UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES

DÉPARTEMENT DE MATHÉMATIQUES

Mémoire de Master

Domaine :	Sciences et Technologies
Mention :	Mathématiques et Applications
Spécialité :	Mathématiques Pures
Option :	Algèbre et Géométrie Algébrique

Thème :

Nombre de Points Rationnels sur une Courbe Elliptique dans un Corps Fini

Présenté par :

Thierno Amadou DIALLO

Sous la direction de : **Dr Moussa FALL**

Sous la supervision de : **Professeur Oumar SALL**

Soutenu publiquement le 11 *Mars* 2023 devant le jury composé de :

Amoussou Thomas GUEDENON	Professeur assimilé	Président du Jury	UASZ
Oumar SALL	Professeur Titulaire	Examinateur	UASZ
Mamadou Eramane BODIAN	Maître de Conférences Titulaire	Examinateur	UASZ
Moussa FALL	Maître de Conférences Titulaire	Directeur	UASZ

Année universitaire : 2021 – 2022

REMERCIEMENTS

"Gloire et pureté à Allah le seigneur de l'univers et il n'y a de puissance ni de force que par Allah le Puissant, le Sage."

La réalisation de ce mémoire a été possible grâce à Allah et au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.
Je voudrais tout d'abord adresser toute ma reconnaissance au directeur de ce mémoire, Docteur Moussa FALL, pour l'encadrement dont j'ai bénéficié de sa part tout au long de ce travail. Je le remercie pour sa disponibilité, ses remarques pertinentes et enrichissantes, ses recadrages et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion. Je suis honoré par la présence du Professeur Amoussou Thomas GUEDENON qui a accepté de présider le jury de mon mémoire et je le remercie sincèrement.
Je souhaite remercier Professeur Oumar SALL qui a accepté de superviser mon travail et Dr Mamadou Eramane BODIAN avoir accepté de faire partie du jury.
Mes remerciements vont à l'endroit de tous les enseignants-chercheurs du département de mathématiques de l'Université Assance SECK de Ziguinchor, pour la qualité de l'enseignement qu'ils nous ont dispensé.
Je remercie monsieur Moustapha CAMARA et Dr Souhaibou SAMBOU pour avoir accepté de faire une relecture de mon mémoire et pour leurs pertinentes suggestions.
Je remercie tous mes camarades promotionaires de la licence au master particulièrement à Ibrahima TRAORE, Ramatoulaye DIALLO, Marie FAYE, Lamine MANE, Omar DIOP, Malick FAYE, Abdoulaye DIOUF, Mouhamed Fadel AIDARA, Pape Aly CISSE, Abdourahmane DIATTA Christ Jesus BASS, Pathé BA, Fatou DIEME, Bamba SECK, Alioune Badara WADE...
Je remercie tous mes ainés de l'école doctorale Mathématiques et Appliquées particulièrement à Saliou DIAW, Papa BADIANE, Algassimou DIALLO, Daouda DIACK, Mamadou Korka BA et Docteure Winnie OSSETTE, Awa BARRY, Fatou DIENG.
Je tiens à témoigner toute ma reconnaissance à mon père, monsieur Mamadou Moctar DIALLO pour son soutien durant tout mon cursus scolaire, ses encouragements et ses prières.
Je remercie également toutes mes soeurs, Adama Hawa, Fatoumata Diaraye, Néné Galé, Diamilatou, Fatoumata DIALLO, Khady MBENGUE et ma fille Aissata Diaraye DIALLO.
Je remercie toute ma famille d'accueil de Ziguinchor, particulièrement ma grande mère Kadiatou DIALLO, mon oncle Thierno BALDE et ma tante Ousseynatou BALDE.
Je remercie également tous mes frères syndicalistes de l'Université particulièrement Ibra-

hima KA, Baye Magatte GUEYE, Amadou GUEYE, Djiby GUEYE, Ibrahima SYLLA, Mamoudou AW, Tidiane DIAO, Adama DIOUF, Aliou BALDE, Babacar NDIOL, Amadou SAWARE, Assane SOW.
Je remercie également mes frères de l'amicale de Keur Massar et la fédération de Pikine particulièrement à Boubacar SENGHOR, Balla NGING, Abdoulaye FAYE, Mamadou NDOM, Idrissa DIOUF, Feu Daouda THIAM et mon filleul Lamine SAGNA.
Je remercie également l'administration du CEM Direct-Aid ainsi que tous mes collègues enseignants.
Mes remerciements à toutes les personnes, qui m'ont soutenu moralement, physiquement et financièrement de près ou de loin tout au long de mon cursus scolaire.

Dédicace

Je dédie ce mémoire,

A ma chère défunte maman,

Adama Hawa Baldé.

Que son âme repose en Paix,

Amine.

Notations et Abréviations

$\mathbb{F}_p$: corps fini de caractéristique p

$\overline{\mathbb{F}_q}$: clôture algébrique de $\mathbb{F}_q$

$a \equiv b \bmod n$: a congrue b modulo n

E : courbe elliptique

$\mathcal{O}$: point à l'infini

$E(\mathbb{K})$: ensemble des points $\mathbb{K}-$rationnels

$\triangle$: discriminant

$j(E)$: $j-$invariant

$\mathbb{K}[x,y]_3$: l'ensemble des polynômes de degré 3

$\mathbb{K}[x,y]_1$: l'ensemble des polynômes de degré 1

$\mid E(\mathbb{K}) \mid$: ordre ou cardinal de l'ensemble des points $\mathbb{F}_p-$rationnels

σ : endomorphisme de Frobenius

t : trace de Frobenius

χ_E : polynôme caractéristique de σ_E

N_n : nombre de points

Z_E : fonction Zêta associé à E

ς : fonction Zêta de Riemann

H_p : intervalle de Hasse pour p

$\left[2\sqrt{q}\right]$: partie entière de $2\sqrt{q}$.

Résumé

L'intérêt de ce mémoire est de présenter en détail les principaux résultats sur le nombre de points rationnels sur une courbe elliptique dans un corps fini.
Nous allons présenter de façon détaillée la fonction Zêta, les bornes sur le nombre de points rationnels sur une courbe elliptique, les méthodes de comptage et enfin donner une application sur le problème du logarithme discret elliptique.
Les résultats fondamentaux de Weil et Serre sont tous formulés pour les courbes elliptiques et peuvent être grossièrement résumé dans l'inégalité :

$$N_q \leqslant q + 1 + \left[2\sqrt{q}\right]$$

où N_q désigne le nombre maximum de points rationnels d'une courbe elliptique.
Nous avons utilisé des méthodes de comptage tels que la méthode du symbole de Legendre, méthode de Shanks et l'algorithme de Baby Step−Giant Step, pour lesquelles on sait déterminer le nombre de points rationnels sur une courbe elliptique dans un corps fini de caractéristique $p \geqslant 5$.

Table des matières

Introduction

L'intérêt suscité par les systèmes de chiffrement à clef publique fut le point de départ d'un nouvel engouement pour la théorie des nombres et l'arithmétique dans ses aspects calculatoires. Les courbes elliptiques ont de nombreuses applications dans des domaines très différents des mathématiques : elles interviennent ainsi en arithmétique dans la construction de grands nombres premiers, en théorie des nombres dans la démonstration du dernier théorème de Fermat (voir [2]), en cryptologie dans le problème de la factorisation des entiers (voir [2], [11]) ou pour fabriquer des codes performants (voir [11]). Pour ses applications, le calcul du nombre de points rationnels de ces courbes est une étape incontournable. Or, seule l'utilisation de courbes elliptiques d'un type particulier était dans un premier temps possible. Il s'agit essentiellement des courbes à multiplication complexe par un ordre dans un corps quadratique imaginaire de nombre de classes petit et des courbes supersingulières. Cependant, ces dernières se sont avérées désastreuses car le problème du logarithme discret y est plus facile (voir [4]).
Le but de ce mémoire est de présenter en détail les principaux résultats sur le nombre de points rationnels sur une courbe elliptique dans un corps fini.
Les objectifs spécifiques sont la présentation des résultats sur les bornes Hasse−Weil et Serre−Weil ainsi que les méthodes de comptage.
Notre mémoire est divisé en trois chapitres.
Le premier chapitre est consacré à présenter les préliminaires en rappelant quelques notions de structures algébriques (voir [1]) et quelques notions de la géométrique algébrique (voir[10],[7]), qui seront utiles tout au long de ce travail.
Le deuxième chapitre est consacré aux courbes elliptiques (voir [2],[4],[11]). On rappelle dans ce chapitre les définitions et quelques propriétés d'une courbe elliptique.
Le troisième chapitre est le coeur du sujet, consacré au nombre de points rationnels sur une courbe elliptique dans un corps fini (voir [12],[11]), [9], [13] , [1],[5],[8]). Dans ce chapitre nous présentons de façon détaillé la fonction Zêta, les bornes sur le nombre de points rationnels sur une courbe elliptique, les méthodes de comptage et enfin donner

une application sur le problème du logarithme discret elliptique.

Ce travail n'a pas seulement un intérêt théorique mais également pratique dans le sens où il intervient en cryptographie, domaine dans lequel on travaille avec des corps de très grande caractéristique.

Chapitre 1

Préliminaires

1.1 Quelques notions de structures algébriques

1.1.1 Notions de groupes

Définition 1.1

On appelle groupe tout ensemble non-vide G muni d'une loi de composition interne $*$, vérifiant les 3 propriétés suivantes (appelées axiomes de la structure de groupe) :

- *la loi $*$ est associative dans G ;*
  c'est−à−dire pour tous x, y, $z \in G$,

$$(x * y) * z = x * (y * z), \tag{1.1}$$

- *la loi $*$ admet un élément neutre dans G ;*
  c'est−à−dire qu'il existe $\mathrm{e} \in G$ tel que pour tout $x \in G$,

$$x * \mathrm{e} = \mathrm{e} * x, \tag{1.2}$$

- *tout élément de G admet un symétrique dans G pour la loi $*$;*
  c'est-à-dire pour tout $x \in G$ il existe $x' \in G$ tel que

$$x * x' = \mathrm{e} = x' * x = x. \tag{1.3}$$

Définition 1.2

On appelle groupe commutatif ou groupe abélien, tout groupe G dont la loi $*$ vérifie de plus la condition supplémentaire de la commutativité :

$$\text{pour tous } x, y \in G, \quad x * y = y * x. \tag{1.4}$$

Définition 1.3
Soient G un groupe et x un élément de G.
x est d'ordre n dans $G \iff x^n = \mathrm{e}$ et $x^m \neq \mathrm{e}$ si $1 \leqslant m < n$.

Définition 1.4
Un groupe G est dit monogène lorsqu'il est engendré par un de ses éléments, c'est-à-dire, il existe un élément $x \in G$ tel que $G = \langle x \rangle$.
Si de plus x est d'ordre fini $n \geqslant 1$, alors on dit que le groupe G est cyclique d'ordre n, et on a :

$$G = \{\mathrm{e}, x, x^2, ..., x^{n-1}\}.$$

1.1.2 Notions d'anneaux

Définition 1.5
Soient A un ensemble et deux lois $+$ et $\times$ de composition interne sur A. On dit que $(A, +, \times)$ est un anneau si :

- *$(A, +)$ est un groupe commutatif dont l'élément neutre est noté 0_A ou 0.*
- *la loi multiplicative $\times$ est associative possédant un élément neutre notée 1_A ou 1.*
- *La loi multiplication $\times$ est distributive par rapport à la loi d'addition $+$.*

Si la loi multiplicative $\times$ est commutative, on dit que l'anneau $(A, +, \times)$ est commutatif.

1.1.3 Corps

Définition 1.6
On appelle corps commutatif (ou tout simplement corps) tout anneau commutatif unitaire dans lequel tout élément non nul est inversible.

Définition 1.7
Soient K un corps et $f : \mathbb{Z} \longmapsto K$ un morphisme canonique défini par $f(n) = n1_K$. On appelle caractéristique du corps K, notée $car(K)$, l'unique entier $k \in \mathbb{N}$ tel que

$$\ker(f) = k\mathbb{Z}.$$

Exemple 1.1
- *Les corps usuels $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulles.*
- *Pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.*

Définition 1.8 *Un corps fini est un corps commutatif dont le nombre d'éléments est fini.*

Exemple 1.2
Si p est un entier premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps fini, noté $\mathbb{F}_p$:

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

En particulier, on a $\mathbb{F}_2 = \{0, 1\}$, $\mathbb{F}_3 = \{0, 1, 2\}$.

Remarque 1.1 (Règle de calcul dans $\mathbb{F}_p$)
- $\forall\ x\ \in\ \mathbb{F}_p, \quad px = 0$;
- $\forall\ x\ \in\ \mathbb{F}_p, \quad x^p = x\ et \forall\ x\ \in\ \mathbb{F}_p \backslash \{0\}, \quad x^{p-1} = 1.$

Proposition 1.1 (Quelques propriétés importantes des corps finis)
i. Le cardinal de tout corps fini est de la forme $q = p^n$,où p est premier et $n\ \in\ \mathbb{N}$.
ii. Un corps fini est de caractéristique non nulle ; on le note le plus souvent $\mathbb{F}_p$ où p est un premier.

1.1.4 Congruence modulo n

Définition 1.9
Soit n un entier strictement positif. On dit que a congru b modulo n si $a - b$ est un multiple de n. Cette relation se note $a \equiv b \mod n$ ou $a \equiv b\ [n]$.

Remarque 1.2
• *On peut reformuler la définition ci dessus par :*
$a \equiv b \mod n \Longleftrightarrow \exists\ k\ \in\ \mathbb{K} : a = b + kn.$
• *n divise a si et seulement si $a \equiv 0 \mod n$.*
• *si r est le reste de la division euclidienne de a par n alors $a \equiv r \mod n$ avec $0 \leq r < n$.*

1.2 Quelques Notions de Géométrie Algébrique

Dans la totalité de cette section, nous considérons un corps k commutatif.
Nous présentons dans cette section quelques notions de base de la géométrie algébrique.

1.2.1 Variété affine

Définition 1.10
On appelle espace affine de dimension n sur k, et on note $\mathbb{A}^n(k)$ ou $\mathbb{A}^n$, l'ensemble k^n produit cartésien itéré n fois du corps k.

Les éléments de l'espace affine sont appelés points.
$\mathbb{A}^1$ et $\mathbb{A}^2$ sont appelés respectivement droite affine et plan affine.
Un point a est dit zéro de $P \in k[X_1, ..., X_n]$ si $P(a) = 0$.

Définition 1.11 (Ensemble algébrique affine)
Soit S un ensemble quelconque de $k[X_1, ..., X_n]$. On pose

$$V(S) = \{a \in \mathbb{A}^n \mid \forall P \in S,\ P(a) = 0\}$$

de sorte que les $a \in V(S)$ sont les zéro communs de tous les polynômes de S.
On dit que $V(S)$ est l'ensemble algébrique affine défini par S.

Définition 1.12
On appelle hypersurface définie par un polynôme P, notée $V(P)$, l'ensemble des zéros de P (pour P non constant et k algébriquement clos). Le degré de $V(P)$ est le degré de P. Une courbe algébrique plane est une hypersurface du plan affine. Un hyperplan est une hypersurface définie par P de degré 1. Une droite est un hyperplan de $\mathbb{A}^n$.

Définition 1.13 (Idéal d'un ensemble de points)
Soit A une partie $\mathbb{A}^n$. On appelle l'idéal de A dans $\mathbb{A}^n$, l'ensemble noté $I(A)$ défini par :

$$I(A) = \{P \in k[X_1, ..., X_n] \mid \forall a \in A,\ P(a) = 0\}.$$

On voit que clairement $I(A)$ est l'ensemble des polynômes nuls sur A.

1.2.2 Variété projective

Considérons la relation $\mathcal{R}$ sur $k^{n+1} - \{0\}$ définie par :
pour tous vecteurs non nuls x et y, on a

$x\mathcal{R}y$ si, et seulement si ils sont colinéaires, i.e.,

$$x\mathcal{R}y \Longleftrightarrow \exists\ \lambda \in k^* : y = \lambda x.$$

La relation $\mathcal{R}$ est une relation d'équivalence sur $k^{n+1} - \{0\}$. Ainsi, deux vecteurs non nuls sont équivalents s'ils sont colinéaires.

Définition 1.14
On appelle espace projectif de dimension n sur k, et l'on note $\mathbb{P}^n$ *(ou* $\mathbb{P}^n(k)$ *ou encore* $\mathbb{P}(k^{n+1})$*), l'ensemble des classes d'équivalence par* $\mathcal{R}$*.*

En d'autres termes, $\mathbb{P}^n$ est l'ensemble des droites vectorielles de k^{n+1}.

Remarque 1.3

i. Si un point $P \in \mathbb{P}^n$ *a pour vecteur directeur* $(x_0, ..., x_n) \in k^{n+1} - \{0\}$*, on écrit* $P = (x_0 : \ldots : x_n)$*; on dit que* $(x_0 : ... : x_n)$ *est un système de coordonnés homogènes de* P*.*

ii. On dit que $\mathbb{P}^1$ *est la droite projective sur k et que* $\mathbb{P}^2$ *est le plan projectif sur k.*

iii. On dit que P *est zéro de* $F \in k[X_1, \ldots, X_n]$ *si* $F(P) = 0$*; pour tout choix de coordonnées homogènes* $(x_0 \ldots : x_n)$ *de* P*,* $F(P) = 0$ *et noté* $F(x_0, \ldots, x_n) = 0$*.*

iv. Si E *est un k-espace vectoriel de dimension n, on définit de la même manière l'espace projectif associé à* E *noté* $\mathbb{P}(E)$ *de dimension* $n - 1$*.*

Cette proposition suivante illustre, l'une des propriétés fondamentales de l'espace projectif ; il n'y a pas de sous−espace parallèles, ils se rencontrent à l'infini.

Proposition 1.2
Soient $\mathbb{P}(F)$ *et* $\mathbb{P}(F')$ *deux sous−espaces linéaires de* $\mathbb{P}^n$ *de dimensions respectives* r *et* r' *vérifiant* $r + r' \geq n$*.*
Alors $\mathbb{P}(F) \cap \mathbb{P}(F') = \mathbb{P}(F \cap F')$ *est un sous−espace linéaire de dimension* $\geq r + r' - n$*; il est en particulier non vide.*

Preuve. Ecrivons $\mathbb{P}^n(k) = \mathbb{P}(E)$, on a $dimF = r + 1$, $dimF' = r' + 1$ et $dimE = n + 1$. $dim(F \cap F') = dim(F) + dim(F') - dim(F + F')$; or $F + F'$ est un sous espace-vectoriel de E, d'où $dim(F + F') \leq dimE$, et par suite $dim(F \cap F') \geq dim(F) + dim(F') - dimE = r + r' - n + \geq r + r' - n$.
Ainsi on en déduit l'inégalité $dim(F \cap F') \leq r + r' - n$.

1.2.3 Points et Courbes lisses

Définition 1.15 *(dimension d'une variété algébrique)*
On dit qu'un ensemble algébrique X *est de dimension pure* n *ou équidimensionnel de dimension* n*, si chaque composante irréductible de* X *est de dimension* n*. Si* x *est un point de* X*, on appelle dimension de* X *en* x*, et l'on note* $dim_x X$*, le maximum des dimensions des composantes irréductibles de* X *passant par* x*.*

Proposition 1.3
Un ensemble algébrique est de dimension 0 *si et seulement si il consiste en un nombre fini de points.*

Preuve. Soit X un ensemble algébrique de dimension 0. Tout fermé irréductible contenant un point est réduit à ce point, donc les composantes irréductibles de X sont des points. La condition suffisante est évidente.

Remarque 1.4 *Une variété algébrique de dimension* 1 *(resp.* 2*) est appelée une courbe (resp. surface)*

On admet le résultat suivant :

Proposition 1.4
Tout ensemble algébrique X est de dimension finie, et tout ouvert dense dans X est de même dimension que X.

Définition 1.16 *(Espace tangent de Zariski)*
Soit X une sous-variété de $\mathbb{A}^n$. On définit l'espace tangent de Zariski à X en un point P, que l'on note $T_P(X)$, comme l'espace vectoriel défini par les équations :

$$\sum_{i=1}^{n} \frac{\partial F}{\partial x_i}(P)x_i = 0 \tag{1.5}$$

pour tout F dans l'idéal $I(X)$.
L'espace affine correspondant passant par $P = (p_1, \ldots, p_n)$ est défini par :

$$\sum_{i=1}^{n} \frac{\partial F}{\partial x_i}(P)(x_i - p_i) = 0. \tag{1.6}$$

Définition 1.17 *(Points lisses et Points singuliers)*
Soit x un point d'une variété (irréductible) X. On dit que x est lisse sur X (ou que X est lisse en x ou x est régulier) si $dimT_xX = dim_xX$. Un point qui n'est pas lisse est dit point singulier.
On dit que X est non singulier (ou régulière ou lisse) si elle l'est à chacun de ses points. L'ensemble des points singuliers de X est un fermé propre de X, appelé lieu de X et noté $SingX$. L'ouvert complémentaire de $SingX$ est noté X_{lisse}.

Remarque 1.5

- *Les points singuliers d'une hypersurface dans $\mathbb{A}^n$ d'idéal engendré par un polynôme F sont définis par les équations :*

$$F(x) = \frac{\partial F}{\partial x_1}(x) = ... = \frac{\partial F}{\partial x_n}(x) = 0. \tag{1.7}$$

- *Les points singuliers d'une hypersurface X dans $\mathbb{P}^n$ d'idéal engendré par un polynôme homogéne F de degré d sont définis par les équations :*

$$F(x) = \frac{\partial F}{\partial x_0}(x) = ... = \frac{\partial F}{\partial x_n}(x) = 0. \tag{1.8}$$

Il faut noter que si la caractéristique de k ne divise pas d, alors les points singuliers sont définis par $n+1$ équations :

$$\frac{\partial F}{\partial x_0}(x) = ... = \frac{\partial F}{\partial x_n}(x) = 0. \tag{1.9}$$

Définition 1.18
Soit $C = V(F)$ une courbe plane projective. On dit que C est définie sur k, et on note C/k, si F est à coefficients dans k.
L'ensemble des points k-rationnels de C est

$$C(k) = C \cap \mathbb{P}^n(k).$$

Remarque 1.6
Soient U_2 et L_∞ les ensembles définis par :

$$U_2 = \left\{(X : Y : Z) \in \mathbb{P}^2 \mid Z \neq 0\right\}. \tag{1.10}$$

$$L_\infty = \left\{(X : Y : Z) \in \mathbb{P}^2 \mid Z = 0\right\}. \tag{1.11}$$

On voit clairement que $\mathbb{P}^2$ est la réunion disjointe

$$\mathbb{P}^2 = U_2 \cup L_\infty$$

du plan affine U_2 et de la droite à l'infinie L_∞.
Un point de L_∞ est appelé point à l'infini que l'on notera P_∞. Le plan projectif $\mathbb{P}^2$ peut donc être vu comme le plan affine auquel on adjoint un point à l'infini par famille de droites parallèles.

Proposition 1.5
Soit $C = V(F)$ une courbe projective plane. On a les équivalences suivantes :
C est irréductible $\iff$ C est une variété projective $\iff$ F est irréductible.

1.3 Théorème de Bézout

On considère deux polynômes homogènes non nuls F, G de $k[X,Y,Z]$, sans facteur commun, de degrés respectifs s et t.

1.3.1 Multiplicité d'intersection en projectif

Soit $P=(x,y,z)\in\mathbb{P}^2$. L'une des coordonnées de P est non nulle, on peut supposer que c'est z, et même que l'on a $z=1$. On considère alors les polynômes déshomogénéisés F^* et G^* respectivement de F et G par rapport à Z (par exemple $F^*(X,Y)=F(X,Y,1)$).

Définition 1.19
On peut définir la multiplicité d'intersections de F et G en P par

$$\mu_P(F,G)=\mu_{(x,y)}(F^*,G^*). \tag{1.12}$$

1.3.2 Enoncé du théorème

Théorème 1.1 (Bézout)
Soient F, $G\in k[X,Y,Z]$ deux polynômes homogènes sans facteur commun, de degrés respectifs s et t. On a

$$\sum_{P\in V(F)\bigcap V(G)}\mu_P(F,G)=st. \tag{1.13}$$

(On peut aussi étendre la somme à tous les points de $\mathbb{P}^2$ puisque si $P\notin V(F)\cap V(G)$, la multiplicité est nulle).

1.4 Genre d'une Courbe Algébrique Projective

Définition 1.20
Soit $C\subset\mathbb{P}^n$ une courbe projective irréductible. Le nombre d de points d'intersections de C(comptés avec leur multiplicité) avec un hyperplan H ne contenant pas C est appelé le degré de C.

Définition 1.21
Soit $C\subset\mathbb{P}^n$ une courbe projective irréductible définie sur $\mathbb{F}_q$ et Q un point singulier.
Le degré de singularité de C, notée δ, est est défini par la formule

$$\delta=\sum_{Q\in Sing(C)}\delta_Q. \tag{1.14}$$

où δ_Q est le degré de singularité au point Q.

Définition 1.22

Soit C une courbe projective, X sa normalisée. On appelle genre géométrique de C, le genre arithmétique de X.

Définition 1.23

Soit $C \subset \mathbb{P}^n$ une courbe projective irréductible définie sur $\mathbb{F}_q$. Le genre arithmétique π de C est l'entier :

$$\pi := g + \delta,$$

où g est le genre géométrique de C.

Remarque 1.7

1. *Il est évident que $\pi = g$ si et seulement si C est une courbe lisse.*
2. *Si C est une courbe plane de degré $d \geq 2$, alors*

   $$\pi = \tfrac{(d-1)(d-2)}{2}$$

   Il s'ensuit que dans ce cas, le genre géométrique de C est donné par la formule

   $$g = \frac{(d-1)(d-2)}{2} - \sum_{Q \in Sing(C)} \delta_Q. \tag{1.15}$$

3. *Si C est une courbe projective plane irréductible de degré $d \geq 2$ qui n'a que des singularités ordinaires alors, on a la formule :*

   $$g = \tfrac{(d-1)(d-2)}{2} - \textstyle\sum_{P \in C} \frac{\mu_p(\mu_p - 1)}{2}$$

où μ_p est la multiplicité de C en P.

Chapitre 2

Courbe Elliptique

La théorie des courbes elliptiques a connu un récent regain d'intérêt grâce à l'émergence de la cryptographie. Tout à commencé lorsque Lenstra a découvert un algorithme de factorisation polynomial sur ces structures. Ensuite, en 1985, Koblitz et Miller ont proposé indépendamment d'adapter les prototypes cryptographiques existants sur les courbes elliptiques.

2.1 Définitions et Invariants

2.1.1 Définitions

Définition 2.1
Une courbe elliptique est une paire $(E, \mathcal{O})$, oú E est une cubique irréductible et non singulière et $\mathcal{O} \in E$. La courbe elliptique est définie sur un corps $\mathbb{K}$ si E est une courbe sur $\mathbb{K}$ et $\mathcal{O} \in E(\mathbb{K})$.

Définition 2.2
Une courbe elliptique sur $\mathbb{K}$ est définie comme l'ensemble des solutions du plan $\mathbb{P}^2(\mathbb{K})$ de l'équation de Weierstrass suivante :

$$E : F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0 \quad (2.1)$$

oú les coefficients $a_1,\ a_2,\ a_3,\ a_4$ et a_6 sont dans $\mathbb{K}$.
Pour alléger la notation, nous allons écrire l'équation de Weierstrass avec des coordonnées non homogènes : $x = X/Z$ et $y = Y/Z$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (2.2)$$

plus le point à l'infini $\mathcal{O} = (0, 1, 0)$.

Remarque 2.1
$\mathcal{O}$ est le seul point à l'infini et n'est pas singulier, car $(\partial F/\partial Z)(0, 1, 0) = 1 \neq 0$.

Proposition 2.1
Une courbe elliptique est une courbe algébrique projective lisse de genre 1.

2.1.2 Invariants

Définition 2.3
Soit $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *une courbe elliptique définie sur* $\mathbb{K}$.
On pose :

$$b_2 = a_1^2 + 4a_2; b_4 = a_1a_3 + 2a_4; b_6 = a_3^2 + 4a_6; b_8 = a_1^2a_6 - a_1a_3a_4 + a_1a_3^2 - a_4^2. \quad (2.3)$$

Le nombre

$$\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \quad (2.4)$$

est appelé le discriminant de E. Il est souvent noté $\triangle_E$ *ou encore* $\triangle(E)$.

Proposition 2.2
Soit E une courbe donnée par une équation de Weierstrass. Alors E est non singulière si et seulement si $\triangle \neq 0$.

Preuve. $\Longleftarrow$) Soit l'équation générale de Weierstrass :

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

On sait que le point à l'infini $\mathcal{O} = (0, 1, 0)$ n'est jamais singulier.
Par absurde, supposons que E soit singulier en un point $P_0 = (x_0, y_0)$. Par changement de variable $(x, y) \longmapsto (x - x_0, y - y_0)$, nous ramenons le point P en $(0, 0)$. Ainsi nous avons $a_6 = f(0, 0) = 0$, $a_4 = (\partial f/\partial x)(0, 0) = 0$ et $a_3 = (\partial f/\partial Y)(0, 0) = 0$. La courbe E a donc pour équation :

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 = 0. \quad (2.5)$$

Le discriminant de cette équation est nul ; ce qui contredit l'hypothèse.
$\Longrightarrow$) Pour simplifier les calculs, nous allons supposer le caractéristique $p \neq 2,\ 3$. Soit la courbe E donnée par l'équation de Weierstrass :

$$E : y^2 = x^3 + a_4x + a_6.$$

Si la courbe est singulière en un point $P_0 = (x_0, y_0)$, alors $2y_0 = 0 \Longrightarrow y_0 = 0$ et $3x_0^2 + a_4 = 0 \Longrightarrow x_0^2 = -\frac{a_4}{3}$. Or le point $P_0 = (x_0, y_0)$ est un point de la courbe, par conséquent $y_0^2 = 0 = x_0^3 + a_4 x_0 + a_6 = \frac{2}{3} a_4 x_0 + a_6$. Il s'ensuit que $x_0^2 = \frac{9a_6^2}{4a_4^2} = -\frac{a_4}{3}$ et donc $\triangle = -16(4a_4^3 + 27a_6^2) = 0$.
Si $p = 2$ *ou* 3, la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes.

Définition 2.4
On appelle $j-$invariant d'une courbe elliptique E définie sur un corps $\mathbb{K}$,

$$j(E) = \frac{c_4^3}{\triangle(E)} \quad o\acute{u} \quad c_4 = d_2^2 + 24d_4. \tag{2.6}$$

Proposition 2.3
Soit un corps $\mathbb{K}$ de caractéristique p. Une courbe E définie sur $\mathbb{K}$ donnée par une équation de Weierstrass prend alors une forme simplifiée :

1. *Si $p \neq 2$ et $p \neq 3$,*

$$y^2 = x^3 + a_4 x + a_6; \quad \triangle = -16(4a_4^3 + 27a_6^2); \tag{2.7}$$

$$j(E) = 1728 \frac{4a_4^3}{a_4^3 + 27a_6^2}.$$

2. *Si $p \neq 2$ et $j(E) \neq 0$,*

$$y^2 + xy = x^3 + a_2 x^2 + a_6; \quad \triangle = a_6; \quad j(E) = \frac{1}{a_6}. \tag{2.8}$$

3. *Si $p = 2$ et $j(E) = 0$,*

$$y^2 + a_3 y = x^3 + a_4 x + a_6; \quad \triangle = a_4^3; \quad j(E) = 0. \tag{2.9}$$

4. *Si $p = 3$ et $j(E) \neq 0$,*

$$y^2 = x^3 + a_2 x^2 + a_6; \quad \triangle = -a_2^3 a_6; \quad j(E) = -\frac{a_2^3}{a_6}. \tag{2.10}$$

5. *Si $p = 3$ et $j(E) = 0$,*

$$y^2 = x^3 + a_4 x + a_6; \quad \triangle = -a_4^3; \quad j(E) = 0. \tag{2.11}$$

2.2 Points rationnels et loi de groupe

2.2.1 Points rationnels

Dans cette partie, on considère une courbe elliptique E définie sur $\mathbb{K}$ par :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{2.12}$$

Définition 2.5

Un point de E est dit rationnel sur $\mathbb{K}$ s'il appartient à $E \cap \mathbb{P}^2(K)$. L'ensemble des points $\mathbb{K}-$rationnels de E, noté $E(\mathbb{K})$ est :

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}. \qquad (2.13)$$

Exemple 2.1

Soit E la courbe elliptique définie sur $\mathbb{F}_5$ d'équation :

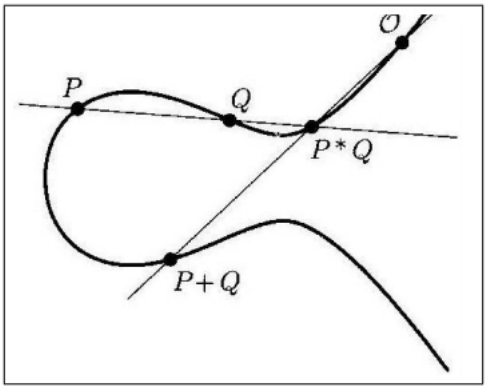
$$y^2 = x^3 + x + 1.$$

L'ensemble des points $\mathbb{F}_5-$rationnels de E est

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)\}.$$

2.2.2 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 $R = P * Q$. En ayant choisi, une origine $\mathcal{O}$ sur la courbe E qui sera l'élément neutre de la loi 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 $\mathcal{O}$ et R.



Graphe de la loi de group sur les courbs elliptiques

Proposition 2.4

Soient E une courbe elliptique et une droite L définies sur un corps $\mathbb{K}$. Si E a deux points d'intersections avec la droite L, alors E a trois points d'intersections avec la droite L.

Preuve. Soit une droite L définie sur un corps $\mathbb{K}$ par $L : ax + by + cz = 0$, où, par symétrie, nous supposons que $c \neq 0$ tel que $E \cap L$ a un nombre fini de points. Les points d'intersections de E et L sont les racines du polynôme.

$$q(x, y) = p(x, y, -\frac{ax + by}{c}) \in \mathbb{K}[x, y]_3. \tag{2.14}$$

Notons $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ (avec éventuellement $P_1 = P2$), deux points d'intersections de E avec L, alors comme, $q(a_1, b_1) = q(a_2, b_2) = 0$, il vient que

$$q(x, y) = v(x, y) \prod_{i=1}^{2} (b_i x - b_i y) \text{ où } v(x, y) \in \mathbb{K}[x, y]_1. \tag{2.15}$$

Le troisième point d'intersection de E avec L est alors donné par :

$$P_3 = (a_3, b_3, -\frac{aa_3 + bb_3}{c}) \tag{2.16}$$

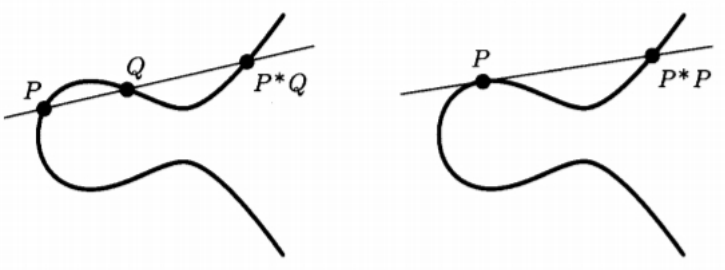
où (a_3, b_3) est l'unique racine de $v(x, y)$.

Remarque 2.2 *:*

Cette proposition permet de définir la loi de composition de la sécante−tangente :

1. *Si $P, Q \in E(\mathbb{K})$ et $P \neq Q$, alors nous définissons $L = PQ$, la droite sécante qui passe par P et Q. Par la proposition précédente, nous savons qu' il existe un troisième point $P * Q$ unique qui appartient à $E \cap L$.*

2. *Si $P \in E(\mathbb{K})$, alors nous définissons $L = PP$, la droite tangente à E qui passe par P. Par la proposition précédente, nous savons qu'il existe un troisième point $P * P$ unique qui appartient à $E \cap L$.*



Proposition 2.5

L'ensemble $E(\mathbb{K})$ est un groupe abélien si on le munit de la loi d'addition $+$ suivante :

- *Pour tout point $P = (x_P, y_P)$ de $E(\mathbb{K})$,*

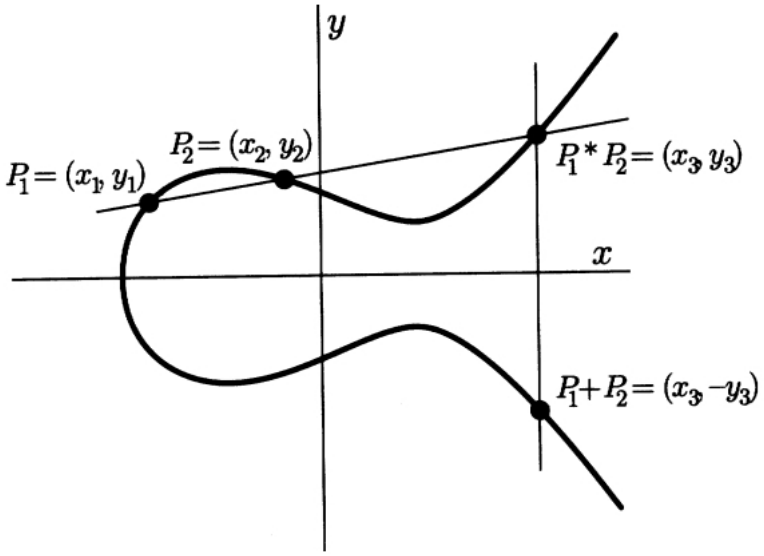
$$P + \mathcal{O} = \mathcal{O} + P = P \text{ et } -P = (x_P, -y_P - a_1 x_P - a_3).$$

- *Pour tous points $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ de $E(\mathbb{K})$ avec $P \neq Q$, les coordonnées (x_{P+Q}, y_{P+Q}) du point $R = P + Q$ sont égales à :*

$$\begin{cases} x_{P+Q} = \lambda^2 + a_1\lambda - a_2 - x_P - x_P, \\ y_{P+Q} = -(\lambda + a_1)x_{P+Q} - \nu - a_3, \end{cases} \tag{2.17}$$

avec

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & si\ P \neq Q \\ \frac{3x_P^2 + 2a^2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x + a_3} & sinon \end{cases} \quad et \quad \nu = y_P - \lambda x_P. \tag{2.18}$$



Exemple 2.2 *Soit E la courbe elliptique définie sur $\mathbb{F}_{23}$ d'équation*

$$y^2 = x^3 + x + 1.$$

Prenons $P = (3, 10)$ et $Q = (9, 7)$ deux points de $E(\mathbb{F}_{23})$.

– *Calculons $R = P + Q$.*

Les formules précédentes donnent,

$\lambda = \frac{7-10}{9-3} = -\frac{3}{6} = -\frac{1}{2} = 11 \in \mathbb{F}_{23}$ *et* $\nu = 10 - 3.11 = -23 = 0 \in \mathbb{F}_{23}$.

$$\begin{cases} x_R = 17 \in \mathbb{F}_{23} \\ y_R = 20 \in \mathbb{F}_{23}. \end{cases}$$

Par conséquent, $R = (17, 20)$.

– *Calculons maintenant* $R = 2P$.
Les formules précédentes donnent, $\lambda = 6 \in \mathbb{F}_{23}$ *et* $\nu = 15 \in \mathbb{F}_{23}$.
$$\begin{cases} x_R = 7 \in \mathbb{F}_{23} \\ y_R = 12 \in \mathbb{F}_{23}. \end{cases}$$
Par conséquent, $R = (7, 12)$.

Proposition 2.6
Soit E *une courbe elliptique définie sur* $\mathbb{K}$. *Pour tous* P_1, P_2, Q_1 *et* $Q_2 \in E(\mathbb{K})$, *nous avons*

$$(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2). \tag{2.19}$$

Preuve. (voir [2])

Théorème 2.1 *(De Poincaré)*
Soient un corps $\mathbb{K}$, E *une courbe elliptique définie sur* $\mathbb{K}$, P *et* Q *deux points de cette courbe. Alors l'opération*

$$P + Q = \mathcal{O} * (P * Q) \tag{2.20}$$

définit une structure de groupe commutatif ayant comme élément neutre $\mathcal{O}$.

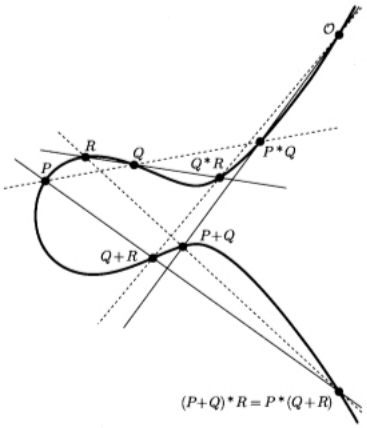
Preuve. La loi $+$ est bien définie, car $P + Q$ est l'intersection d'une courbe et d'une droite ; c'est à dire un point de la courbe.

a. Vu la définition de la loi de composition de la sécante-tangente, la commutativité est évidente :
$$P + Q = \mathcal{O} * (P * Q) = (\mathcal{O} * P) * Q = Q + P \ .$$
b. $\mathcal{O}$ est l'élément neutre. En effet,
$$P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = P.$$
$$\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = P.$$
c. Tout point P possède un inverse pour la loi $+$. Vérifions que le point
$$-P = (\mathcal{O} * \mathcal{O}) * P$$
est bien l'inverse de P :
$$P + (-P) = \mathcal{O} * (P * ((\mathcal{O} * \mathcal{O}) * P) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} * \mathcal{O} = \mathcal{O}.$$
$$-P + P = \mathcal{O} * (((\mathcal{O} * \mathcal{O})) * P) * P = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} * \mathcal{O} = \mathcal{O}.$$

d. Enfin la loi + est associative. En effet, P, Q et R sont trois points de la courbe, on a :

$$\begin{aligned} P*(Q+R) &= P*(\mathcal{O}*(Q*R)) \\ &= (P*Q)*Q)*(\mathcal{O}*(Q*R)) \qquad car \quad P=(P*Q)*Q \\ &= ((P*Q)*\mathcal{O})*(Q*(Q*R) \\ &= ((P*Q)*\mathcal{O})*R \qquad car \quad R=Q*(Q*R) \\ &= (\mathcal{O}*(P*Q))*R \\ &= (P+Q)*R \end{aligned} \tag{2.21}$$

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



2.2.3 Les Théorèmes fondamentaux : Mordell−Weil et Siegel

Nous présentons quelques théorèmes fondamentaux sur les courbes elliptiques :

Théorème 2.2 *(Mordel−Weil, première version)*
Si E est une courbe elliptique, il existe un ensemble fini de points rationnels tels que tous les points rationnels de E se déduisent de cet ensemble fini par le procédé corde et tangente.
Le nombre minimal de points rationnels s'appelle le rang de la courbe.

La deuxième version de ce théorème définit plus précisément le rang de la courbe.

Théorème 2.3 *(Mordel−Weil, deuxième version)*
Le groupe $E(\mathbb{K})$ associé à une courbe elliptique est de type fini.

Il est donc de la forme $\mathbb{Z}^r \times \mathbb{Z}|\alpha_1\mathbb{Z} \times \cdots \times \mathbb{Z}|\alpha_t\mathbb{Z}$. *L'entier* r *est appelé le rang de la courbe.*

Théorème 2.4 *(Siègel)*
Une courbe elliptique n'a qu'un nombre fini de points entiers.

2.2.4 Structure du groupe des points rationnels sur un corps fini

Dans le cas où $\mathbb{K}$ est un corps fini $\mathbb{F}_q$, la structure de groupe des points $\mathbb{F}_q-$rationnels est donnée par :

Théorème 2.5
Le groupe $E(\mathbb{F}_q)$ *est soit cyclique ou produit de deux groupes cycliques. Dans le premier cas, on a :*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}|d_2\mathbb{Z}$$

où $d_2 = |E(\mathbb{F}_q)|$.
Dans le second cas, on a :

$$E(\mathbb{F}_q) \simeq \mathbb{Z}|d_1\mathbb{Z} \times \mathbb{Z}|d_2\mathbb{Z}$$

où $d_1|d_2 \quad et \quad d_1|q-1$.

Preuve.

- Le premier cas est évident. En effet, le groupe $\mathbb{Z}|d_2\mathbb{Z}$ est cyclique d'ordre d_2, c'est−à−dire isomorphe à $E(\mathbb{F}_q)$.

- D'après le théorème des structures de groupes abélien, il existe des entiers uniques non nuls $d_1 \cdots d_r$ tel que le groupe $E(\mathbb{K})$ soit isomorphe au groupe produit
$$\mathbb{Z}|d_1\mathbb{Z} \times \cdots \times \mathbb{Z}|d_r\mathbb{Z} \quad \text{et} \quad d_1 \text{ divise } d_{i+1}$$
Pour chaque indice i, vu que d_1 divise d_i, le groupe $\mathbb{Z}|d_1\mathbb{Z}$ contient d_1 éléments d'ordre divisant d_1.
Il reste à établir que d_1 divise $q-1$. On remarque que $\mathbb{Z}|d_2\mathbb{Z}$ contient un sous-groupe isomorphe à $\mathbb{Z}|d_1\mathbb{Z}$, car $(d_1|d_2)$. Ainsi $E(\mathbb{K})$ contient un sous-groupe isomorphe à $\mathbb{Z}|d_1\mathbb{Z} \times \mathbb{Z}|d_1\mathbb{Z}$. D'où le résultat.

Exemple 2.3 *Sur* $\mathbb{K} = \mathbb{F}_5$, *on définit la courbe elliptique* E *par :*

$$y^2 = x^3 + 4x + 1.$$

Les points $E(\mathbb{F}_5)$ sont donnés par :

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (1,1), (1,4), (3,0), (4,1), (4,4)\}.$$

Par exemple (0,1) est d'ordre 8 et le groupe $E(\mathbb{F}_5)$ est cyclique engendré par le (0,1)(ou par (0,4),(1,1)et (1,4)).

Théorème 2.6 *(Hasse– Weil)*
Soit E une courbe elliptique définie sur $\mathbb{F}_q$, on a :

$$|E(\mathbb{F}_q)| = q + 1 - t \quad où \quad |t| \leq 2\sqrt{q}. \tag{2.22}$$

Remarque 2.3
De plus, si p est un nombre premier, alors pour toute valeur entière de t dans l'intervalle $[-2\sqrt{p}, 2\sqrt{p}]$, il existe une courbe elliptique E définie sur $\mathbb{F}_p$ telle que $|E(\mathbb{F}_p)| = p+1-t$. Supposons que nous connaissons un point $G \in \mathbb{F}_q$ ainsi que son ordre $l \in \mathbb{N}$, alors si $l > \frac{q+1}{2} + \sqrt{q}$, le théorème de Hasse– Weil montre que le groupe $E(\mathbb{F}_q)$ est cyclique engendré par G et que ce groupe est d'ordre l. L'utilisation directe de ce procédé est ce pendant assez rare car, en principe, on calcule d'abord l'ordre du groupe $E(\mathbb{F}_q)$ et on l'utilise pour trouver l'ordre du point G.

Définition 2.6
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

$$\sigma_E : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$$
$$P \longmapsto \begin{cases} \mathcal{O} & si \quad P = \mathcal{O} \\ (X^q, Y^q) & si \quad P = (X,\ Y). \end{cases} \tag{2.23}$$

Définition 2.7
L'entier t défini dans le théorème précédent est appelé la trace Frobenius ou la trace de l'endomorphisme de Frobenius.

On peut caractériser les courbes supersingulières grâce à ce nombre t.

Proposition 2.7
Soient $\mathbb{K} = \mathbb{F}_q$ un corps fini de caractéristique p, E une courbe elliptique définie sur $\mathbb{K}$ et

t la trace de Frobenius associée à E. La courbe elliptique E est supersingulière si $p \mid t$. En particulier si p=2 ou 3 la courbe est supersingulière si et seulement si $j(E) = 0$. Si $p \geq 5$ premier, la courbe E est supersingulière si et seulement si $t = 0$.

Si E est une courbe elliptique sur $\mathbb{F}_q$ et si t désigne la trace de Frobenius, on pose :

$$\chi_E(T) = T^2 - tT + q, \tag{2.24}$$

si de plus $|E(\mathbb{F}_q)| = \chi_E(1)$. Le polynôme $\chi_E(T)$ est le polynôme caractéristique de l'endomorphisme de Frobenius, on a :

$$\chi_E(\sigma_q) = \mathcal{O} \text{ (i.e endomorphisme nul)}$$

C'est−à−dire pour tout point P $\in E(\overline{\mathbb{F}_q})$ on a :

$$\sigma_q^2 \cdot P - t\sigma_q \cdot P + qP = \mathcal{O}. \tag{2.25}$$

De plus t est l'unique entier r tel que $\sigma_q^2 \cdot P - r\sigma_q \cdot P + qP = \mathcal{O}$.
Si on écrit $P = (x, y)$, cette dernière égalité s'écrit aussi :

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x, y) = \mathcal{O}. \tag{2.26}$$

Théorème 2.7
Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soient λ_1 et $\lambda_2 = \overline{\lambda_1}$ les racines complexes du polynôme $\chi_E(T)$. Pour tout $n \geq 1$, on a :

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \lambda_1 - \lambda_2. \tag{2.27}$$

Ce théorème permet donc de calculer l'ordre du groupe $|E(\mathbb{F}_{q^n})|$ dès que l'on connait l'ordre de $|E(\mathbb{F}_q)|$.
Demonstration commençons par établir que ${\lambda_1}^n + {\lambda_2}^n$ est un entier. C'est une conséquence directe du lemme suivant.

Lemme 2.1 *Pour tout $k \in \mathbb{N}$ posons $s_k = {\lambda_1}^n + {\lambda_2}^n$. On a :*

$$s_0 = 2, \quad s_1 = t, \quad s_{k+1} = ts_k - qs_{k-1}.$$

Preuve. On a $X^2 - tX + q = (X - \lambda_1)(X - \lambda_2)$ d'où $t = \lambda_1 + \lambda_2$. Considérons un entier $k \geq 1$. On a ${\lambda_1}^2 - t\lambda_1 + q = 0$, d'où

$${\lambda_1}^{k+1} - t{\lambda_1}^k + q{\lambda_1}^{k-1} = 0$$

puis le résultat en additionnant cette égalité avec la même obtenue en remplaçant λ_1 par λ_2.

Preuve. (Du théorème (2.7))

Posons

$$f = (X^n - {\lambda_1}^n)(X^n - {\lambda_2}^n) = X^{2n} - ({\lambda_1}^n + {\lambda_2}^n)X^n + q^n \in \mathbb{Z}[X].$$

Puisque $(X-\lambda_1)$ et $(X-\lambda_2)$ divisent respectivement $(X^n-\lambda^n)$ et $(X^n-\lambda^n)$, le polynôme est divisible par $X^2 - tX + q$. Puisque ce dernier est unitaire , il existe $H \in \mathbb{Z}[X]$ tel que :

$$f = (X^2 - tX + q)H.$$

Dans l'anneau $\mathbb{Z}[\phi_q]$, on obtient ainsi

$$\sigma_q^2 - ({\lambda_1}^n + {\lambda_2}^n){\sigma_q}^n + q^n\sigma_q = f(\sigma_q) = (\sigma_q^2 - t\sigma_q + q)H(\sigma_q) = 0. \tag{2.28}$$

D'après l'égalité (2.26) appliqué avec le corps $\mathbb{F}_{q^n}$, il existe un unique entier r tel que

$$\sigma_{q^n}^2 - r\sigma_{q^n} + q^n = 0 \tag{2.29}$$

et on a (la formule de (Hasse) :

$$r = q^n + 1 - |E(\mathbb{F}_{q^n})|. \tag{2.30}$$

Il en résulte alors des égalitées (2.29) et (2.30) que l'on a $r = {\lambda_1}^n + {\lambda_2}^n$ d'où le résultat.

Chapitre 3

Nombre de Points Rationnels d'une Courbe Elliptique dans un Corps Fini

3.1 Fonction Zêta associée à une courbe elliptique

La fonction *Zêta* d'une courbe elliptique sur un corps fini est en quelque sorte une fonction génératrice rassemblant les informations sur le nombre de points de la courbe dans toutes les extensions (finies) du corps de base.

Définition 3.1 *Soit E une courbe elliptique définie dans un corps fini $\mathbb{F}_q$. Soit*

$$N_n = |E(\mathbb{F}_{q^n})|$$

le nombre de points sur E dans $E(\mathbb{F}_{q^n})$. La fonction Zêta associée à E est définie par :

$$Z_E(T) = \exp(\sum_{n=1}^{+\infty} \frac{N_n}{n} T^n). \tag{3.1}$$

Théorème 3.1 ***(Weil, 1948)***
Soit E une courbe elliptique définie dans $\mathbb{F}_q$, et soit $|E(\mathbb{F}_q)| = q + 1 - t$. Alors

$$Z_E(T) = \frac{qT^2 - tT + 1}{(1-T)(1-qT)} \tag{3.2}$$

où le numérateur est un polynôme de degré 2 dont les racines inverses sont des entiers algébriques de module $\sqrt{q}$.

Preuve. On a $(X^2 - tX + q) = (X - \lambda_1)(X - \lambda_2)$. D'après l'équation (2.27), on

$$N_n = q^n + 1 - \lambda_1^n - \lambda_2^n.$$

Donc, en utilisant l'expression $-log(1-t) = \sum \frac{t^n}{n}$, nous avons :

$$\begin{aligned} Z_E(T) &= \exp(\sum_{n=1}^{+\infty} \frac{N_n}{n} T^n) \\ &= \exp(\sum (q^n + 1 - \lambda_1^n - \lambda_2^n) \frac{T^n}{n} \\ &= \exp(-log(1-qT) - log(1-T) + log(1-\lambda_1 T) + log(1-\lambda_2 T) \\ &= \frac{((1-\lambda_1 T)(1-\lambda_2 T)}{(1-T)(1-qT)} \\ &= \frac{qT^2 - tT + 1}{(1-T)(1-qT)}. \end{aligned} \tag{3.3}$$

Corollaire 3.1 *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. On a :*

$$|E(\mathbb{F}_q)| = q + 1 - \sum_{n=1}^{2} \lambda_i. \tag{3.4}$$

Preuve. D'après l'équation (3.2) de la fonction $Zêta$, on pose :

$$\frac{dZ_E(T)}{dT} |_{T=0} = | E(\mathbb{F}_q)|.$$

D'autre part, en dérivant, on obtient :

$$\frac{dZ}{dt}(T) |_{T=0} = q + 1 - \sum_{n=1}^{2} \lambda_i = |E(\mathbb{F}_q)|.$$

Remarque 3.1 *Plus généralement pour tout entier $n \geq 1$, on a :*

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \sum_{n=1}^{2} \lambda_i. \tag{3.5}$$

Définition 3.2 *Une fonction Zêta de Riemann E est définie par :*

$$\zeta(s) = Z_E(q^{-s})\ ;$$

où s est une variable complexe.

Remarque 3.2 *Par analogie, la fonction Zêta de Riemann peut être considérée comme :*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Théorème 3.2

1. $\zeta_E(s) = \zeta_E(s-1)$,

2. *si* $\zeta_E(s) = 0$, *alors* $Re(s) = \frac{1}{2}$.

Preuve.

1. La preuve découle du théoréme (3.1)

$$\begin{aligned} \zeta(s) &= \frac{q^{1-2s} - aq^{-s} + 1}{(1-q^{-s})(1-q^{1-s})} \\ &= \frac{1 - aq^{1-s} + q^{-1+2s}}{(q^s-1)(q^{s-1}-1)} \\ &= \zeta_E(s-1). \end{aligned} \tag{3.6}$$

2. Puisque le numérateur de $Z_E(T)$ est $(1-\lambda_1 T)(1-\lambda_1 T)$, on a :

$$\zeta = 0 \iff q^s = \lambda_1 \ ou\ \lambda_2.$$

Par la formule quadratique,

$$\lambda_1, \lambda_2 = \frac{t \pm \sqrt{t^2 - 4q}}{2}.$$

D'après le théorème de Hasse, on sait que

$$|t| \geq 2\sqrt{q}.$$

Si $q^s = \lambda_1, \lambda_2$, alors

$$q^{Re(s)} = |q^s| = \sqrt{q}.$$

Par conséquent $Re(s) = 1/2$.

Proposition 3.1 *(Produit Eulerien)*
Soit E une courbe elliptique sur $\mathbb{F}_q$. Alors

$$\zeta_E(s) = \prod_{Sp}(1 - \frac{1}{q^{sdeg(P)}})^{-1} \tag{3.7}$$

où le produit est sur le point $P \in E(\bar{\mathbb{F}}_q)$, mais nous prenons un seul point de Sp.

Remarque 3.3 *L'application de Frobenius agit sur les P, l'ensemble*

$$S_p = \{P, \sigma_q(P), \sigma_q^2(P), ..., \sigma_q^{n-1}(P)\}$$

contient $n = deg(P)$ éléments et, que $\sigma_q(P) = P$. Chacun des points de P est de degré n.

Preuve. :(De la proposition)
Si $deg(P) = m$, alors P et tous les autres points de Sp ont des coordonnées dans $\mathbb{F}_q^m$. Ainsi $\mathbb{F}_q^m \subset \mathbb{F}_q^n$ si et seulement si $m|n$. Donc

$$N_n = \sum_{m|n} \sum_{Sp, deg(P)=m} m. \tag{3.8}$$

En remplaçant N_n dans l'expression de $Z_E(T)$, on obtient :

$$\begin{aligned} logZ_E(T) &= \sum_{n=1}^{\infty} \frac{N_n}{n} T^n \\ &= \sum_{n=1}^{\infty} \frac{1}{n} \sum_{m|n} \sum_{Sp, deg(P)=m} m \\ &= \sum_{j=1}^{\infty} \sum_{m=1} \frac{1}{mj} \sum_{Sp, deg(P)=m} mT^m j(oumj = n) \\ &= \sum_{j=1}^{\infty} \sum_{Sp} \frac{1}{j} T^j deg(p) \\ &= -\sum_{Sp} log(1 - T^d eg(P)). \end{aligned} \tag{3.9}$$

En posant $T = q^{-s}$ et en utilisant l'exponentielle, on obtient le résultat.

Exemple 3.1 *: Considérons la courbe elliptique $E \subset \mathbb{P}^2$ définie sur $\mathbb{F}_2$ par :*

$$X_0^3 + X_1^3 + X_2^3 = 0.$$

Les points $\mathbb{F}_2-$ rationnels de E sont :

$$\{(0:1:1), (1:1:0), (1:0:1)\}.$$

Ainsi $N_1 = 3$ et en utilisant la fonction Z_E, on peut alors écrire

$$3 = N_1 = \frac{d}{dt} log Z_E(T)|_{T=0} = \left[\frac{t+4T}{1+tT+2T^2} + \frac{1}{1-T} + \frac{2}{1-2T}\right]_T = 0. \tag{3.10}$$

D'où $t = 0$ et

$$P(T) = 1 + 2T^2 = (1 - i\sqrt{2T})(1 + i\sqrt{2T}).$$

Ainsi, on a $N_m = 1 + 2^m - (i\sqrt{2})^m - (-i\sqrt{2})^m$ et finalement

$$|N_m| = \begin{cases} 1 + 2^m & m \equiv 1 \ mod\ 2 \\ 1 + 2^m + 2(\sqrt{2})^m & m \equiv 2 \ mod\ 4 \\ 1 + 2^m - 2(\sqrt{2})^m & m \equiv 0 \ mod\ 4. \end{cases} \tag{3.11}$$

3.2 Bornes sur le nombre de points rationnels d'une courbe elliptique

Une courbe définie sur un corps fini a un nombre fini de points rationnels, car ce dernier est trivialement borné par le nombre de points rationnels de l'espace projectif dans lequel la courbe est plongée : un aspect arithmétique de la géométrie algébrique, qui a influencé de façon prépondérante des domaines d'application tels que la cryptographie et la théorie des codes. En partant du théorème de Weil pour les courbes elliptiques, nous parcourrons dans ce paragraphe les résultats fondamentaux concernant les bornes sur le nombre de points rationnels d'une courbe elliptique définie sur un corps fini.

3.2.1 La borne de Hasse-Weil

Une conséquence immédiate de l'équation (2.22) est la borne de Hasse−Weil pour le nombre de points rationnels d'une courbe elliptique définie sur un corps fini :

Théorème 3.3
Soit E une courbe elliptique définie sur $\mathbb{F}_q$. On a :

$$|| E(\mathbb{F}_q) | -(q+1) | \leq 2\sqrt{q}. \tag{3.12}$$

3.2.2 La borne de Serre-Weil

Une amélioration significative de l'équation (3.12) lorsque q n'est pas un carré a été donnée par Serre en 1983. Cette nouvelle borne est appelée borne de Serre−Weil :

Théorème 3.4
Soit E une courbe elliptique définie sur $\mathbb{F}_q$. On a :

$$|| E(\mathbb{F}_q) | -(q+1) | \leq [2\sqrt{q}]. \tag{3.13}$$

Preuve. D'après l'équation du corollaire (3.1), il suffit de montrer que

$$| \sum_{i=1}^{2} \lambda_i | \leq [2\sqrt{q}].$$

Pour $i \in \{1, 2\}$, on pose :

$$\alpha_i = \lambda_i + [2\sqrt{q}] + 1.$$

Si on applique l'inégalité arithmético−géométrique :

$$\sum_{i=1}^{2} \alpha_i \geq \prod_{i=1}^{2} \alpha_i \geq 1. \tag{3.14}$$

Il s'ensuit

$$1 \leq \sum_{i=1}^{2} \alpha_i = \sum_{i=1}^{2} \lambda_i + [2\sqrt{q}] + 1, \tag{3.15}$$

autrement dit

$$-\sum_{i=1}^{2} \lambda_i \leq [2\sqrt{q}]. \tag{3.16}$$

Pour l'autre inégalité, il suffit de remplacer λ_i par $-\lambda_i$ dans la définition de α_i.

Exemple 3.2 *Pour $q = 23$, la borne de Hasse-Weil donne*

$$|| E(\mathbb{F}_{23}) | -24 | \leq 10, \tag{3.17}$$

alors que la borne de Serre-Weil donne

$$|| E(\mathbb{F}_{23}) | -24 | \leq 9. \tag{3.18}$$

Notation : On note de façon usuelle N_q, le nombre maximum de points rationnels d'une courbe elliptique définie sur un corps fini.
Le corollaire suivant découle directement de la borne Serre−Weil.

Corollaire 3.2 *On a l'inégalité :*

$$N_q \leq q + 1 + [2\sqrt{q}]\,. \tag{3.19}$$

Le résultat suivant est connu depuis les travaux de Hasse et Deuring.

Théorème 3.5 *Soit $q = p^n$ avec p premier. Alors*

$$N_q = \begin{cases} q + \left[2\sqrt{q}\right] & \text{si } p \text{ divise } \left[2\sqrt{q}\right], \text{ et si } n \geq 3 \\ q + 1 + \left[2\sqrt{q}\right] & \text{sinon.} \end{cases} \tag{3.20}$$

3.3 Méthode de Comptage des points rationnels

On considère dans ce paragraphe un nombre premier $p \geq 5$. Soit E une courbe elliptique définie sur $\mathbb{F}_p$ d'équation

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

Dans les algorithmes de primalité et de factorisation utilisant les courbes elliptiques, il importe de pouvoir disposer des courbes elliptiques sur $\mathbb{F}_p$, pour lesquelles on sait déterminer le nombre de points rationnels. On va décrire quelques méthodes permettant parfois d'y parvenir.

3.3.1 Méthode du symbole de Legendre

Soit $\chi : \mathbb{F}_p \longrightarrow \{-1, 0, 1\}$ l'application définie pour tout $x \in \mathbb{F}_p$ par

$$\chi(x) = \tfrac{x}{p}.$$

Rappelons $\chi(0) = 0$, $\chi(x) = 1$ si x est un carré non nul sur $\mathbb{F}_p$ et $\chi(x) = -1$ si x n'est pas un carré sur $\mathbb{F}_p$.

Proposition 3.2 *On a l'égalité :*

$$\mid E(\mathbb{F}_p) \mid = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + ax + b). \tag{3.21}$$

Preuve. Pour tout $x \in \mathbb{F}_p$, il y a deux points d'abscisse x dans $E(\mathbb{F}_p)$ si $\chi(x^3+ax+b) = 1$. Il n'y en a pas si $\chi(x^3 + ax + b) = -1$ et il y a un seul si $x^3 + ax + b = 0$. Par la suite, en comptant le point à l'infini, on obtient :

$$\mid E(\mathbb{F}_p) \mid = 1 + \sum_{x \in \mathbb{F}_p} 1 + \chi(x^3 + ax + b), \tag{3.22}$$

ce qui conduit à l'égalité annoncée.

Exemple 3.3 *(Voir [3])*
Considérons E la courbe elliptique sur $\mathbb{F}_{11}$ d'équation

$$y^2 = x^3 + x + 5.$$

On a,

$$\mid E(\mathbb{F}_{11}) \mid = 12 + \sum_{x \in \mathbb{F}_{11}} 1 + \chi(x^3 + x + 5), \tag{3.23}$$

On obtient ainsi,

$$\mid E(\mathbb{F}_{11}) \mid = 11.$$

En fait, cette méthode de comptage fonctionne bien, disons pour les nombres premiers p plus petit que 10^6 ou à la limite 10^7.

Exemple 3.4 *(Voir [3])*
Considérons E la courbe elliptique d'équation

$$y^2 = x^3 + x + 1.$$

Avec $p = 10^6 + 3$, on trouve avec le logiciel de calcul Pari/GP que

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 + x + 1) = 723,$$

d'où $\mid E(\mathbb{F}_p) \mid = 1000727$.
Avec $p = 10^7 + 19$, on trouve, avec le logiciel de calcul, que

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 + x + 1) = -1439,$$

d'où $\mid E(\mathbb{F}_p) \mid = 9998581$.

3.3.2 Méthode de Shanks - Algorithme de Baby Step−Giant Step

a. Méthode Shanks

L'algorithme qui suit est dû à Shanks. Rappelons que

$$H_p = \left[p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}\right]$$

est l'intervalle de Hasse pour p.

1. On choisit un point P quelconque dans $E(\mathbb{F}_p)$. Pour cela, on détermine une abscisse x au hasard jusqu'à ce que $x^3 + ax + b$ soit un carré dans $\mathbb{F}_p$ et on extrait une racine carré y de $x^3 + ax + b$ pour obtenir l'ordonnée. On prend alors $P = (x, y)$.
2. On détermine ensuite un entier m tel que

$$mP = \mathcal{O} \quad et \quad m \in H_p. \tag{3.24}$$

   Il existe un tel entier m, car $\mid E(\mathbb{F}_p) \mid P = \mathcal{O}$ et $\mid E(\mathbb{F}_p) \mid$ est dans H_p. Si m est le seul entier de H_p réalisant cette condition, alors m est l'ordre de $E(\mathbb{F}_p)$. En fait, la longueur de H_p étant $4\sqrt{p}$, il est coûteux de vérifier, si p est grand, que m est le seul entier de H_p satisfaisant (3.24) si tel est le cas. On peut procéder autrement.

Lemme 3.1 *Soit d l'ordre de P. Supposons que l'on ait :*

$$d \geq 4\sqrt{p}.$$

Soit m un entier vérifiant la condition (3.24). Alors, m est l'ordre de $E(\mathbb{F}_p)$. De plus, m est l'unique multiple de d dans H_p.

Preuve. L'entier d divise m et l'ordre de $E(\mathbb{F}_p)$. Parce que la longueur de H_p est $4\sqrt{p}$, il y a un seul multiple de d dans H_p. On a donc $m = \mid E(\mathbb{F}_p) \mid$.

Exemple 3.5 *(Voir [3])*
Prenons pour E la courbe elliptique sur $\mathbb{F}_p$ d'équation

$$y^2 = x^3 + x + 1.$$

Le point $P = (0, 1)$ appartient à $E(\mathbb{F}_p)$.

1. *Avec $p = 10^6 + 3$, avec le logiciel de calcul, on trouve que*

$$m = 1000727$$

   est le seul entier dans H_p tel que $mP = \mathcal{O}$, d'où $\mid E(\mathbb{F}_p) \mid = m$.

2. *Avec* $p = 10^{10} + 19$, *avec le logiciel de calcul, on trouve que*

$$m = 999881780$$

est le seul entier dans H_p *tel que* $mP = \mathcal{O}$, *d'où* $\mid E(F_p) \mid = m$.

b. L'algorithme Baby Step−Giant Step

Soit un point $P \in E(\mathbb{F}_p)$, l'algorithme s'agit alors d'expliquer comment trouver un entier m tel que la condition (3.24) soit vérifié.
On peut tester les entiers de H_p jusqu' a trouver un vérifiant de la condition (3.24) , ce qui peut nécessiter $4\sqrt{p}$ tests. L'algorithme de Baby Step−Giant Step permet en fait de se limiter à environ $4p^{\frac{1}{4}}$ tests.
On procède comme suit :

1. On calcule $Q = (p+1)P$.
2. On choisit un entier $s > p^{\frac{1}{4}}$, par exemple $s = \left[p^{\frac{1}{4}}\right] + 1$ et on dresse la liste des points

$$jP \quad pour \quad j = 1, ..., s.$$

Connaissant jP , on connait aussi $-jP$. On détermine ainsi $2s+1$ points de $E(\mathbb{F}_p)$. L'appellation de Baby Step est relative à ce calcul pour le passage de jP à $(j+1)P$.

3. On calcule les points

$$Q + k(2sP) \quad pour \quad k \in [-s, s].$$

Pour cela, on calcule au départ le point $Q+2sP$. On obtient alors $Q+(k+1)(2sP)$ (resp. $Q+(k-1)(2sP)$)à partir de $Q+k(2sP)$ en lui ajoutant $2sP$ (resp. $-2sP$). L'appellation Giant Step est relative à ce passage.

Lemme 3.2 *Soit* c *un entier relatif tel que* $\mid c \mid \leqslant 2s^2$. *Il existe des entiers* c_0 *et* c_1 *tels que l'on ait :*

$$c = c_0 + 2sc_1 \quad avec \quad c_0, c_1 \in [-s, s].$$

Preuve. Il existe un entier c_0 tel que l'on ait :

$$c \equiv c_0 \ mod\ 2s \quad avec \quad c_0 \in [-s, s].$$

Posons $c - c_0 = 2sc_1$. On a :

$$\mid c1 \mid \leq \frac{2s^2+s}{s} < s + 1,$$

ce qui entraine le résultat.

Théorème 3.6 *Il existe des entiers naturels tel que l'on ait :*

$$jP = Q + k(2sP) \quad avec \quad j, k \in [-s, s] \quad et \quad \mid j - 2ks \mid \leq 2\sqrt{p}. \tag{3.25}$$

Si j et k sont des entiers satisfaisant ces conditions, en posant

$$m = p + 1 + 2ks - j,$$

on a la condition (3.24).

Preuve. Appliquons le lemme précédent avec $t = p + 1 - \mid E(\mathbb{F}_p) \mid$. D'après le choix de s, on a $s^2 > \sqrt{p}$, d'où $\mid t \mid \leq 2s^2$ (le théorème de Hasse). Il existe donc j, $k \in [-s, s]$ tels que $t = j - 2ks$. On a $\mid j - 2ks \mid \leq 2\sqrt{p}$ et les égalités

$$Q + k(2sP) = (p + 1 + 2sk)P = (p + 1 + j - t)P = (\mid E(\mathbb{F}_p) \mid + j)P = jP \ ,$$

ce qui entraîne le résultat.

Exemple 3.6 *(Voir [3])*
Soit E la courbe elliptique sur $\mathbb{F}_p$ d'équation

$$y^2 = x^3 + x + 1.$$

Posons $P = (0, 1)$ $E(\mathbb{F}_p)$. On reprend les notations du théorème précédent.
Prenons $p = 10^{15} + 37$. Avec $s = 5624$, on trouve

$$j = 3111 \quad et \quad k = -164,$$

d'où $m = 999999998152255$.

3.3.3 Applications : Problème du logarithme discret elliptique

Soient $\mathbb{K}$ un corps fini et E une courbe elliptique définie sur $\mathbb{K}$. Soit A un point de $E(\mathbb{K})$. Le problème de logarithme discret sur E à base A est le suivant.
Problème : Soit P un point de $E(\mathbb{K})$. Trouver un entier n, s'il existe, tel que

$$nA = P.$$

Un tel entier n n'existe pas toujours. De plus, $E(\mathbb{K})$ n'est pas nécessairement cyclique. Afin d'essayer de résoudre ce problème, on peut utiliser l'algorithme de Baby Step−Giant Step.
Posons

$$N = |E(\mathbb{K})|.$$

L'algorithme de Baby Step−Giant Step

Supposons que n existe et que l'on a $0 \leqslant n \leqslant N$. Cet algorithme permet de trouver n en $O(\sqrt{N})$ opérations.

1. On fixe un entier $m > \sqrt{N}$ et on calcule mA.
2. On établit la liste des points jA pour $j = 0, ..., m-1$.
3. On détermine les points $P - k(mA)$ pour $k = 0, ..., m-1$,

jusqu'à en trouver un qui soit égal à l'un des jA précédemment calculés. Il y a toujours une coïncidence.

Lemme 3.3 *Il existe un j et k dans $\{0, ..., m-1\}$ tel que l'on ait $jA = P - kmA$. En particulier, on a $nA = P$ avec $n = j + km$.*

Preuve. Puisque $N < m^2$, on a :

$$0 \leqslant n < m^2.$$

Il existe des entiers naturels n_0 et n_1 tels que l'on ait (division euclidienne)

$$n = mn_1 + n_0 \text{ avec } 0 \leqslant n_0 < \text{m}.$$

On alors

$$n_1 = \frac{n-n_0}{m} \leqslant \frac{n}{m} < m.$$

On obtient

$$P - n_1(mA) = nA - n_1(mA) = (n - n_1 m)A = n_0 A,$$

ce qui entraîne le résultat.

Exemple 3.7 *(Voir [3])*
Prenons $\mathbb{K} = \mathbb{F}_{53}$ et pour E la courbe elliptique d'équation

$$y^2 = x^3 + 5x + 2.$$

Le groupe $E(\mathbb{K})$ est cyclique d'ordre 63 engendré par le point $A = (-1, 7)$. Le point $P = (20, 24)$ appartient à $E(\mathbb{K})$. Cherchons l'entier naturel $n < 63$ tels que $nA = P$.
Prenons $m = 8$. Les points jA pour j=0,...7, sont (par indices croissants)

$\mathcal{O}$, (−1, 7), (15, 39), (20, 29), (50, 38), (19, 58), (6, 6), (8, 17).

Par ailleurs les points $P - kmA$ pour k = 0, ..., 7 sont (par indices croissants)

P, (35, 4), (33, 45), (16, 16), (49, 17), (5, 24), (17, 12), (50, 58).

La coïncidence a eu lieu pour k= 7, ce qui a rendu nécessaire le calcul de sept points, et pour j = 4. Finalement, on obtient n= 60.

Remarque 3.4

Afin de résoudre le problème de logarithme discret dans $E(\mathbb{K})$, il n'est pas nécessaire de déterminer l'ordre de $E(\mathbb{K})$. En supposant qu'il existe n tel que $nA = P$, il suffit en fait de savoir que l'on peut prendre pour n un entier plus petit d'une borne explicite. Tel est le cas dans notre situation, vu que $|E(\mathbb{K})|$ est plus petit que $q + 1 + 2\sqrt{q}$ où q est le cardinal de $\mathbb{K}$. Si l'entier n cherché existe, on peut donc supposer que $n \leqslant q + 1 + 2\sqrt{q}$. Ainsi, l'algorithme précédent fonctionne en choisissant au départ un entier m vérifiant $m^2 > q + 1 + 2\sqrt{q}$, auquel cas, on a de nouveau $n < m^2$, et l'énoncé du lemme précédent est encore valable, avec la même démonstration.

Conclusion

Le but de notre travail était de présenter quelques méthodes à mettre en oeuvre pour compter le nombre de points rationnels sur une courbe elliptique dans un corps fini. D'une part, nous avons abordé les bornes de Hasse-Weil et Serre-Weil sur une courbe elliptique pour estimer le nombre de points rationnels. D'autre part, nous avons procédé par des méthodes de comptages : la méthode du symbole de Legendre et la méthode de Shanks. Cependant, il existe d'autres méthodes de comptage permettant de compter ou calculer le nombre de points rationnels. Parmi lesquelles, on peut citer l'algorithme de SEA(School-Elkies-Atkin), travaux de Conveignes et Morain (Voir [6],[12],[8]). En guise d'application, nous avons montré comment utiliser le groupe des points rationnels pour résoudre le problème de logarithme discret elliptique par l'algorithme de Baby Step−Giant Step dû à Daniel Shanks en 1971. Le problème de logarithme discret est généralement beaucoup plus difficile à résoudre dans le groupe des points rationnels d'une courbe elliptique dans un corps fini $\mathbb{K}$, que celui d'un groupe multiplicatif $\mathbb{K}^*$. Il convient toutefois de prendre certaines précautions sur le choix de la courbe elliptique.

Bibliographie

[1] F. Dumas, Algèbre : Groupes et Anneaux 1. Université Blaise Pascal.

[2] M. Joye, Introduction à la théorie élémentaire des courbes elliptiques. Département de Mathématique(AGEL), Université catholique de Louvain. 25 juin 1995

[3] A. Krauss, Cours de cryptographie. Université Pierre et Marie Curie.

[4] N. Koblitz, Introduction to elliptic curves and modular froms.

[5] N. Koblitz, Elliptic curve cryptosystems. Math. Comp., 48(177) 203-209, January 1987.

[6] R. Lercier, Algorithme des courbes elliptiques dans un corps fini. Informatique [cs]. Ecole polytechnique, 1997. Français.

[7] F. Liret, Arithmétique : cours et exercices.

[8] F. Morrain, Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. J. Théor. Nombres Bordeaux, 7 :255-282, 1995.

[9] M. Perret, Nombre maximum de points rationnels d'une courbe dans un corps fini. Sém.Théor. Nombres Bordeaux (2), 3(2), :261-274, 1991.

[10] D. Perrin, Géométrie algébrique, Introduction. IUFM de Versaille, Université de Paris-Sud, Orsay.

[11] J. H. Silverman, John T. Tate, Rational Points on Elliptic Curves. Second Edition.

[12] C. L. Washington, Elliptic Curves number theory and cryptography. University of Maryland.

[13] A. Weil, L'arithmétique sur les courbes algébriques. Acta Math., 52(1) :281-315, 1929.