$ *trouver l'entier* $l \in [0, n-1]$ *tel que* $Q = lP$*.*
L'entier l *est appelé le logarithme discret de* Q *en base* P *noté* $l = log_P Q$*.*

Il existe des cas de courbes elliptiques pour les quelles le problème du logarithme discret peut être prolongé dans des corps finis, et donc peuvent être considérées comme triviales pour la cryptographie.

Définition 3.3.

1. ***Les courbes supersingulières*** *: (Menezes ; Okamato ; Vanstone) :*
   Ce sont les courbes pour les quelles $N_q = q + 1$*. Le problème du logarithme discret sur ces courbes peut être réduit au groupe multiplicatif* $\mathbb{F}_q^*$*.*
2. ***Les courbes elliptiques à anomalies" anomalous"(Samaev ; Araki ; Satoh ; Smart)*** *:*
   Ce sont les courbes pour les quelles $N_q = q$*. Le problème du logarithme discret sur ces courbes peut être réduit au groupe additif* $\mathbb{F}_q$*.*
3. ***Les courbes spéciales*** *:*
   Ce sont les courbes pour les quelles N_q *n'admet que des facteurs premiers petits ; dans ce cas la méthode de Pollard et celle de Western-Pohling- Hallman peuvent être efficacement utilisées.*

Nous parlerons plus précisément du Baby Step-Giant Step qui est apparemment l'un des algorithmes les plus efficaces, mais nous parlerons aussi de l'algorithme MOV qui ramène le problème au cas du logarithme discret dans $\mathbb{F}_{p^m}^*$ pour certain nombre premier p.

3.2 L'algorithme de Shanks (Baby step, Giant step)

Cette méthode développée par D-Shanks[15], fait environ $\sqrt{N}$ pas et stocke environ $\sqrt{N}$ données. C'est pourquoi elle ne fonctionne bien que pour des N de taille modérée. La méthode du Baby step, Giant step pour un groupe de la forme $E(\mathbb{F}_q)$ avec E une courbe elliptique sur $\mathbb{F}_q$ mais elle est valable pour un groupe quelconque.

Nous supposerons qu'il existe un nombre entier k tel que $Q = kP$ avec $P, Q \in E(\mathbb{F}_q)$ et que N l'ordre de E est connu. L'algorithme se déroule comme suit :

1. Choisir un entier $m \geq \sqrt{N}$ et calculer mP.
2. Calculer et stocker dans une liste les iP pour $0 \leq i < m$.
3. Calculer les points $Q - jmP$ pour $j = 0, 1, ..., m-1$ jusqu'à ce qu'un de ces éléments correspondent à un iP de la liste précédente.
4. Si $iP = Q - jmP$, nous avons $Q = kP$ avec $k \equiv i + jm \pmod{N}$.

Nous allons maintenant regarder pourquoi cet algorithme fonctionne. Puisque $m^2 > N$, nous avons $0 \leq k < m^2$.
Écrivons $k = k_0 + mk_1$; ainsi $k \equiv k_0 \pmod{m}$ avec $0 \leq k_0 < m$ et $k_1 = \frac{k-k_0}{m}$ et donc $0 \leq k_1 < m$.
Posons $i = k_0$ et $j = k_1$, nous obtenons donc $Q - k_1 mP = kP - k_1 mP = k_0 P$ est la relation voulue.
Le point iP est calculé en ajoutant P "Baby step" à $(i-1)P$; le point $Q - jmP$ est trouvé en ajoutant $-mP$(Giant step) à $Q - (j-1)mP$ remarquons que nous ne devons pas connaître l'ordre exacte de $E(\mathbb{F}_q)$. Nous devons juste connaître une borne supérieure de N. Ainsi pour une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, nous pouvons prendre un m tel que : $m^2 \geq q + 1 + 2\sqrt{q}$ par le théorème de Hasse.

Exemple 3.1. *Soit $G = E(\mathbb{F}_{41})$, où E est donnée par $E : y^2 = x^3 + 2x + 1$.*
Les seuls points de cette courbe sont :
$(0,1); (0,40); (1,2); (1,39); (8,18); (8,23); (9,16); (9,25); (11,1); (11,40); (12,20); (12,21);$
$(13,16); (13,25); (18,2); (18,39); (19,16); (19,25); (20,13); (20,28); (21,19); (21,22); (23,18);$
$(23,23); (26,9); (26,32); (28,19), (28,22); (30,1); (30,40); , (32,19); (32,22); (38,3); (38,38);$
$(40,30)$.
D'après le théorème de Hasse on a l'ordre de G est :

On a $| q + 1 - \sharp E(\mathbb{F}_q) | \leq 2\sqrt{q}$ *donc* $| 41 + 1 - \sharp E(\mathbb{F}_{41}) | \leq 2\sqrt{41}$

d'où $\sharp E(\mathbb{F}_{41}) \leq 42 + 2\sqrt{41} \Longrightarrow \sharp E(\mathbb{F}_{41}) \leq 55.$

Posons $m = 8$ *(*$8^2 > 55$*).*

Les points ip pour $0 \leq i \leq 7$ *sont :*

$P, 2P, 3P, 4P, 5P, 6P, 7P$ *c.à.d* $(0,1); (1,39); (8,23); (38,38); (23,23); (20,28); (26,9).$

Soient $P = (0,1)$ *et* $Q = (30,40)$ *; calculons* $Q - jmP$ *pour* $j = 0, 1, 2$ *:*

1. $j = 0$:
   $Q - 0P = Q = (30,40).$
2. $j = 1$:
   $Q - 8P = (30,40) - 8(0,1)$
   =(30,40)-(10,18)
   =(30,40)+(10,23)
   =(9,25)
3. $j = 2$:
   $Q - 2(8)P = (30,40) - 2(10,18)$
   =(30,40)-(30,1)
   =(30,40)+(30,40)
   =(26,9)
   Nous trouvons que le troisième point correspond à $7P$*.*
   Donc : $Q = (7 + 2 \times 8)P = 23P.$
   d'ou $k = 23.$

Exemple 3.2. *Soit* $E : y^2 = (x^3 + 2x + 2) \mod 17$ *;* $|E| = 19.$
Les seuls points de cette courbe sont :
(5,1) ;(6,3) ;(10,6) ;(3,1) ;(9,16) ;(16,13) ;(0,6) ;(13,7) ;(7,6) ;(7,11) ;
(13,10) ;(0,11) ;(16,4) ;(9,1) ;(3,16) ;(10,11) ;(6,14) ;(5,16).
On choisit $m = 5$
Les points ip pour $0 \leq i \leq 4$ *sont :*
$P, 2P, 3P, 4P$ *c.à.d :(5,1) ;(6,3) ;(10,6) ;(3,1)*

Soint $P = (5, 1)$ *et* $Q = (6, 14)$ *; calculons* $Q - jmP$ *pour* $j = 0, 1, 2, 3$:

1. $j = 0$:
   $Q - 0P = Q = (6, 14)$
2. $j = 1$:
   $Q - 5P = (6, 14) - (9, 16)$
   =(6,14)+(9,1)
   =(0,11)

3. $j = 2$:
   $Q - 2(5)P = (6, 14) - (7, 11)$
   =(6,14)+(7,6)
   =(0,6)

4. $j = 3$:
   $Q - 15(5)P = (6, 14) - (3, 16)$
   $= (6, 14) + (3, 1)$
   $= (6, 3)$

Nous trouvons que le troisième point correspond à $2P$.
Donc : $Q = (2 + 3 \times 5)P = 17P$.
d'ou $k = 17$.

3.3 L'algorithme MOV

• Cet algorithme spécifique pour résoudre le problème du logarithme discret dans le cas des courbes elliptiques.
• Le MOV ([3]p.144), développé par Menezes, Okamoto et Vanstone, utilise l'accouplement de Weil pour transformer un problème de logarithme discret dans $E(\mathbb{F}_q)$ en un problème de logarithme discret dans $\mathbb{F}_{q^m}^*$ pour un certain entier m.
• En fait, l'entier m de $E(\mathbb{F}_{q^m})$ peut très bien être grand, auquel cas le problème du logarithme discret dans le groupe $\mathbb{F}_{q^m}^*$ qui est d'ordre $q^m - 1$ est aussi difficile à résoudre que le problème du logarithme discret dans $E(\mathbb{F}_q)$ qui a un ordre d'environ q par le théorème de Hasse.
Par contre, pour une courbe supersingulière, nous pouvons en général prendre $m = 2$.
Soit E une courbe elliptique définie sur $\mathbb{F}_q$, soient $P, Q \in E(\mathbb{F}_q)$ et N l'ordre de P. Supposons que

$$pgcd(q, N) = 1$$

nous cherchons un entier k tel que $Q = kP$.
Puisque tout point de $E[N]$ a ses coordonnées dans $\overline{\mathbb{F}}_q = \bigsqcup_{j\geq 1} \mathbb{F}_{q^j}$ il existe m tel que

$$E[N] \subseteq E(\mathbb{F}_{q^m})$$

L'algorithme MOV se déroule ainsi :

1. Choisir un point $T \in E(\mathbb{F}_{q^m})$.
2. Calculer M, l'ordre de T.
3. Soit $d = pgcd(M, N)$. Posons $T_1 = (\frac{M}{d})T$, l'ordre de T_1 est d. Celui-ci divise N ainsi $T_1 \in E[N]$.
4. Calculer $\xi_1 = e_N(P, T_1)$ et $\xi_2 = e_N(Q, T_1)$. Donc, ξ_1 et ξ_2 sont dans $\mu_d \subset \mu_N \subset \mathbb{F}_{q^m}^*$. En effet,

   $$1 = e_N(P, 0) = e_N(P, dT_1) = e_N(P, T_1)^d = \xi_1^d$$

   même chose pour ξ_2.
5. Résoudre le problème du logarithme discret pour $\xi_2 = \xi_1^k$ dans $\mathbb{F}_{q^m}^*$. Nous trouvons $k \pmod d$.
6. Recommencer avec des points T choisis au hasard jusqu'à ce que nous ayons $pgcd(M, N) = N$, ceci détermine $k \pmod N$.

Proposition 3.1. *Soit E une courbe elliptique sur $\mathbb{F}_q$ et supposons que $a = 0$, c'est-à- dire E est supersingulière. Soit N un nombre entier positif premier à p où $q = p^j$. S'il existe un point $p \in E(\mathbb{F}_q)$ d'ordre N, alors :*

$$E[N] \subseteq E(\mathbb{F}_{q^2})$$

preuve :
L'endomorphisme de Frobenius Φ_q satisfait la relation :

$$\Phi_q^2 - a\Phi_q + q = 0$$

puisque $a = 0$ par hypothèse, nous avons :

$$\Phi_q^2 = -q.$$

Soit $S \in E[N]$, puisque $\sharp E(\mathbb{F}_q) = q + 1$ et qu'il existe un point d'ordre N, nous avons $N \mid (q + 1)$; c'est-à-dire $-q \equiv 1 \pmod{N}$.
Ainsi $\Phi_q^2(S) = -qS = S$, puisque $\Phi_q^2 = \Phi_{q^2}$ et $S \in E(\mathbb{F}_{q^2})$.
Donc, l'algorithme MOV est très efficace lorsque $E(\mathbb{F}_q)$ est supersingulière et que $a = 0$ puisque nous pouvons ramener à un problème de logarithme discret sur $\mathbb{F}_{q^2}$.

3.4 Courbe à anomalies

Définition 3.4. *Une courbe elliptique E définie sur $\mathbb{F}_q$ est appellée une courbe à anomalie si*

$$\sharp E(\mathbb{F}_q) = q.$$

Nous ne traiterons que le cas $q = p$; ou p est un nombre premier, soit E une courbe elliptique définie sur $\mathbb{F}_p$ et les points $P, Q \in E(\mathbb{F}_p)$ sur une courbe elliptique sur $\mathbb{Z}$.

Proposition 3.2. *Soient E une courbe elliptique sur $\mathbb{F}_p$ et $P, Q \in E(\mathbb{F}_p)$. Supposons que E soit écrite sous la forme d'une équation de Weierstrass : $y^2 = x^3 + Ax + B$.*
Alors il existe des entiers $\widetilde{A}, \widetilde{B}, x_1, x_2, y_1, y_2$ et une courbe elliptique $\widetilde{E}$ donnée par :

$$y^2 = x^3 + \widetilde{A}x + \widetilde{B}$$

telle que $\widetilde{P} = (x_1, y_1), \widetilde{Q} = (x_2, y_2) \in \widetilde{E}(\mathbb{Z})$ et telle que :
$A \equiv \widetilde{A}, B \equiv \widetilde{B}, P \equiv \widetilde{P}, Q \equiv \widetilde{Q} \pmod{p}$.

preuve :([3]pp.147-148)

Remarque :
Si nous avons la relation $Q = kP$ pour un certain entier k, nous n'avons pas, en général $\widetilde{Q} = k\widetilde{P}$ dans $\widetilde{E}$. Ce qui est remarquable sur les courbes à anomalies est que malgré que même si $\widetilde{Q}$ et $\widetilde{P}$ sont indépendants, nous pouvons obtenir suffisamment d'informations pour trouver k.

Définition 3.5. *Soit $a \mid b \neq 0$ un nombre rationnel, ou a, b sont des entiers premiers entre eux. Ecrivons $a \mid b = p^r a_1 \mid b_1$ avec p premier et $p \nmid a_1 b_1$.*
On définit la valuation p-adic comme suit :

$$v_p(a/b) = r$$

On pose $v_p(0) = +\infty$.
Par exemple ;

$$v_2(7/40) = -3, v_3(9/2) = 2, v_{13}(8/5) = 0.$$

Soit $\widetilde{E}$ une courbe elliptique sur $\mathbb{Z}$ donnée par $y^2 = x^3 + \widetilde{A}x + \widetilde{B}$. Soit $r \geq 1$ entier. On pose

$$\widetilde{E}_r = \{(x, y) \in \widetilde{E}(\mathbb{Q}) / v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{0\}$$

C'est l'ensemble des points tels que x a au moins le facteur p^{2r} au dénominateur et y au moins le facteur p^{3r} au dénominateur. Il est clair que

$$\widetilde{E}_r \supseteq \widetilde{E}_{r+1} \supseteq ...$$

Théorème 3.1. *Soit $y^2 = x^3 + \widetilde{A}x + \widetilde{B}$, avec $\widetilde{A}, \widetilde{B}$ des entiers. Soient encore p un nombre premier et r un entier positif. Alors*

1. *$\widetilde{E}_1$ est sous-groupe de $\widetilde{E}(\mathbb{Q})$.*
2. *Si $(x, y) \in \widetilde{E}(\mathbb{Q})$, alors $v_p(x) < 0$ si et seulement si $v_p(y) < 0$. Dans ce cas, il existe un entier $r \geq 1$ tel que $v_p(x) = -2r, v_p(y) = -3r$.*
3. *L'application*

$$\begin{aligned} \lambda_r : \widetilde{E}_r / \widetilde{E}_{5r} &\longrightarrow \mathbb{Z}/p^{4r}\mathbb{Z} \\ (x, y) &\longmapsto p^{-r}x/y \pmod{p^{4r}} \\ 0 &\longmapsto 0 \end{aligned}$$

   est un homomorphisme injectif.
4. *Si $(x, y) \in \widetilde{E}_r$ mais que $(x, y) \notin \widetilde{E}_{r+1}$, alors $\lambda_r(x, y) \equiv 0 \pmod{p}$.*

preuve :([3]pp.189-197)

Proposition 3.3. *On définit la réduction modulo p comme suit :*

$$\begin{aligned} red_p : \widetilde{E}(\mathbb{Q}) &\longrightarrow \widetilde{E} \pmod p \\ (x,y) &\longmapsto (x,y) \pmod p \quad si \quad (x,y) \notin \widetilde{E}_1 \\ \widetilde{E}_1 &\longrightarrow \{0\}. \end{aligned}$$

L'application red_p est un homomorphisme dont le noyau est $\widetilde{E}_1$.

nous pouvons maintenant regarder comment et pourquoi marche l'algorithme pour résoudre les problèmes du logarithme discret dans le cas de courbes à anomalies.
Soient E une courbe elliptique sur $\mathbb{F}_p$ à anomalies, $P, Q \in E(\mathbb{F}_p)$. Nous cherchons k tel que $Q = kP$.
Supposons que $k \neq 0$. Puisque E est une courbe à anomalie sur $\mathbb{F}_q$, $\sharp E(\mathbb{F}_p) = p$.
L'algorithme se déroule ainsi :

1. Relever E, P, Q dans $\mathbb{Z}$ pour obtenir $\widetilde{E}, \widetilde{P}, \widetilde{Q}$.
2. Soient $\widetilde{P}_1 = p\widetilde{P}, \widetilde{Q}_1 = p\widetilde{Q}$. Remarqons que $\widetilde{P}_1, \widetilde{Q}_1 \in \widetilde{E}_1$ puisque

   $$red_p(p\widetilde{P}) = p.red_p(\widetilde{P}) = 0$$

   car E est une courbe à anomalie sur $\mathbb{F}_q$.
3. Si $\widetilde{P}_1 \in \widetilde{E}_2$, choisir des nouveaux $\widetilde{E}, \widetilde{P}, \widetilde{Q}$ et réessayer. Sinon, soient $l_1 = \lambda_1(\widetilde{P}_1)$ et $l_2 = \lambda_1(\widetilde{Q}_1), l_1, l_2$ sont bien définis puisque $\widetilde{P}_1, \widetilde{Q}_1 \in \widetilde{E}_1$. Nous avons

   $$k \equiv l_2 l_1^{-1} \pmod p$$

Remarquons que l_1 est inversible modulo p car $\widetilde{P}_1 \notin E_2$, ce qui veut dire que la puissance de p de $\lambda_1(\widetilde{P}_1)$ est 0.
Comme $\widetilde{K} = k\widetilde{P} - \widetilde{Q}$. Nous avons :

$$kP - Q = red_p(k\widetilde{P} - \widetilde{Q}) = red_p(\widetilde{K}) = 0.$$

Ainsi $\widetilde{K} \in \widetilde{E}_1$ et donc $\lambda_1(\widetilde{K})$ est défini et

$$\lambda_1(p\widetilde{K}) = p\lambda_1(\widetilde{K}) \equiv 0 \pmod p.$$

Ainsi,

$$kl_1 - l_2 = \lambda_1(k\widetilde{P}_1 - \widetilde{Q}_1) = \lambda_1(kp\widetilde{P} - p\widetilde{Q}) = \lambda_1(p\widetilde{K}) \equiv 0 \pmod p.$$

Ce qui veut dire que $k \equiv l_2 l_1^{-1} \pmod p$.

3.5 L'algorithme de Schoof

Cet algorithme dû à René Schoof en 1985 [7] qui permet de calculer $\sharp E(\mathbb{F}_{p^n})$ pour un grand nombre premier p. Ainsi nous pouvons calculer $\sharp E(\mathbb{F}_{p^n})$ grâce au théorème 2-9.

Soit $E : y^2 = x^3 + Ax + B$ une courbe elliptique définie sur $\mathbb{F}_p$ avec p un nombre premier et soit $a = p + 1 - \sharp E(\mathbb{F}_p)$.

l'idée de cet algorithme est de déteminer $a \mod l$ pour de petits nombres premiers l. D'aprés le théorème de Hasse nous avons :

$$p + 1 - 2\sqrt{p} < \sharp E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}$$

c'.à.d que $|a| \leq 2\sqrt{p}$. Il nous suffit donc de prendre tous les k premiers nombres premiers l_i de manières à avoir

$$\prod_{i=1}^{k} l_i > 4\sqrt{p}$$

Pour pouvoir déterminer $\sharp E(\mathbb{F}_p)$ de manière unique grâce au théorème Chinois.
Notons S l'ensemble de ces premiers. Et comme p est grand, les premiers l_i sont petits par rapport à p et $l_i \neq p$.
Nous allons voir comment déterminer $a \mod l_i$ pour les différents $l_i \in S$.

1-cas $l = 2$:

Si $\sharp E(\mathbb{F}_p) \equiv 0 \pmod 2$; c.à.d que l'ordre du groupe est pair, sinon son ordre est impair. Nous savons que les seuls éléments d'ordre 2 de $E(\mathbb{F}_p)$ sont de la forme (e, o) avec $e \in \mathbb{F}_p$; c.à.d e est une racine de $x^3 + Ax + B$ et donc $p + 1 - a \equiv 0 \pmod 2$ ce qui veut dire que

$$a \equiv 0 \pmod 2$$

Si $x^3 + Ax + B$ n'a pas de racine dans $\mathbb{F}_p$, alors $\sharp E(\mathbb{F}_p) \equiv 1 \pmod 2$ et donc

$$a \equiv 1 \pmod 2$$

Pour déterminer si $x^3 + Ax + B$ possède des racines dans $\mathbb{F}_p$, il suffit de se rappeller que les éléments de $\mathbb{F}_p$ sont exactement les racines de $x^p - x$. Ainsi $x^3 + Ax + B$ a une racine dans $\mathbb{F}_p$ si et seulement s'il a une racine en commun avec $x^p - x$ c.à.d si et seulement si

$$pgcd(x^3 + Ax + B; x^p - x) = 1$$

Pour faire ce calcul, nous utilisons l'algorithme d'Euclide appliqué aux polynômes. Si p est grand le polynôme x^p est de degré grand.

Il est donc préférable de calculer

$$[x] \equiv x^p \pmod{x^3 + Ax + B}$$

donc :

$$pgcd([x] - x, x^3 + Ax + B) = pgcd(x^p - x, x^3 + Ax + B)$$

ceci termine le cas $l = 2$.

2-cas $l \neq 2$:

Pour déterminer $a \pmod{l_i}$, il suffit d'examiner quelle relation du type $\phi_p^2 - k\phi_p + p$ peut avoir lieu sur $E[l_i]$. On aura alors $k \equiv a \pmod{l_i}$.

Polynômes de division :

Définition 3.6. [3] *Nous définissons les polynômes de division $\Psi_m \in \mathbb{Z}[x, y, A, B]$ comme suit :*

$\Psi_0 = 0$

$\Psi_1 = 1$

$\Psi_2 = 2y$

$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$

$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, \quad m \geq 2$

$\Psi_{2m} = (2y)^{-1}\Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2), \quad m \geq 2$

Proposition 3.4.

1. *Si n est impair, alors $\Psi_n \in \mathbb{Z}[x, y^2, A, B]$.*
2. *Soit n un nombre impair, alors le degré de $\Psi_n \in \mathbb{Z}[x]$ est $(n^2 - 1)/2$.*
3. *Soient $(x, y) \in E(\overline{\mathbb{F}}_P)$ et $n \in \mathbb{N}$, alors :*

$$(x, y) \in E[n] \Longleftrightarrow \Psi_n(x) = 0.$$

Soit $l \in S$ avec $l \neq 2$ et soit $(x, y) \in E(\mathbb{F}_P) \cap E[l]$. Alors :

$$\begin{cases} (x^{p^2}, y^{p^2}) + p(x, y) = a(x^p, y^p)\,; \\ \\ \Psi_l(x) = 0\,; \end{cases}$$

Soit $p_l \in [\frac{-l}{2}, \frac{l}{2}]$ tel que $p_l \equiv p \pmod{l}$. Comme $(x, y) \in E[l]$ nous avons encore $p(x, y) = p_l(x, y)$ et donc

$$(x^{p^2}, y^{p^2}) + p_l(x, y) = a(x^p, y^p)$$

Ceci nous permet de travailler avec des valeurs plus petites. Puisque (x^p, y^p) est aussi d'ordre l (car Φ_q est un endomorphisme), la relation ci-dessus détermine $a \mod l$.

L'idée est de calculer tous les termes de cette expression excepté a, puis de déterminer a pour que cette relation soit satisfaite. Notons que si cette relation est satisfaite pour un point de $(x, y) \in E[l]$, alors nous avons déterminer $a \mod l$ et donc elle sera vraie pour tout $(x, y) \in E[l]$.

1^{er}-cas :

Supposons tout d'abord que $(x^{p^2}, y^{p^2}) \neq \pm p_l(x, y)$ pour $(x, y) \in E[l]$.
Posons

$$(x', y') = (x^{p^2}, y^{p^2}) + p_l(x, y) \neq 0$$

Ainsi $a \equiv 0 \pmod{l}$. Vu comment nous avons défini la loi de groupe sur E, nous avons que $x^{p^2} \neq x$.
Posons : $j(x, y) = (x_j, y_j)$.
Pour j un entier ; nous avons :

$$x' = (\frac{y^{p^2} - y_{p_l}}{x^{p^2} - x_{p_l}})^2 - x^{p^2} - x_{p_l}$$

Nous pouvons exprimer $(y^{p^2} - y)^2$ en fonction de x, en effet

$$(y^{p^2} - y)^2 = y^2(y^{p^2-1} - 1)^2;$$

$$= (x^3 + Ax)((x^3 + Ax + B)^{(p^2-1)/2} - 1)^2;$$

Même chôse pour x_{p_l}. Nous pouvons exprimer x' comme une fonction rationnelle de x.
Nous cherchons j de telle manière à avoir

$$(x', y') = (x_j^p, y_j^p).$$

Nous avons $(x, y) \in E[l]$, avec $(x', y') = \pm(x_j^p, y_j^p)$ si et seulement si $x' = x_j^p$. Si cette relation est vraie pour un point de $E[l]$, alors elle est vraie pour tout point de $E[l]$.
Puisque les racines de Ψ_l sont les premières coordonnées des points finis de $E[l]$, ceci implique que :

$$x' - x_j^p \equiv 0 \; mod \; \Psi_l.$$

Il faut aussi se rendre compte que les racines de Ψ_l sont simples. En effet, il y a $l^2 - 1$ points finis d'ordre l puisque

$$E[l] \simeq \frac{\mathbb{Z}}{l\mathbb{Z}} \oplus \frac{\mathbb{Z}}{l\mathbb{Z}}.$$

Il y a donc $(l^2 - 1)/2$ points de $E[l]$ ayant la première coordonnée distincte des autres, puisque si $(x, y) \in E[l]$ alors $(x, -y) = -(x, y) \in E[l]$.
De plus le degré de Ψ_l est $(l - 1)/2$, donc Ψ_l n'a que des racines simples.

Ainsi $\Psi_l/x' - x^p$; nous calculons donc $(x^p)_j$ pour $1 \leq j \leq (l-1)/2$ jusqu'à ce que $x' - x_j^p \equiv 0 \pmod{\Psi_l}$ soit satisfait.
Supposons que nous ayons trouvé un tel j. Alors :

$$(x', y') = \pm(x_j^p, y_j^p) = (x_j^p, \pm y_j^p).$$

Pour déterminer le singne de a il nous faut regarder y'. Les expressions $\frac{y'}{y}$ et $\frac{y_j^p}{y}$ sont des fonctions de x [7].

Si $(y' - y_j^p)/y \equiv 0 \pmod{\Psi_l}$; alors $a \equiv j \pmod{l}$.
Sinon nous avons : $(y' + y_j^p)/y \equiv 0 \pmod{l}$ et donc $a \equiv j \pmod{l}$.

$2^{ème}$-cas :
Il nous reste à considérer le cas où $(x^{p^2}, y^{p^2}) = \pm p(x, y)$ pour tout $(x, y) \in E[l]$.
Si nous avons

$$\Phi_p^2(x, y) = -p(x, y);$$

alors $aP = (\Phi_p^2 + p)(P) = 0$, pour tout $P \in E[l]$. Ainsi $a \equiv 0 \pmod{l}$
si

$$\Phi_p^2(x, y) = (x^{p^2}, y^{p^2}) = p(x, y)$$

alors

$$a\Phi_p(x, y) = \Phi_p^2(x, y) + p(x, y) = 2p(x, y),$$

autrement dit,

$$a^2 p(x, y) = a^2 \Phi_p^2(x, y) = (2p)^2(x, y).$$

Ainsi, $a^2 p \equiv 4p^2 \pmod{l}$, c-à-d que $p \equiv a^2(2^{-1})^2 \pmod{l}$ ce qui veut dire que p est un carré $mod\ l$.
Posons $w^2 \equiv p \pmod{l}$. Nous avons :

$$(\Phi_p - w)(\Phi_p + w)(x, y) = \Phi_p^2(x, y) = 0$$

Pour tout $(x, y) \in E[l]$. Soit $P \in E[l]$, alors soit $(\Phi_p - w)(P) = 0$, et donc : $\Phi_p(P) = wP$.

Soit $(\Phi_p - w)(P) = P'$ est un point fini avec : $(\Phi_p + w)(P') = 0$.
Dans tous les cas, il existe un point $P \in E[l]$ avec $\Phi_p(P) = \pm wP$.
Supposons qu'il existe un point $P \in E[l]$ tel que $\Phi_p(P) = wP$. Alors :

$$(\Phi_p^2 - a\Phi_p + p)(P) = (p - aw + p)(P) = 0,$$

ainsi $aw \equiv 2p \equiv 2w^2 \pmod{l}$ et donc $a \equiv 2w \pmod{l}$.

De la même manière, s'il existe P tel que $\Phi_p(P) = -wP$, alors $a \equiv -2w \pmod{l}$.
Ainsi si $\Phi_p^2(x,y) = p(x,y)$ nous avons forcément que p est un carré modulo l. Nous procédons donc ainsi, nous regardons si p est un carré modulo l en calculont le symbole de Legendre $(\frac{p}{l})$ qui est assez facile à calculer. Si p n'est pas un carré modulo l alors nous somme forcément dans le cas $\Phi_p^2(x,y) = -p(x,y)$.
Si nous avons que p est carré modulo l, il faut regarder s'il existe un point $P \in E[l]$ tel que $\Phi_p(P) = \pm wP$ où $w^2 = p$. Donc il suffit de calculer :

$$pgcd(numérateur(x^p - x_w), \Psi_l).$$

Si $pgcd(numérateur(x^p - x_w), \Psi_l) \neq 1$, alors il existe un tel point (x,y) qui est dans $E[l]$ tel que $\Phi_p(x,y) = \pm w(x,y)$.
Pour déterminer le signe, il nous faut encore calculer

$$pgcd(numérateur(y^p - y_w)/y), \Psi_l).$$

Si $pgcd(numérateur(y^p - y_w)/y), \Psi_l) \neq 1$, alors $a \equiv 2w \pmod{l}$. Sinon $a \equiv -2w \pmod{l}$.
Si $pgcd(numérateur(x^p - x_w), \Psi_l) = 1$, alors nous nous retrouvons dans le cas
$\Phi_p^2(P) = -pP$ et donc $a \equiv 0 \pmod{l}$.

Résumé de l'algorithme de Schoof

Soit une courbe elliptique $E : y^2 = x^3 + Ax + B$ définie sur $\mathbb{F}_p$, nous voulons calculer $\sharp E(\mathbb{F}_p) = p + 1 - a$. L'algorithme se déroule ainsi :

1. Soit S l'ensemble défini plus haut.
2. Si $l = 2, a \equiv 0 \pmod{2}$ si et seulement si $pgcd(x^3 + Ax + B, x^p - x) \neq 1$.
3. Pour chaque nombre premier $l \in S$ avec $l \neq 2$ faire ce qui suit :

   (a) Posons $P_l \equiv P \pmod{l}$ avec $\mid P_l \mid < \frac{l}{2}$.

   (b) Calculer x', la première coordonnée de

   $$(x', y') = (x^{p^2}, y^{p^2}) + p_l(x,y) \pmod{\Psi_l}.$$

   (c) Pour $j = 1, ..., (l-1)/2$, faire ce qui suit :

i. Calculer x_j, la première coordonnée de

$$(x_j, y_j) = j(x, y).$$

ii. Si $x' - x_j^p \equiv 0 \pmod{\Psi_l}$ aller à l'étape C ; sinon essayer la prochaine valeur de j à l'étape *iii*.
Si toutes les valeurs de $1 \leq j \leq (l-1)/2$ ont été essayées aller à l'étape *iv*.

iii. calculer y' et y_j. Si $(y' - y_j)/y \equiv 0 \pmod{\Psi_l}$, alors $a \equiv j \pmod{l}$. Sinon, $a \equiv -j \pmod{l}$

(d) Si toutes valeurs $1 \leq j \leq (l-1)/2$ ont été essayées sans succées, posons $w^2 \equiv p \pmod{l}$.
Si p n'est pas un carré modulo l, alors $a \equiv 0 \pmod{l}$.

(e) Si $pgcd(numérateur(x^p - x_w), \Psi_l) = 1$, alors $a \equiv 0 \pmod{l}$.
Sinon, calculer $pgcd(numérateur(y^p - y_w)/y), \Psi_l)$. Si le pgcd n'est pas 1, alors $a \equiv 2w \pmod{l}$. Sinon, $a \equiv -2w \pmod{l}$.

4. Connaissant $a \pmod{l}$ pour chaque $l \in S$, nous pouvons calculer $a \pmod{\Pi_{l \in S} l}$.
Par le théorème Chinois ; choisir la valeur de a qui satisfait cette congruence et telle que $\mid a \mid \leq 2\sqrt{2}$. Alors

$$\sharp E(\mathbb{F}_p) = p + 1 - a.$$

Conclusion

Dans ce travail, nous allons traiter quelques propriétés des courbes elliptiques sur les corps finis et on a étudié quelques méthodes qui permettent à résoudre le problème du logarithme discret qui est dans certains cas facile à résoudre rapidement.
C'est pour cela, on a présenté l'algorithme de Baby Step, Giant Step et l'algorithme MOV qui sont les plus efficaces.
En effet puisque le cryptage des messages avec des courbes elliptiques se base sur la difficulté de résoudre le problème du logarithme discret en un temps raisonnable.

Bibliographie

[1] **Antoine Chambert.**
Loir. Algèbre corporelle. 2004.

[2] **Henri Cotlen.**
A cours in computational algebraic number theory. Springer, 1993.

[3] **Lawrance C. Washington.**
Elliptic curves number theory and cryptography.Discrete Mathematics and its application. Chapmon Hall/CRC. 2003.

[4] **Cassels J.W.S.**
Diophantine equations with special reference to elliptic curves. J. London Math. Soc.41 (1966). 193-291

[5] **Serge Lang.**
(1) Elliptic fonctions 14LAN .1973.

(2) Elliptic curves diophantine analysis-springer.1972.

[6] **Joseph H. Silverman.**
The arithmetic of elliptic curves. Springer. 1986.

[7] **Schoof,R.**
Elliptic curves over finite fields and the computation of square roots mod$p$.Math.Camp.44,Avril 1985.

[8] **Hartshorne,R,ed.**
Algebraic Geometry,Arcata 1974.Amer.Math.Soc.Proc.Symp.Pure Math 29,1975.

[9] **Shafarevich,I.R.**

Basic algebric geometry,springer.Verlag.1977.

[10] **A.W.Knapp.**

Elliptic curves.Mathematical notes 40.Princeton university press.1992.

[11] **Neal Koblitz.**

Introduction to elliptic curves and modular forms- 2^{nd} Ed (2000) graduate texts in mathematics 97(2).

A course in number theory and cryptography 2^{nd} -graduate texts in mathematics 114(1988).

[12] **Goro Shimura.**

Introduction of the arithmetic theory of automorphic functions-Princeton university press.1971.

[13] **Y.Hellegouarch.**

Invitation aux mathématiques de Fermat-Wiles ;Dunod,Paris.1997 ;2001.

[14] **Henri Cohen.**

Acourse in computational algebraic number theory.Springer ;1993.

[15] **D.Shanks.**

Class number, a theory of factorisation, and genera, Proc.Symp in pure Maths 20, A.M.S, Providence, R.I, 1969, pp. 415-440.