الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Ref :.....

Centre Universitaire de Mila

Institut des Sciences et de la Technologie Département de Mathématiques et Informatiques

Mémoire préparé En vue de l'obtention du diplôme de Master
en : - Filière Mathématiques Fondamentales
- Spécialité Mathématiques Fondamentales et Appliquées

Le Nombre de Points d'une Courbe Elliptique sur un Corps Fini

Préparé par : Barkat Abla
Mermoul Roqiya

Soutenue devant le jury :

Président	S. Kaouache	Grade M.A.A
Examinateur	M. Khalfaoui	Grade M.A.B
Promoteur	M. Bouguebina	Grade M.A.A

Année universitaire : 2013/2014

Remerciement

Nous remercions nos trés chers parents, frères, soeurs, collègues et amis respectifs qui nous ont encouragés, soutenu durant tout notre parcours.

Nous présentons notre grand remerciement à professeur : *Bouguebina Mounir* sur tous ce qu'il nous a présenté comme conseils et orientations durant la réalisation de notre mémoire.

Nous remercions égale ment les membres de jury qui ont accepté de critiquer ce travail.

Nous remercions aussi tout éducateur, maitre et professeur qui nous appris un mot ou un cours, et orienté sur le chemin de la connaissance et du savoir depuis le cycle primaire, jusqu'au cycle universitaire.

Nous souhaitons la réussite à tous les étudiants des sections Mathématique et Informatique.

Enfin, nous remercions, tous ceux et celles qui nous ont aidées à faire ce mémoire.

Barkat Abla

Mermoul Roqiya

Résumé

Dans ce travail nous présentons quelques méthodes pour calculer le nombre de points d'une courbe elliptique E définie sur un corps fini (F_q) donnée par l'equation de Weierstrass :

$$Y^2 = X^3 + AX + B$$

avec $A, B \in F_q$.

Dans le premier chapitre nous présentons les notions de Géométrie Algébrique qui nous sont nécessaires pour définir les courbes elliptiques et établir la loi de groupe sur l'ensemble de leurs points rationnels, ce que l'on fait au chapitre deux.

Dans le troisieme chapitre, on s'intéresse au cas ou le corps de base est un corps fini, obtenant du coup un groupe fini, celui des points rationnels. Ici le résultat principal est le théoreme de Hasse qui permet de situer l'ordre de ce groupe dans un intervalle précis. Ce théoreme sera un ingrédient essentiel dans l'algorithme de Schoof.

Dans le chapitre quatre, on présente d'abord quelques méthodes pour calculer le cardinal des points rationnels en insistant sur celle de Lang-Trotter et celle du Baby Step-Giant Step qui existaient avant l'algorithme de Schoof et qui n'étaient efficaces que pour des corps finis de taille pas trop grande.

Enfin nous présentons l'algorithme de Schoof en détail et nous l'illustrons avec quelques exemples.

Abstract

In this work we present some methods to calculate the number of points an elliptic curve $\overline{E}$ defined over a finite field (F_q) given by equation Weierstrass :

$$Y^2 = X^3 + AX + B$$

avec $A, B \in F_q$.

In the first chapter we introduce the concepts of algebraic geometry that we are required to define elliptic curves and establish the group law on the set of their rational points, that we made in chapter two

In the third chapter, we are interested in cases where the base is a finite field. Here the main result is the theorem of Hasse that ranks the order of this group in a specific interval. This theorem will be an essential ingredient in the algorithm schoof

In chapter four, we first present some methods to calculate the cardinal rational points emphasizing the Lang -Trotter and that of Baby Step-Giant Step that existed before algorithm Schoof and were only effective for finished body size not too big.

Finally, we present algorithm Schoof in detail and illustrate with some examples.

ملخص

في هذا العمل نقدم بعض الطرق لحساب عدد النقاط لمنحنى إهليجي E معرف على حقل محدود بإستخدام معادلة Weierstrass:

بحيث : $A, B \in Fq$

في الفصل الأول نقدم مفاهيم الهندسة الجبرية المطلوبة لتحديد المنحنيات الإهليجية و وضع قانون الزمرة على الزمرة و التي أوضحناها في الفصل الثاني .

و في الفصل الثالث إهتممنا بالحالات التي تكون فيها قاعدة الحقل محدودة . هنا النتيجة الرئيسية و هي نظرية Hasse بحيث يرتب أمر من هته الزمرة في فترة زمنية محددة و هذه النظرية عنصرا أساسيا في خوارزمية Schoof

و في الفصل الرابع قمنا أولا بتقديم بعض الطرق لحساب عدد النقاط المتواجدة في القطوع الإهليجية من بينها طريقة Lang-Trotter وطريقة Baby Step-Giant Step التي ظهرت قبل خوارزمية Schoof .

أخيرا فإننا نقدم خوارزمية Schoof بالتفصيل و توضيح مع بعض الأمثلة .

Le Nombre de Points d'une Courbe Elliptique sur un Corps Fini

Mermoul Roqiya et Barkat Abla

Table des matières

Introduction Générale

Les courbes elliptiques sont un sujet d'étude classique (et toujours moderne) en Géométrie Algébrique et en Géométrie Arithmétique. Depuis le milieu des années quatre vingt, elles ont vu leur importance s'accroitre a cause de leurs nombreuses applications en Cryptographie [4, 5, 10]. Etant donnée une courbe elliptique sur un corps K, on peut définir sur l'ensemble de ses points rationnels une structure de groupe abélien. Si le corps K est fini, ce groupe est fini et on peut l'utiliser comme base pour des protocoles cryptographiques assurant la sécurité et la confidentialité des données. De plus la richesse des courbes elliptiques est telle que la sécurité de ces protocoles est bien supérieure a celle de protocoles basés sur des groupes plus classiques. La connaissance du nombre de points rationnels de la courbe sur le corps fini est donc importante tant d'un point de vue théorique que pratique. Dans ce mémoire nous présentons quelques méthodes pour calculer ce nombre et nous détaillons l'algorithme de Schoof [13, 14] qui est considéré comme le premier algorithme déterministe à complexité polynômiale et donc comme étant trés rapide. Un algorithme plus récent, l'AES (pour Atkin-Elkies-Schoof) [1], est apparemment beaucoup plus rapide mais nous n'en parlerons pas du tout dans ce travail qui est organisé comme suit. Dans le premier chapitre nous présentons les notions de Géométrie Algébrique qui nous sont nécessaires pour définir les courbes elliptiques et établir la loi de groupe sur l'ensemble de leurs points rationnels, ce que l'on fait au chapitre deux. Dans le troisieme chapitre, on s'intéresse au cas ou le corps de base est un corps fini, obtenant du coup un groupe fini, celui des points rationnels. Ici le résultat principal est le théoreme de Hasse qui permet de situer l'ordre de ce groupe dans un intervalle précis. Ce théoreme sera un ingrédient essentiel dans l'algorithme de Schoof. Dans le chapitre quatre, on présente d'abord quelques méthodes pour calculer le cardinal des points rationnels en insistant sur celle de Lang-Trotter [8] et celle du Baby Step-Giant Step [1, 4] qui existaient

avant l'algorithme de Schoof et qui n'étaient efficaces que pour des corps finis de taille pas trop grande. Enfin nous présentons l'algorithme de Schoof en détail et nous l'illustrons avec quelques exemples.

Chapitre 1

Courbes Algébriques

Ce premier chapitre peut être considéré comme un mini cours de Géométrie algébrique. Notre présentation est inspirée de Fulton [3] et des premiers chapitres de Silvermann [15]. Pour le côté algébrique nous renvoyons à l'Algebra de Lang [7]. Le sujet étant difficile nous nous concentrons sur les courbes algébriques qui sont les seules variétés qui nous intéressent ici. Nous les définissons comme lieu de zéros de polynômes (en fait d'un polynôme) aussi bien dans le plan affine que dans le plan projectif. Nous insistons sur le fait qu'une courbe projective est la réunion d'une courbe affine plus des points à l'infini, ce qui simplifie beaucoup la présentation et les calculs puisqu'une courbe affine plane est déterminée par un polynôme irréductible à deux variables (au lieu de trois pour une courbe projective). Ceci facilite aussi le traitement des notions de fonction rationnelle et de point singulier sur la courbe. Le résultat principal de ce premier chapitre est le théorème de Riemann-Roch qui permet de calculer la dimension de certains espace vectoriels définis à partir de diviseurs sur la courbe et qui permet de savoir s'il y a telle ou telle fonction sur la courbe avec un nombre donné de zéros et de pôles. Un diviseur particulier sur la courbe s'avère être le diviseur canonique que l'on forme en utilisant les différentielles (algébriques). Il intervient de manière essentielle dans l'énoncé du théorème de Riemann-Roch. Tout ceci se passant sur un corps algébriquement clos, nous expliquons, à la fin du chapitre, les changements qu'on doit effectuer quand le corps n'est plus algébriquement clos, concernant par exemple les points rationnels de la courbe sur son corps de définition.

1.1 Courbes Affines

Soit K un corps algébriquement clos. L'espace affine sur K est :

$$\mathbb{A}^2 = \mathbb{A}^2(K) = \{(x, y), x, y \in K\}$$

Si $P = (a, b) \in \mathbb{A}^2$, a et b sont les coordonnées du point P. Pour toute partie $S \subseteq K[X, Y]$ de l'anneau des polynômmes à deux variables, on pose :

$$Z(S) = \{P \in \mathbb{A}^2 / F(P) = 0, \forall F \in S\}$$

Définition 1.1.1 *: Les ensembles de la forme $Z(S)$ pour $S \subseteq K[X, Y]$ sont les ensembles algébriques de $\mathbb{A}^2$.*

Il est clair que si $I(S)$ est l'idéal de l'anneau $K[X, Y]$ engendré par S, alors :

$$Z(S) = Z(I(S))$$

Si V est un ensemble algébrique de $\mathbb{A}^2$, son idéal est :

$$I(V) = \{F \in K[X, Y] / F(P) = 0, \forall P \in V\}$$

Si $V = Z(J)$, le théorème des zéros de Hilbert permet de préciser la relation entre J et $I(V)$:

$$I(Z(J)) = \sqrt{J}$$

avec

$$\sqrt{J} = \{F \in K[X, Y] / \exists n \geq 0, F^n \in J\}$$

le radical de J.
comme $K[X, Y]$ est noethérien, tout idéal J est de type fini (i.e engendré par un nombre fini de polynômes) :

$$J =< F_1, ..., F_r >, F_i \in K[X, Y]$$

et donc :

$$V = Z(J) = \left\{P \in \mathbb{A}^2 / F_1(P) = 0, \ldots, F_r(P) = 0\right\}$$

est l'ensemble des zéros d'un nombre fini de polynômes. Pour un ensemble algébrique général de $\mathbb{A}^2$, on va montrer que $r = 1$ (et on précisera le sens

du mot "général").
Parmi les ensembles algébriques de $\mathbb{A}^2$, il y a d'abord $\emptyset$ et $\mathbb{A}^2$ tout entier

$$\emptyset = Z(K[X,Y])$$

$$\mathbb{A}^2 = Z((0))$$

(0) etant l'idéal de $K[X,Y]$ engendré par le polynôme nul : $F(X,Y) = 0$. Il y a aussi les points $P = (a,b)$:

$$P = Z((X-a, Y-b))$$

avec $(X-a, Y-b)$ l'idéal engendré par $X-a$ et $Y-b$. On vérifie facilement que la réunion finie et l'intersection d'ensembles algébriques est aussi un ensemble algébrique. Tout réunion finie de points est donc aussi un ensemble algébrique. Nous dirons qu'un ensemble algébrique de $\mathbb{A}^2$ est "général" s'il est différent de $\emptyset$, $\mathbb{A}^2$ on toute réunion finie de points.

Proposition 1.1.1 *: Soit $V \subseteq \mathbb{A}^2$ un ensemble algébrique "général" de $\mathbb{A}^2$. Alors il existe $F \in K[X,Y]$ tel que :*

$$V = \{P \in \mathbb{A}^2 / F(P) = 0\}$$

Preuve : Remarquons d'abord que $Z((F,G)) = Z(F) \cap Z(G)$ où F et G sont deux polynômes dans $K[X,Y]$ et (F,G) est l'idéal engendré par F et G. Montrons alors (en suivant Fulton [3]) que si F et G n'ont pas de facteur commun, alors $Z((F,G)) = Z(F) \cap Z(G)$ est formé d'un ensemble fini de points. On regarde $F, G \in K[X,Y]$ comme des éléments de $F(X)[Y]$ qui est un anneau principal($F(X)$ est le corps des fractions de $F[X]$), et dans lequel l'analogue de l'algorithme d'Euclide étendu a lieu. Comme F et G n'ont pas de facteur commun dans $F(X)[Y]$, il existe U, V dans $K(X)[Y]$ tels que :

$$UF + VG = 1$$

En reduisant au même dénominateur, on peut trouver $D \in K[X]$ tel que :

$$DUF + DVG = D$$

Posons $A = DU$ et $B = DV$. Donc $AF + BG = D$. Si $P = (a,b) \in Z((F,G))$ alors $D(a) = 0$. Comme D n'a qu'un nombre fini de zéros, les a possibles sont en nombre fini. En remplaçant X par Y dans toute la discussion précédente,

le nombre de b possibles est aussi fini. Ainsi le nombre de points $P = (a, b)$ dans $Z((F, G))$ est fini.Soit maintenant V un ensemble algébrique général de $\mathbb{A}^2$. On sait que

$$V = Z(F_1, \ldots, F_r)$$

avec $F_i \in K[X, Y], i = 1, \ldots, r$. Si les F_i ont un facteur commun F, alors $V = Z(F)$. Sinon, on applique le résultat précedent et on obtient :

$$V = Z(F_1) \cap \ldots \cap Z(F_r)$$

qui constitue un nombre fini de points et donc V ne serait pas "général".

Un ensemble algébrique V de $\mathbb{A}^2$ est irréductible si on ne peut pas l'ecrire $V = V_1 \cup V_2$ avec $V_1 \subsetneqq V$ et $V_2 \subsetneqq V$ des ensembles algébriques. De manière équivalente V est irréductible si $I(V)$ est un idéal premier de $K[X, Y]$.

Définition 1.1.2 *Une courbe algébrique affine C (plane) est un ensemble algébrique de $\mathbb{A}^2$ qui est général et irréductible.*

On sait qu'un ensemble algébrique V de $\mathbb{A}^2$ sécrit :

$$V = Z(F)$$

avec $F \in K[X, Y]$. Ce dernier anneau est un UFD (unique factorisation domain). Cela veut dire que tout polynôme est produit unique de polynômes irréductibles :

$$F = F_1^{n_1} \ldots . F_k^{n_k}$$

avec les F_i irréductibles. Si $V = C$ est une courbe affine, il n ya qu'un seul facteur (car C est irréductible et $Z(FG) = Z(F) \cup Z(G))$ $F = F_1^{n_1}$. Donc $C = Z(F) = Z(F_1^{n_1}) = Z(F_1)$. Autrement dit pour une courbe affine C, on peut toujours trouver un polynôme irréductible F tel que :

$$C = \{P \in \mathbb{A}^2 / F(P) = 0\}$$

Ceci nous amène à une deuxième définition d'une courbe qui parait beaucoup plus agréable que la première :

Définition 1.1.3 *: Une courbe algébrique affine (plane) est le lieu des zéros d'un polynôme irréductible $F \in K[X, Y]$:*

$$C = \{P \in \mathbb{A}^2 / F(P) = 0\}$$

ou encore

$$C = \{(x, y) \in K^2 / F(x, y) = 0\}$$

Remarquer qu'une courbe C a une nombre infini de points (K algébriquement clos). Remarquer aussi que si F est irréductible alors $C = Z(F) \Rightarrow I(C) = (F)$. (En général $V = Z(F)$ irréductible $\not\Rightarrow$ F irréductible, la réciproque est comme on vient de le voir vraie : F irréductible $\Rightarrow I(C) = (F)$ premier $\Rightarrow C = Z(F)$ irréductible). La définition d'un courbe affine fait intervenir essentiellement la notion de polynôme irréductible. On peut donc se demander comment savoir si $F \in K[X, Y]$ est irréductible. Pour cela on peut montrer directement que F ne peut pas sécrire $F = G.H$ avec $G, H \in K[X, Y]$ ou alors utiliser l'un des critères d'irréductibilité, par exemple celui d'Eisenstein :

Proposition 1.1.2 *(Critère d'irréductibilité d'Eisenstein) : Soit R un anneau d'unique factorisation (UFD) et soit $F(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ un polynôme. S'il existe $p \in R$ irréductible tel que :*

1. *p divise $a_i, \forall i \neq n$*
2. *p ne divise pas a_n*
3. *p^2 ne divise pas a_0*

alors F est un polynôme irréductible.

Preuve : Supposons les proprietés $1, 2, 3$ satisfaites et

$$F(X) = (\sum_{i=0}^{s} b_i X^i)(\sum_{i=0}^{t} c_i X^i)$$

avec $s > 0$ et $t > 0$. Comme $a_0 = b_0 c_0$, on a que p divise soit b_0 , soit c_0 mais pas les deux (1 et 3). Supposons que p divise b_0 mais pas c_0. Donc p ne divise pas $a_n = \sum_{i=0}^{n} b_i c_{n-i}$ et donc p ne peut pas diviser tous les c_i. Soit k minimun tel que p ne divise pas c_k. Mais on a $a_k = \sum_{i=0}^{n} b_i c_{k-i}$ qui est divisible par p (par 2), mais p ne divise pas b_0 et ne divise pas c_k, contradiction. On doit donc avoir soit $s = 0$, soit $t = 0$.
En utilisant l'isomorphisme $K[X][Y] \cong K[X, Y]$ on applique ce critère dans $R[Y]$ avec $R = K[X]$ (qui est un UFD).

Exemple 1.1.1 *: Soit $F(X) = X^2 + Y^2 - 1 \in K[X, Y]$. Supposons que*

$$F(X) = (aX + bY + c)(a^{'}X + b^{'}Y + c^{'})$$

$$= aa'X^2 + (ab^{'} + b^{'}a)XY + bb^{'}Y^2 + (ac^{'} + c^{'}a)X + (bc^{'} + b^{'}c)Y + cc^{'}$$

On doit donc avoir :

$$aa^{'} = bb^{'} = 1$$

$$cc^{'} = -1$$

$$ab^{'} + ba^{'} = ac^{'} + a^{'}c = bc^{'} + b^{'}c = 0$$

$$ac^{'} + a^{'}c = 0 \Rightarrow ac^{'}c + a^{'}c^2 = 0 \Rightarrow a^{'}c^2 = a$$

$$ab^{'} + ba^{'} = 0 \Rightarrow ab^{'}b + b^2a^{'} = 0 \Rightarrow b^2a^{'} = -a$$

donc $a^{'}(c^2 + b^2) = 0$, *contradiction puisque* $a^{'} \neq 0, b \neq 0$ *et* $c \neq 0$. *(*$aa^{'} = 1, bb^{'} = 1, cc^{'} = -1$*). Le polynôme* $F(X)$ *est donc irréductible. Il définit la courbe affine (le cercle) :*

$$C = Z(X^2 + Y^2 - 1)$$

Exemple 1.1.2 *: Dans cet exemple nous allons utiliser le critère d'Eisenstein. Soit* $K = \mathbb{F}_q$ *un corps fini avec* $q = p^n$ *(*p *un nombre premier) et soit* $K = \overline{\mathbb{F}_q}$ *la clôture algébrique de* $\mathbb{F}_q$. *Soit dans* $K[X, Y]$

$$F(X) = X^{q+1} + Y^{q+1} - 1$$

$$= Y^{q+1} + X^{q+1} - 1$$

$$= a_{q+1}Y^{q+1} + a_0$$

avec $a_{q+1} = 1$ *et* $a_0 = X^{q+1} - 1$ *et* $a_i = 0$ *pour* $i \neq 0, q+1$ *vu comme polynôme en* Y *à coefficients dans* $K[X]$. *Soit* $P = X + 1 \in K[X]$. P *est clairement irréductible dans* $K[X]$.
Si K *est de caractéristique* 2 *alors on a :*

$$X^{q+1} + 1 = X^{q+1} - 1 = (X - 1)(\sum_{i=0}^{q} X^i)$$

et donc $X + 1$ *divise* a_0 *mais pas* a_{q+1} *et comme*

$$\sum_{i=0}^{q} 1^i = q + 1 = 1 \neq 0$$

On voit que $(X - 1)^2$ *ne divise pas* a_0. *Par le critère d'Eisenstein,* F *est irréductible. Si car* $K \neq 2$, *on doit avoir* $q + 1 = 2r$ *pour un certain entier* r *(*q *impair). Donc*

$$X^{q+1} + 1 = X^{2r} + 1 = (X^r + 1)(X^r - 1)$$

$$= (X^r + 1)(X - 1)\sum_{i=0}^{r-1} X^i$$

Donc $X - 1$ divise a_0 mais pas a_{q+1}. De plus $(X - 1)^2$ ne divise clairement pas a_0 et donc F est irréductible. On a ainsi la courbe

$$C = Z(X^{q+1} + Y^{q+1} - 1)$$

sur $K = \overline{\mathbb{F}}_q$.

Définition 1.1.4 *: Soit C une courbe affine. L'anneau quotient $K[C] = \frac{K[X,Y]}{I(C)}$ est appelé l'anneau des coordonnées (ou l'anneau des fonctions régulières sur C).*

Comme $I(C)$ est un idéal premier, $K[C]$ est un anneau intégre (sans diviseurs de zéro : $ab = 0 \Rightarrow a = 0$ ou $b = 0$). Un élément f de $K[C]$ est une classe d'équivalence modulo $I(C)$:

$$f = F + I(C) = F \pmod{I(C)}$$

et f peut -être vue comme une fonction sur C :

$$\begin{array}{rcl} f : C & \longrightarrow & K \\ P & \longmapsto & f(P) = F(P). \end{array}$$

Définition 1.1.5 *: Une fonction régulière sur C est une application*

$$f : C \longrightarrow K.$$

telle qu'il existe $F \in K[X, Y]$ avec $f = F_{/_C}$ (ie $f(P) = F(P), \forall P \in C$).

Les fonctions régulières sur C sont donc les éléments $f \in K[C]$ (ceci explique pourquoi $K[C]$ est appelé l'anneau des fonctions régulièrs). Comme $K[C]$ est intègre, il a un corps des fractions qu'on va noter $K(C)$:

$$K(C) = \{f = \frac{\overline{g}}{h}, \quad g, h \in K[C], \quad h \neq 0\}$$

avec $\frac{\overline{g}}{h} = \frac{\overline{g'}}{h'} \Leftrightarrow gh' = g'h$. $K(C)$ est appelé le corps des fonctions rationnelles sur C car tout élément $f \in K(C)$ définit une fonction :

$$f : C \longrightarrow K$$

f est définie en $P \in C$ si on peut l'écrire $f = \frac{g}{h}$ avec $g, h \in K[C]$ et $h(P) \neq 0$. On pose alors :

$$f(P) = \frac{g(P)}{h(P)}$$

On a evidemment des inclusions :

$$K \subseteq K[C] \subseteq K(C)$$

Pour tout point $P \in C$, on pose :

$$O_P(C) = \{f \in K(C)/ \text{ f définie en P}\}$$

C'est un anneau local au sens algébrique. Son unique idéal maximal est :

$$M_P(C) = \{f \in K(C)/f(P) = 0\}$$

Si $C = Z(F)$ avec $F \in K[X, Y]$ irréductible est une courbe affine, un point $P \in C$ est dit singulier si

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = 0$$

Sinon P est non singulier.

Définition 1.1.6 *: Une courbe affine C est non singulière si tous ses points sont non singuliers.*

Remarque 1.1.1 *: La non singularité de $P \in C$ peut se lire sur son anneau local $O_P(C)$: P est non singulier $\Leftrightarrow$ L'anneau $O_P(C)$ est un anneau de valuation discrète [3].*

Exemple 1.1.3 *: Soit $C = Z(X^2 + Y^2 - 1)$. On a :*

$$\frac{\partial F}{\partial X}(P) = 2X \quad et \quad \frac{\partial F}{\partial Y}(P) = 2Y$$

donc $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = 0 \Leftrightarrow P = (0, 0)$. Mais $P = (0, 0)$ n'appartient pas à C. Tous les points de C sont donc non singuliers et C est non singulière.

1.2 Courbes Projectives

Sur $K^3 - \{(0,0,0)\}$ définissons la relation :

$$(x,y,z) \backsim (x^{'},y^{'},z^{'}) \Leftrightarrow \exists \lambda \in K^* / x = \lambda x, y = \lambda y, z = \lambda z$$

On vérifie facilement que c'est une relation d'équivalence. La classe de (x,y,z) sera noteé $(x:y:z)$. Le plan projectif $\mathbb{P}^2 = \mathbb{P}^2(K)$ est :

$$\mathbb{P}^2(K) = \{(x:y:z)/(x,y,z) \neq (0,0,0)\}$$

$$= \frac{K^3 - \{(0,0,0)\}}{\sim}$$

Si $P = (a:b:c) \in \mathbb{P}^2(K)$, a,b,c sont appeleés les coordonneés homogènes (ou projectives) de P.

Définition 1.2.1 *: Un monôme de degré d est un polynôme $G \in K[X,Y,Z]$ de la forme :*

$$G = aX^{d_1}Y^{d_2}Z^{d_3}$$

avec $a \neq 0 \in K$ et $d_1 + d_2 + d_3 = d$. Un polynôme $F \in K[X,Y,Z]$ est dit homogène s'il est la somme de monômes de même degré. Un idéal $I \subseteq K[X,Y,Z]$ est homogène s'il est engendré par des polynômes homogènes.

Soient $P = (a:b:c) \in \mathbb{P}^2$ et $F \in K[X,Y,Z]$ homogéne. Comme $F(\lambda a, \lambda b, \lambda c)$ $= \lambda^d F(a,b,c)$ (avec d le degré de F), l'écriture :

$$F(P) = 0$$

a un sens pour $P \in \mathbb{P}^2$.

Définition 1.2.2 *: Un ensemble algébrique de $\mathbb{P}^2$ est un ensemble de la forme :*

$$V = Z(M) = \{P \in \mathbb{P}^2 / F(P) = 0,\ \forall F \in M\}.$$

avec $M \subseteq K[X,Y,Z]$ une partie de polynômes homogènes. L'idéal de V est :

$$I(V) = \{F \in K[X,Y,Z] \quad \textit{homogène} / F(P) = 0, \forall P \in V\}$$

V est irréductible ssi $I(V)$ est un idéal premier.

Comme dans le cas affine, on arrive à la définition d'une courbe projective (plane) :

Définition 1.2.3 *: Une courbe projective plane est un ensemble algébrique $\overline{C}$ qui est irréductible et "général" (général a le même sens que dans le cas affine).*

Ainsi $\overline{C}$ s'écrit :

$$\overline{C} = Z(F) = \{P \in \mathbb{P}^2 / F(P) = 0\}$$

avec F un polynôme homogène irréductible. Avant de donner quelques exemples nous allons voir qu'il y a un lien entre les courbes affines et les courbes projectives. Soient les applications :

$$\begin{array}{rccc} \phi_1 : & \mathbb{A}^2 & \longrightarrow & \mathbb{P}^2 \\ & (a,b) & \longmapsto & (1,a,b) \end{array}$$

$$\begin{array}{rccc} \phi_2 : & \mathbb{A}^2 & \longrightarrow & \mathbb{P}^2 \\ & (a,b) & \longmapsto & (a,1,b) \end{array}$$

$$\begin{array}{rccc} \phi_3 : & \mathbb{A}^2 & \longrightarrow & \mathbb{P}^2 \\ & (a,b) & \longmapsto & (a,b,1) \end{array}$$

ϕ_1 , ϕ_2 et ϕ_3 appliquent bijectivement $\mathbb{A}^2$ sur les partie :

$$U = \{(a:b:c) \in \mathbb{P}^n / a \neq 0\}$$

$$V = \{(a:b:c) \in \mathbb{P}^n / b \neq 0\}$$

$$W = \{(a:b:c) \in \mathbb{P}^n / c \neq 0\}$$

De plus on voit bien que :

$$\mathbb{P}^2 = U \cup V \cup W$$

et $\mathbb{P}^2$ est recouvert par trois copies de $\mathbb{A}^2$. Soit $\overline{C}$ une courbes projective. Alors

$$\overline{C} = (\overline{C} \cap U) \cup (\overline{C} \cap V) \cup (\overline{C} \cap W)$$

Donc $C_1 = (\overline{C} \cap U)$, $C_2 = (\overline{C} \cap V)$ et $C_3 = (\overline{C} \cap W)$ sont des courbes affines données par les idéaux :

$$I(C_1) = \{F(1,Y,Z), F \in I(\overline{C})\}$$

$$I(C_2) = \{F(X, 1, Z), F \in I(\overline{C})\}$$
$$I(C_3) = \{F(X, Y, 1), F \in I(\overline{C})\}$$

Les polynômes $F(1, Y, Z)$, $F(X, 1, Z)$ et $F(X, Y, 1)$ sont appelés les deshomogénisations de F. Ainsi toute courbe projective donne naissance à trois courbes affines et on a par exemple :

$$\overline{C} = C_1 \cup (\overline{C} \cap H_U)$$

avec $H_U = \mathbb{P}^2 - U$ (on suppose bien sur $\overline{C} \cap U \neq \emptyset$ sinon on choisit V ou W). H_U est appelé hyperplan à l'infini. Ses points sont les points à l'infini. On a donc montré :

Proposition 1.2.1 *: Toute courbe projective $\overline{C}$ est la réunion d'une courbe affine C et de points à l'infini.*

Exemple 1.2.1 *: Soit $\overline{C} = Z(X^2 + Y^2 - Z^2)$. En faisant $Z = 1$, on obtient la courbe affine $C_3 = Z(X^2 + Y^2 - 1) = \overline{C} \cap W$. les points à l'infini sont ceux pour lequels $Z = 0$:*

$$\overline{C} \cap H_W = \{P = (a : b : c) \in \overline{C} / c = 0\}$$

Comme a, b, c ne doivent pas être tous nuls, a ou b doit être non nul. Supposons $a \neq 0$ et donc $a = 1$. Les points à l'infini sont donc les $(1, b, 0)$ avec $b^2 + 1 = 0$. Si $K = \mathbb{C}$ par exemple , on trouve $b^2 = -1$ et $b = \pm i$, ce qui donne deux points à l'infini : $(1, i, 0)$ et $(1, -i, 0)$. (Remarquer que $b^2 + 1 = 0$ a toujours des solutions dans tout corps K algébriquement clos). En faisant $X = 1$, on obtient C_1 et en faisant $Y = 1$, on obtient C_2. On a donc par exemple, si $K = \mathbb{C}$:

$$\overline{C} = C_3 \cup \{(1, i, 0), (1, -i, 0)\}$$

Si $F \in K[X, Y]$, son homogéinesé est le polynôme $F^h \in K[X, Y, Z]$ donné par :

$$F^h(X, Y, Z) = Z^d F(\frac{X}{Z}, \frac{Y}{Z}).$$

avec $d = degF$. F^h est un polynôme homogène et il est irréductible si F l'est.

Définition 1.2.4 *: Soit $C = Z(F)$ courbe affine. La clôture projective de C est :*

$$\overline{C} = Z(F^h)$$

C'est une courbe projective (plane).

On peut récuper C à partir de $\overline{C}$ par :

$$C = \phi_3^{-1}(\overline{C} \cap W)$$

Exemple 1.2.2 *: Reprenons l'exemple de* $C = Z(X^2+Y^2-1)$ *avec* $F(X,Y) = X^2+Y^2-1$. *L'homogéneisé de* F *est :*

$$F^h(X,Y,Z) = Z^2F(\frac{X}{Z},\frac{Y}{Z})$$

$$= Z^2(\frac{X^2}{Z^2}+\frac{Y^2}{Z^2}-1)$$

$$= X^2+Y^2-Z^2$$

et $\overline{C} = Z(F^h)$ *est la courbe projective de l'exemple précédent.*

Contrairement aux courbes affines, on ne peut parler de fonctions régulières pour les courbes projectives. En effet une fonction régulière sur $\overline{C}$ serait la restriction d'un polynôme homogène à $\overline{C}$. Mais si $F(X,Y,Z) \in K[X,Y,Z]$, on a $F(a,b,c) \neq \lambda^d F(a,b,c) = F(\lambda a, \lambda b, \lambda c)$ en général (d = degré de F) et donc $F(P)$ ne serait pas définie pour $P = (a:b:c) \in \overline{C}$. Par contre la notion de fonction rationnelle persiste.

Définition 1.2.5 *: Une fonction rationnelle sur* $\overline{C}$ *est la classe d'équivalence* $\frac{G}{H}$ *avec* G, H *des polynômes homogènes de même degré pour la relation déquivalence* $\frac{G}{H} \equiv \frac{G'}{H'} \Leftrightarrow GH' = G'H$.

On obtient donc :

$$f : \overline{C} \longrightarrow K$$

f est définié en P si on peut l'écrire $f = \frac{G}{H}$ avec $H(P) \neq 0$. On pose alors

$$f(P) = \frac{G(P)}{H(P)}.$$

Remarquer que comme G et H ont même degré, cette dernière écriture a un sens. En effet si $P = (a:b:c)$, on a :

$$f(a,b,c) = \frac{G(a,b,c)}{H(a,b,c)}.$$

et

$$f(\lambda a, \lambda b, \lambda c) = \frac{\lambda^d G(a,b,c)}{\lambda^d H(a,b,c)} = \frac{G(a,b,c)}{H(a,b,c)}$$

Les fonctions rationnelles sur $\overline{C}$ forment un corps $K(\overline{C})$. C'est le corps des fonctions rationnelles sur $\overline{C}$. Comme $\overline{C}$ est irréductible $I(\overline{C})$ est premier et donc :

$$K[\overline{C}] = \frac{K[X,Y,Z]}{I(\overline{C})}$$

est un anneau integre et a donc un corps quotient qu'on va noter $Quot(K[\overline{C}])$.
Le corps $K(\overline{C})$ des fonctions rationnelles sur $\overline{C}$ est un sous-corps de $Quot(K[\overline{C}])$.

$$K(\overline{C}) = \{\frac{\overline{G}}{H}, \quad G, H \in K[\overline{C}], \quad degG = degH, \quad H \neq 0\}$$

Le corps des fonctions rationnelles d'une courbe projective est isomorphe au corps des fonctions rationnalles de l'une des courbes affines associés.Par exemple si $f = \frac{G}{H}$ est une fonction rationnelle sur $\overline{C}$, alors

$$g = \frac{G(X,Y,1)}{H(X,Y,1)}$$

est une fonction rationnelle sur C_3. Inversement par homogénéisation toute fonction sur C_3 donnera une fonction sur $\overline{C}$.
L'anneau local en $P \in \overline{C}$ d'une courbe projective est :

$$O_P(\overline{C}) = \{f \in K(\overline{C}) / \text{ f définie en P}\}$$

C'est aussi un anneau local d'idéal maximal :

$$M_P(\overline{C}) = \{f \in O_P(\overline{C}) / f(P) = 0\}$$

La non singularité se définit comme dans le cas affine. Si $\overline{C} = Z(F)$ avec $F \in K[X,Y,Z]$ homogène alors $P = (a:b:c) \in \overline{C}$ est singulier si :

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0$$

en P. Sinon P est non singulier. $\overline{C}$ est non singulière ou régulière si tous ses points sont non singuliers.
Une courbe projective est donc formée d'une partie affine plus les points à l'infini :

$$\overline{C} = C \cup \{ \text{ points à l'infini } \}$$

Le nombre de points à l'infini est fini. En effet si on fait $Z = 0$ et $X = 1$, les points à l'infini sont les $(1, b, 0)$ avec b solution de

$$F(1, Y, 0) = 0.$$

C'est un polynôme en Y disons de degré n et il y a au plus n solutions.

1.3 Ordre d'une fonction en un point

La discussion etant de nature locale en P, on peut supposer que notre courbe C une courbe affine. Soit donc C une courbe affine et $P \in C$. L'anneau local de C en P est :

$$O_{P,C} = \{f \in K(C)/\text{f définie en P}\}$$

d'idéal maximal :

$$M_P(C) = \{f \in K(C)/f(P) = 0\}.$$

$O_P(C) - M_P(C) = U_P(C)$ sont les unités de $O_{P,C}$ *i.e* les éléments inversibles pour la multiplication. On peut caractériser la non singularité de P de manière purement algébrique ne faisant pas intervenir l'equation de C :

Proposition 1.3.1 *: $P \in C$ est non singulier si et seulement si $M_P(C)$ est un idéal principal de $O_P(C)$. De plus tout idéal de $O_{P,C}$ est de la forme $M_P(C)^n$. Si $f \in O_P(C)$, l'ordre de f en P est :*

$$v(f) = ord_P(f) = min\{n/f \in M_P(C)^n\}$$

Pour P non singulier, on obtient donc une application (une valuation) :

$$\begin{array}{rccc} v: & O_P(C) & \longrightarrow & \mathbb{N} \cup \infty \\ & f & \longmapsto & v(f) \end{array}$$

C'est une valuation discrète sur $O_P(C)$ *i.e* que v a les propriétés :

* $v(f + g) \geqslant min(v(f), v(g))$.
* $v(fg) = v(f) + v(g)$.
* $v(0) = \infty, v(a) = 0$ si a $\in K$.

Définition 1.3.1 *: Un paramètre local en P est un générateur t de $M_P(C)$. En particulier $v(t) = 1$.*

Deux paramètres locaux t, t' diffèrent par une unité $u \in U_P(C)$:

$$t' = ut$$

et tout élément $f \in O_P(C)$ s'écrit :

$$f = ut^n$$

avec $n = v(f), u \in U_P(C)$. On peut étendre v à $K(C)$ entier en posant :

$$v(\frac{f}{g}) = v(f) - v(g)$$

Tout $f \in K(C)$ s'écrit alors :

$$f = ut^n$$

avec cette fois ci, $n \in \mathbb{Z}$ et $n = ord_P(f) = v(f)$.

Définition 1.3.2 *: La fonction rationnelle f a un zéro d'ordre m en P si $ord_P(f) = m > 0$. Elle a un pôle d'ordre m en P si $ord_P(f) = -m < 0$ avec $m > 0$. Si $ord_P(f) = 0$, alors f est définie en P et $f(P) \neq 0$.*

En termes de la valuation V, on a :

$$O_P(C) = \{f \in K(C)/v(f) \geq 0\}$$
$$M_P(C) = \{f \in K(C)/v(f) > 0\}$$
$$U_P(C) = \{f \in O_P(C)/v(f) = 0\}$$

Exemple 1.3.1 *: Soit $C = Z(X^2 + Y^2 - 1)$. Tous les points de C sont non singuliers. Soit $P = (1, 0) \in C$, $y = Y \pmod{X^2+Y^2-1}$ est un paramètre local en P puisque $y(P) = 0$. Soit $f = 1 - x$ ($x = X \pmod{X^2 + Y^2 - 1}$). On peut écrire :*

$$f = 1 - x = \frac{1}{1+x}.y^2$$

$\frac{1}{1+x}.(P) \neq 0$, donc $\frac{1}{1+x} \in U_P(C)$. L'ordre de f en P est donc $ord_P(f) = 2$.

Remarque 1.3.1 *: Bien sur la même démarche aurait pu être faite dans le cas d'une courbe projective avec les mêmes résultats. Nous mentionnons neanmoins un résultat important qui marche dans le cas projectif mais pas dans le cas affine : Soit $\overline{C}$ une courbe projective non singulière. Soit $f \in \overline{K}(C)$ une fonction rationnelle. Alors f a autant de zéros que de pôles (comptés avec multiplicité). Voir par exemple [3] ou [15]*

1.4 Applications entre Courbes

Intuitivement une application entre courbes envoie un point vers un autre point mais peut ne pas être définie partout. Soient $\overline{C_1}$ et $\overline{C_2}$ deux courbes projectives. Une application rationnelle :

$$\phi : \overline{C_1} \longrightarrow \overline{C_2}$$

est une application de la forme $\phi = (f_1, f_2, f_3)$, avec $f_1, f_2, f_3 \in \overline{C_1}$ des fonctions rationnelles, telles que $(f_1(P), f_2(P), f_3(P)) \in K(\overline{C_2})$ en tout point P en laquel les f sont définies (et au moin un $f_i(P) \neq 0$).

Définition 1.4.1 *: $\phi = (f_1, f_2, f_3) : \overline{C_1} \longrightarrow \overline{C_2}$ est définie en $P \in \overline{C_1}$ si on peut trouver une fontion $g \in K(\overline{C_1})$ telle que :*

- *gf_i définie en P, $\forall i$.*
- *$(gf_i)(P) \neq 0$ pour au moins un i.*

On pose alors :

$$\phi(P) = (gf_1(P), gf_2(P), gf_3(P))$$

Remarque 1.4.1 *:*

1. *$g = 1$ est possible.*
2. *g dépend de P. pour un autre point il peut être nécessaire de changer de g.*

Un morphisme entre courbes est une application rationnelle partout définie. Un isomorphisme est un morphisme bijectif d'inverse un morphisme.

Proposition 1.4.1 *: L'application rationnelle $\phi : \overline{C_1} \longrightarrow \overline{C_2}$ est définie en P si $P \in \overline{C_1}$ est non singulier.*

Preuve : Soit $\phi = (f_1, f_2, f_3)$ avec $f_i \in K(\overline{C_1})$. Soit t un paramètre local en $P \in \overline{C_1}$, posons :

$$n = min_{i=1,2,3} ord_P(f_i)$$

On a alors :

$$ord_P(t^{-n} f_i) \geq 0, \forall i = 1, 2, 3$$

et

$$ord_P(t^{-n} f_j) = 0$$

pour au moins un j et $t^{-n} f_1$, $t^{-n} f_2$ et $t^{-n} f_3$ sont donc définies en P et $t^{-n} f_j(P) \neq 0$. Cela veut dire que ϕ est définie en P.

Corollaire 1.4.1 *: Si $\overline{C_1}$ est non singulière, alors toute application rationnelle $\phi : \overline{C_1} \longrightarrow \overline{C_2}$ est un morphisme.*

Preuve : Tous les points sont non singulièrs. Appliquer la proposition précédente. Signalons aussi (saus démonstration) que si $\phi : \overline{C_1} \longrightarrow \overline{C_2}$ est non constante, alors elle est forcément surjective.
Un morphisme $\phi : \overline{C_1} \longrightarrow \overline{C_2}$ réduit par composition avec ϕ, un morphisme (injectif entre corps) :

$$\begin{array}{rcl} \phi^* : K(\overline{C_1}) & \longrightarrow & K(\overline{C_2}) \\ f & \longmapsto & \phi^* f = f \circ \phi. \end{array}$$

Entre les corps de fonctions des deux courbes.

1.5 Diviseurs et Différentielles

Soit $\overline{C}$ une courbe projective non singulière (sur un corps K-algebriquement clos).

Définition 1.5.1 *: Un diviseur sur $\overline{C}$ est un élément D du groupe abelien libre engendré par les points de C.Un tel diviseurs sécrit donc :*

$$D = \sum_{P \in \overline{C}} n_P P$$

avec $n_P \in \mathbb{Z}$ et $n_P = 0$ pour presque tout P .

Le support de D est :

$$suppD = \{P \in \overline{C} / n_P \neq 0\}$$

L'addition de deux diviseurs

$$D = \sum_{P \in \overline{C}} n_P P \quad et \quad D = \sum_{P \in \overline{C}} n_{P'} P.$$

est :

$$D + D' = \sum_{P \in \overline{C}} (n_P + n_{P'}) P$$

Le diviseur 0 et $D = \sum n_P P$ avec $n_P = 0, \forall P$. Un ordre pariel sur les diviseurs peut être défini par :

$$D \leq D' \Longleftrightarrow n_P \leq n_{P'}, \forall P \in \overline{C}$$

Si $n_P \geq 0$ pour tout P, D est un diviseur effectif.

Définition 1.5.2 *: Le degré du diviseur $D = \sum n_P P$ est*

$$degD = \sum_{P \in \overline{C}} n_P$$

si $f \in K(\overline{C})$ est une fonction rationnelle sur $\overline{C}$, son diviseur est :

$$(f) = \sum_{P \in \overline{C}} v_P(f)P = \sum_{P \in \overline{C}} ord_P(f)P.$$

Un tel diviseur est dit principal.
Deux diviseurs D et $D^{'}$ seront dits linéairement équivalents si $D - D^{'} = (f)$ pour une certaine fonction f

Comme une fonction rationnelle f a autant de zéros que de pôles (comptés avec multiplicité), on a :

$$deg(f) = \sum_{P \in \overline{C}} ord_P(f) = 0$$

Ainsi l'application :

$$\begin{array}{rcl} deg : Div(\overline{C}) & \longrightarrow & \mathbb{Z} \\ D & \longmapsto & degD. \end{array}$$

descend au quotient par l'equivalence linéaire :

$$\begin{array}{rcl} deg : \frac{Div(\overline{C})}{Prin(\overline{C})} & \longrightarrow & \mathbb{Z} \\ [D] & \longmapsto & deg[D] = degD. \end{array}$$

avec $Div(\overline{C})$ le groupe des diviseurs sur $\overline{C}$ et $Prin(\overline{C})$ le sous groupe des diviseurs principaux. $[D]$ est la classe du diviseur D modulo l'équivalence linéaire.

Définition 1.5.3 *Le groupe de Picard de $\overline{C}$ est :*

$$Pic(\overline{C}) = \frac{Div(\overline{C})}{Prin(\overline{C})}$$

Il a comme sous groupe

$$Pic^0(\overline{C}) = \frac{\{\text{Diviseurs de degré } 0\}}{Prin(\overline{C})}$$

On peut montrer que $Pic^0(\overline{C})$ est en fait une varieté algébrique. C'est la jacobienne de la courbe.
Soit $\overline{C}$ une courbe projective non singulière et soit $K(\overline{C})$ son corps des fonctions rationnelles.

Définition 1.5.4 *: L'espace des formes differentielles sur $\overline{C}$ est le K-espace vectoriel Ω_C engendré par les symbles de la forme df avec $f \in K(\overline{C})$ avec les relations :*

- *$d(f + g) = df + dg$.*
- *$d(fg) = f\,dg + g\,df \quad \forall f, g \in K(\overline{C})$.*
- *$d(\lambda) = 0, \forall \lambda \in K$.*

En tant que $K(\overline{C})$-espace vectoriel , Ω_C est de dimension 1 . Par exemple si $P \in \overline{C}$ et si t est un paramètre local en P, alors toute forme $\omega \in \Omega_C$ sécrit :

$$\omega = gdt$$

avec $g \in K(\overline{C})$ une fonction unique (mais qui dépend de ω et t). En particulier si $\omega = df = gdt$ alors $g = \frac{df}{dt}$ est appelleé la différentieble de f en t et g sera définie en P si f l'est.

Proposition 1.5.1 *: Soit $\omega \in \Omega_C$ avec $\omega \neq 0$. Si $\omega = gdt$ on pose $g = \frac{\omega}{dt}$. Alors $ord_P(\frac{\omega}{dt})$ ne dépend que de ω et P. On le note $ord_P(\omega)$.*

Preuve : Soit t' un autre paramètre local en P. Alors $\frac{dt}{dt'}$ et $\frac{dt'}{dt}$ sont toutes deux définies en P et donc $ord_P(\frac{dt'}{dt}) = 0$. Si $\omega = gdt'$ on a :

$$\omega = gdt' = g(\frac{dt'}{dt})dt$$

et

$$\frac{\omega}{dt'} = get\frac{\omega}{dt} = g(\frac{dt'}{dt})$$

donc $ord_P(\frac{\omega}{dt'}) = ord_P g$ et $ord_P(\frac{\omega}{dt}) = ord_P(g) + \underbrace{ord_P(\frac{dt'}{dt})}_{0} = ord_P(g)$ *i.e* $ord_P(\frac{\omega}{dt'}) = ord_P(\frac{\omega}{dt})$.

Remarque 1.5.1 *: Comme pour les fonctions rationnelles, on a* $ord_P(\omega) = 0$ *sauff pour un nombre fini de points* $P \in \overline{C}$.

Définition 1.5.5 *: La forme* ω *est régulière (ou holomorphe) si*

$$ord_P(\omega) \geq 0, \forall P \in \overline{C}$$

Elle est non nulle si

$$ord_P(w) \leq 0, \forall P \in \overline{C}$$

Deux formes différentielles non nulles ω_1, ω_2 diffèrent par une fonction rationnelle (Ω_C est un $K(\overline{C})$-espace de dimension 1) :

$$\omega_2 = f\omega_1$$

avec $f \in K(\overline{C})^*$.

Définition 1.5.6 *: Le diviseur de* $\omega \in \Omega_C$ *est :*

$$div(\omega) = \sum_{P \in \overline{C}} ord_P(w)P \quad \in Div(\overline{C})$$

Pour deux formes non nulles ω_1, ω_2 on a donc :

$$div(\omega_2) = div(f) + div(\omega_1)$$

si $\omega_2 = f\omega_1$. ie que $div(\omega_1)$ et $div(\omega_2)$ sont linéariement équivalents. Ceci motive la :

Définition 1.5.7 *: Le diviseur canonique de* $\overline{C}$ *est la classe dans* $Pic(\overline{C})$ *du diviseur d'une forme* ω *non nulle. On la note* $K_{\overline{C}}$.

$$K_{\overline{C}} = div(\omega) \in Pic(\overline{C})$$

1.6 Le théorème de Riemann-Roch

Soit $\overline{C}$ une courbe projective non singulière. Soit $D \in Div(\overline{C})$. On pose :

$$L(D) = \{f \in K(\overline{C})^* / div(f) + D \geq 0\} \cup \{0\}$$

Rappelons que $D \geq 0$ si $D = \sum n_P P$ et $n_P \geq 0, \forall P$ (un tel diviseur est dit effectif). $L(D)$ est donc l'ensemble des fonctions rationnelles sur $\overline{C}$ (non nulles) telles que $div(f) + D$ soit effectif. C'est un K-espace vectoriel de dimension finie. Si $D = \sum n_P P$ la condition $div(f) + D \geq 0$ veut dire que f a des pôles en P d'ordre au plus $-n_P$ si $n_P \leq 0$ et des zéros en P d'ordre n_P si $n_P > 0$. Cette condition d'éffectivité permet donc de décrire les pôles et les zéros des fonctions rationnelles.

Définition 1.6.1 *: On note* $l(D) = dim_K L(D)$

Exemple 1.6.1 *:*

1. *Si* $degD < 0$ *alors* $L(D) = \{0\}$ *et* $l(D) = 0$. *En effet si* $f \in L(D)$ *et* $f \neq 0$, *on a :* $0 = deg(div(f)) \geq deg(-D) = -deg(D)$ *et donc* $deg(D) \geq 0$
2. *Si* D *et* D' *sont deux diviseurs linéairement équivalents i.e* $D' = D + div(f)$, *alors* $L(D) \cong L(D')$ *et* $l(D) = l(D')$. *En effet l'application (linéaire) :*
$$\begin{array}{ccc} L(D) & \longrightarrow & L(D') \\ g & \longmapsto & gf. \end{array}$$
est un isomorphisme.
3. *Soit* $K_{\overline{C}} = div(\omega)$ *le diviseur canonique sur* $\overline{C}$. *Soit* $f \in L(K_{\overline{C}})$. *On doit donc avoir*
$$div(f) \geq -K_{\overline{C}}$$
et donc $div(f\omega) \geq 0$. *Autrement dit* $f\omega$ *est une forme holomorphe (ou régulière). Inversement si* $f\omega$ *est holomorphe, alors* $f \in L(K_{\overline{C}})$ *donc :* $L(K_{\overline{C}})$ *est isomorphe à l'espace des formes holomorphes sur* $\overline{C}$ *en envoyant* f *vers* $f\omega$.

Nous donons maintenant (sans démonstration) l'un des résultats les plus fondamentaux de la théorie des courbes algébriques. Nous l'utiliserons au chapitre deux pour trouver l'équation générale d'une courbe elliptique.

Théorème 1.6.1 *(Théorème de Riemann Roch)[3] : Soit* $\overline{C}$ *une courbe projective non singulière et soit* $K_{\overline{C}}$ *son diviseur canonique. Il existe un entier* $g \geq 0$, *appelé le genre de la courbe, tel que pour tout diviseur* $D \in Div(C)$ *on ait :*
$$l(D) - l(K_{\overline{C}} - D) = degD - g + 1$$

On peut déja trier quelques conséquences importantes de ce théorème. Par exemple on a $l(K_{\overline{C}}) = g$. En effet en prenant $D = 0$ le théorème donne :

$$l(0) - l(K_{\overline{C}}) = deg(0) - g + 1$$

$$1 - l(K_{\overline{C}}) = 1 - g$$

$$l(K_{\overline{C}}) = g$$

$$(L(0) = K, l(0) = 1)$$

On aurait d'ailleurs pu définir le genre g comme la dimension $l(K_{\overline{C}})$ de $L(K_{\overline{C}})$, ou en en termes du degré de $K_{\overline{C}}$ puisque le théorème donne aussi :

$$degK_{\overline{C}} = 2g - 2$$

En effet si $D = K_{\overline{C}}$, on a :

$$l(K_{\overline{C}}) - l(K_{\overline{C}} - K_{\overline{C}}) = degK_{\overline{C}} - g + 1$$

$$g - 1 = degK_{\overline{C}} - g + 1$$

$$degK_{\overline{C}} = 2g - 2$$

Enfin le théorème permet de déterminer $l(D)$ si le degré de D assez large. plus exactement on a :

$$l(D) = degD - g + 1$$

Si $degD > 2g - 2$. En effet si $degD > 2g - 2$ alors $deg(K_{\overline{C}} - D) < 0$. Donc $L(K_{\overline{C}} - D) = \{0\}$ et $l(K_{\overline{C}} - D) = 0$. Le théorème donne :

$$l(D) - 0 = degD - g + 1$$

$$l(D) = degD - g + 1$$

1.7 Courbes sur un corps non algébriquement clos

L'étude des courbes sur des corps non algébriquement clos est assez courante et est trés importante. Selon la nature du corps K, cette étude peut prendre différentes formes. Par exemple l'étude de l'arithmetique des courbes a lieu quand le corps K est par exemple un corps fini, un corps local, ou un

corps global ($\mathbb{Q}$, ou les corps de nombres). Il est donc nécessaire de se debarasser de la condition que K soit un corps algébriquement clos. Dans ce mémoire, nous donnons les changements qui doivent s'imposer dans toutes les discussions précédentes quand K n'est pas algébriquement clos. Soit donc K un corps (parfait) et soit $\overline{K}$ sa clôture algébrique.
Une courbe affine $C \subseteq \mathbb{A}^2(\overline{K})$ sera dite définie sur K si $C = Z(F)$ avec $F \in K[X,Y]$. L'ensemble :

$$C(K) = C \cap \mathbb{A}^2(K) = \{P = (a,b) \in C / a, b \in K\}$$

est appelé l'ensemble des points rationnels de C sur K. De même une courbes projective $\overline{C} \subseteq \mathbb{P}^2(\overline{K})$ sera dite définie sur K si $\overline{C} = Z(F)$ avec $F \in K[X,Y,Z]$. Un point $P \in \overline{C}$ est K-rationnel s'il a des coordonnées homogènes $a, b, c \in K$. L'ensemble :

$$\overline{C}(K) = \{P \in \overline{C} / \text{P est K-rationnel}\}$$

est l'ensemble des points de $\overline{C}$ a coordonnées dans K. Si $C \subseteq \mathbb{A}^2(\overline{K})$ est une courbe affine définie sur K, posons :

$$I(C/K) = I(C) \cap K[X,Y]$$

$I(C/K)$ est un idéal et on peut aussi définir

$$K[C] = \frac{K[X,Y]}{I(C/K)}$$

qui est un anneau intègre ($I(C)$ premier $\Rightarrow I(C/K)$ premier). Le corps quotient :

$$K(C) = Quot(K[C]) \subseteq \overline{K}(C)$$

est le corps des fonctions rationnelles sur C définies sur K ou encore le corps des K-fonctions rationnelles. On définit de même le corps des K-fonctions d'une courbe projective $\overline{C}$ définie sur K. Une application rationnelle $\phi : \overline{C_1} \longrightarrow \overline{C_2}$ entre deux courbes projectives définie sur K sera dite définie sur K si $\phi = (f_1, f_2, f_3)$ avec les f_i des fonction K-rationnelles.
Une autre manière de décrire les points K-rationnels, les fonctions K-rationnelles, etc ...est d'utiliser le groupe de Galois $G = Gal(\overline{K}/K)$. L'action de G sur $\overline{K}$ s'étend naturellement en une action de G sur $\mathbb{A}^2(\overline{K})$, $\mathbb{P}^2(\overline{K})$, $\overline{K}[X,Y]$, $\overline{K}[X,Y,Z]$, $\overline{C}$, C, $\overline{K}[C]$ et $\overline{K}(C)(= \overline{K}(\overline{C}))$. Soit par exemple $\overline{C} \subseteq \mathbb{P}^2(\overline{K})$ une

courbe projective définie sur K. Si $P = (a : b : c) \in \overline{C}$ et $\sigma \in G$, l'action de σ sur P est :

$$\sigma(P) = (\sigma(a) : \sigma(b) : \sigma(c))$$

et on a

$$\overline{C}(K) = \{P \in \overline{C} / \sigma(P) = P, \forall \sigma \in G\}$$

$$K(C) = \{f \in \overline{K}(\overline{C}) / \sigma(f) = f, \forall \sigma \in G\}$$

etc,...(σ opère sur f en opérant sur les coefficients des polynômes G, H tels que $f = \frac{g}{h}$ avec $g = G \bmod I(\overline{C})$ et $h = H \bmod I(\overline{C})$). Un diviseur

$$D = \sum_{P \in \overline{C}} n_P P \in Div(\overline{C})$$

est définie sur K si $\sigma(D) = D$ pour tout $\sigma \in G = Gal(\overline{K}/K)$ (cela veut dire que $n_{\sigma(P)} = nP, \forall P \in \overline{C}$). Les diviseures de $\overline{C}$ définis sur K forment un sous-groupe $Div(\overline{C}/K) \subseteq Div(\overline{C})$. Pour $D \in Div(C/K)$, l'espace :

$$L_K(D) = K(\overline{C}) \cap L(D)$$

est un K-espace vectoriel de dimension finie et sa dimension (sur K) est égale à la dimension de $L(D)$ (sur $\overline{K}$). Un diviseur $D \in Div(\overline{C}/K)$ avec $D > 0$ est dit premier si D ne peut pas s'ecrire $D = D_1 + D_2$ avec D_1, D_2 effectifs $\in Div(\overline{C}/K)$. $Div(\overline{C}/K)$ est engendré par les diviseurs premiers qui correspondent en quelque sorte aux points rationnels de $\overline{C}$ sur K et ses différentes extensions algébriques.

Chapitre 2

Courbes Elliptiques

Dans ce chapitre nous définissons ce qu'est une courbe elliptique sur un corps quelconque. Nous utilisons le théorème de Riemann-Roch pour caractériser ces courbes en termes d'un polynôme particulier appelé équation de Weirstrass. La courbe elliptique est alors la réunion de la courbe affine donnée par ce polynôme plus exactement un point à l'infini. Quand la caractéristique du corps est différente de 2 et 3, l'équation de Weirstrass se simplifie encore et prend la forme simple $Y^2 = X^3 + AX + B$ avec une condition sur les coefficients A et B qui reflète la non singularité de la courbe. Un fait remarquable, qui est à l'origine des nombreuses applications des courbes elliptiques, est que les points de la courbe forment un groupe pour une certaine opération d'addition. Cette addition est définie dans un premier temps purement de manière géométrique mais nous en donnons une expression algébrique qui utilise l'équation de Weirstrass. Les fonctions rationnelles da la courbe vers elle même qui préservent cette structure de goupe seront appelés ici des endomorphismes et acquièrent une importance capitale dans l'étude des propriétés de la courbe. Parmi eux notons les endomorphismes de multiplication par m pour $m \in \mathbb{Z}$ qui servent par exemple à définir les points de torsion de la courbe comme étant les éléments du noyau de la multiplication par m pour différents m. Nous caractérisons ces points à la fin du chapitre en termes de polynômes spéciaux appelés les polynômes de division. Ces polynômes permettent aussi de calculer les multiples nP d'un point P. Pour ce chapitre notre référence principale est [15], mais nous utilisons aussi l'approche plus élémentaire de [2], pour définir par exemple le degré et la séparabilité d'un endomorphisme.

2.1 Définition

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

Définition 2.1.1 *: Une courbe elliptique (sur $\overline{K}$) est une paire $(\overline{E}, O)$ avec $\overline{E}$ une courbe projective non singulière de genre 1 et O un point de $\overline{E}$. La courbe elliptique $(\overline{E}, O)$ est définie sur K si $\overline{E}$ est définie sur K (en tant que courbe) et $O \in E(K)$.*

On sait que $\overline{E} = Z(F)$ avec $F(X, Y, Z) \in K[X, Y, Z]$ (si $\overline{E}$ est définie sur K). Le théorème de Riemann-Roch va nous permettre de déterminer la nature de F. Remarquons d'abord que, par Riemann-Roch, on a :

$$dimL(n(O)) = deg(nO) - g + 1 = n$$

pour tout $n \geq 1$, puisque $g = 1$ et $deg(nO) = n > 2g - 2 = 0$. Il existe donc une fonction rationnelle x possédant un unique pôle d'ordre deux exactement en P et une fonction rationnelle y possédant un unique pôle d'ordre 3 exactement en P. Il y a donc 7 fonctions dans $L(6O)$ à savoir : $1, x, x^2, x^3, xy, y$ et y^2 et il doit donc y avoir une relation de dépendance entre elles : $\exists A_i, i = 1, ..., 7 \in K$ tel que :

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

qu'on peut arranger (voir [15]) en :

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

On obtient ainsi une application ($\overline{E}$ est non singulière) :

$$\begin{array}{rccc} \phi : \overline{E} & \longrightarrow & \mathbb{P}^2 \\ P & \longmapsto & (x(P) : y(P) : 1) \end{array}$$

dont l'image est la partie affine d'une courbe projective $\overline{C}$ dans $\mathbb{P}^2$ d'equation :

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

et par homogéneisation :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

$a_i \in K$. $\overline{C}$ n'a qu'un seul point à l'infini qui est $(0:1:0)$. De plus on a :

$$\phi(O) = (x(0), y(0), 1) = (\frac{x}{y}(0), 1, \frac{1}{y}(0)) = (0, 1, 0)$$

($\frac{1}{y}$ est définie en O est $\frac{1}{y}(O) = 0$, car y a un pôle d'ordre 2 en O, $\frac{x}{y}$ est définie en P et $\frac{x}{y}(O) = 0$). On a donc montré :

Proposition 2.1.1 *: Toute courbe elliptique $(\overline{E}, O)$ définie sur K est isomorphe à une courbe $\overline{C}$ d'équation (de Weierstrass) :*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

qui a un seul point à l'infini $(0:1:0)$ et qui correspond au point O de $\overline{E}$.

Grâce à cette proposition, on va identifier $\overline{E}$ à $\overline{C}$ et $(0:1:0)$ à O. De plus comme il n y a qu'un seul point à l'infini, on a :

$$\overline{E} = E \cup \{(0:1:0)\}$$

avec E la partie affine de $\overline{E}$ d'équation :

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

$a_1, ..., a_6 \in K$. On peut donc travailler avec cette partie affine (en n'oubliant pas le point à l'infini). Si le corps K est de caractéristique différente de 2 et 3, on peut encore simplifier l'equation de Weierstrass d'une courbe elliptique. Si car $(K) \neq 2$, on peut effectuer le changement de variable :

$$Y \longmapsto \frac{1}{2}(Y - a_1X - a_3)$$

pour transformer l'equation en :

$$Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6$$

avec $b_2 = a_1^2 + 4a_2$; $b_4 = 2a_4 + a_1a_3$ et $b_6 = a_3^2 + 4a_6$. Si de plus car $K \neq 3$, le changement de variables :

$$(X, Y) \longmapsto (\frac{X - 3b_2}{36}, \frac{Y}{108})$$

la transforme encore en :

$$Y^2 = X^3 + 27c_4X - 54c_6$$

avec $c_4 = b_2^2 - 24b_4$; $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. En posant $A = -27c_4$ et $B = -54c_6$, on obtient :

Théorème 2.1.1 *: Si car $K \neq 2, 3$, toute courbe elliptique $(\overline{E}, O)$ a une équation de Weierstrass (simplifiée) :*

$$Y^2 = X^3 + AX + B$$

avec

$$\Delta = -(4A^3 + 27B^2) \neq 0$$

et $A, B \in K$ si $\overline{E}$ est définie sur K.

Preuve : Il nous reste seulement à montrer la condition $\Delta = -(4A^3 + 27B^2) \neq 0$. Remarquons d'abord que le point à l'infini $(0 : 1 : 0)$ n'est jamais singulier. En effet, on a pour $F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3$ l'equation homgène de la courbe :

$$\frac{\partial F}{\partial Z} = Y^2 - 2AXZ - 3BZ^2$$

$= 1$ en $(0 : 1 : 0)$. S'il y a des points singuliers, ils doivent se situer dans la partie affine. Comme l'équation affine est $F(X, Y) = Y^2 - X^3 - AX - B$ un point singulier doit vérifier :

$$F = \frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = 0$$

en ce point. Un tel point existe donc si et seulement si le polynôme $P(X) = X^3 + AX + B$ a des racines multiples ce qui a lieu si et seulement si son discriminant

$$\Delta = \prod_{i \neq j} (r_i - r_j) = 0$$

avec les r_i, les racines du polynôme. On peut calculer le discriminant d'un polynôme du troisième degré $aX^3 + bX^2 + cX + d$ par :

$$\Delta = b^2c^2 + 18abcd - 27a^2d^2 - 4ac^3 - 4b^3d$$

Dans notre cas $a = 1, b = 0, c = A$ et $d = B$. Donc $\Delta = -(4A^3 + 27B^2)$. Comme une courbe elliptique est non singulière on doit donc avoir :

$$\Delta = -(4A^3 + 27B^2) \neq 0$$

Dans la suite de ce travail, on supposera toujours, en suivant Schoof [13], que $carK \neq 2, 3$. Pour nous une courbe elliptique sur un corps K sera toujours donnée par l'équation de Weierstrass simplifiée :

$$Y^2 = X^3 + AX + B$$

avec $-(4A^3 + 27B^2) \neq 0$. Le point base O étant la seul point à l'infini de la clôture projective de l'équation affine :

$$O = (0 : 1 : 0)$$

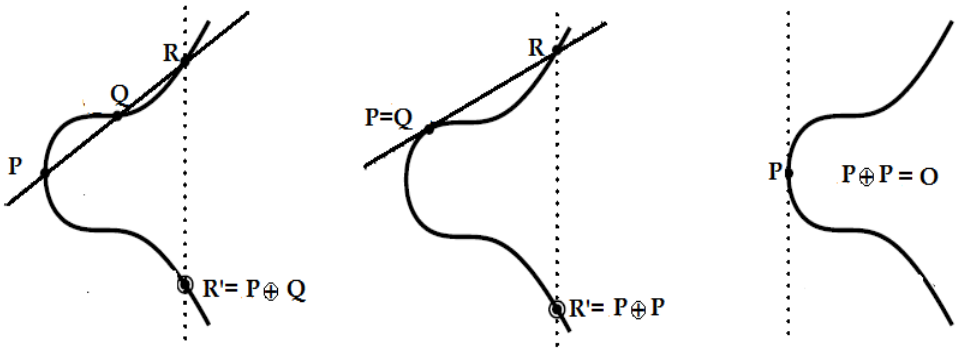
Remarquer aussi que le polynôme $Y^2 - X^3 - AX - B$ est irréductible. En effet on peut le réecrire $a_2Y^2 + a_1Y + a_0$ avec $a_2 = 1, a_1 = 0$ et $a_0 = -X^3 - AX - B$. Soit α une racine de $X^3 + AX + B$. Alors $P = X - \alpha$ est un polynôme irréductible qui divise a_0 et a_1 mais qui ne divise pas a_2. De plus P^2 ne divise pas a_0 car sinon le polynôme $X^3 + AX + B$ aurait α comme racine double, ce qui contredit la non-singularité de la courbe. On applique alors Eisenstein.

2.2 Loi de Groupe

Soit $\overline{E}$ une courbe elliptique d'équation de Weierstrass $Y^2 = X^3 + AX + B$ plus le point à l'infini $(0 : 1 : 0)$, avec $A, B \in \overline{K}$. Par le théorème de Bezout (voir par exemple Fulton [3]) toute droite D a exactement tois points d'intersection avec $\overline{E}$ (car l'équation de la courbe est de degré 3 et celle de la droité de degré 1 et $3.1 = 3$). Ces trois points peuvent ne pas être distincts, par exemple si D est la tangente à la courbe en un point. Ce fait est à la base de la définition d'une loi de groupe sur l'ensemble des points de la courbe elliptique, ce qui ouvre tant un champ d'applications inattendues (par exemple en théorie des codes et en cryptographie).

Définition 2.2.1 *: La loi $\oplus$ sur $\overline{E}(\overline{K})$ est définie de la manière suivante. Soient $P, Q \in E(\overline{K})$ et soit D la droite passant par P et Q (la tangente en P si $P = Q$). Soit R la troisième point d'intersection de D avec E et Soit D' la droite passant par R et le point à l'infini $O = (0 : 1 : 0)$. Soit R' la troisième point d'intersection de D' avec $\overline{E}$. On pose :*

$$P \oplus Q = R'$$



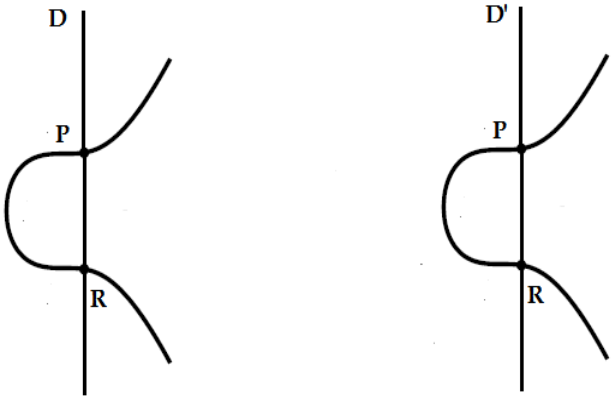
Remarque 2.2.1 *: La droite passant par R et O est la verticale à la courbe passant par R puisque O se situe sur la droite à l'infini (une droite horizontale à l'infini).*

Proposition 2.2.1 *: La loi $\oplus$ est une loi de groupe abélien sur $\overline{E}(\overline{K})$ d'elément neutre $O = (0 : 1 : 0)$.*

Preuve : Remarquons d'abord que si P, Q, R sont les points d'intersection de $D = PQ$ avec $\overline{E}$, alors on a $(P \oplus Q) \oplus R = O$. En effet la droite $RR^{'}$ avec $R^{'} = P \oplus Q$ rencontre la courbe en O et la droite OO (la tangente en O) rencontre la courbe en O. D'autre part la construction de $P \oplus Q$ est symétrique en P et Q et donc :

$$P \oplus Q = Q \oplus P$$

Ceci montre la commutativité. Montrons que O est élément neutre. Soient D et $D^{'}$ les droites passant respectivement par P, O et $P \oplus O, O$.



On a $D = D^{'}$. Les points d'intersection de D et $D^{'}$ avec E sont respectivement P, O, R et $R, O, P \oplus O$. Donc :

$$P \oplus O = P \qquad \forall P \in \overline{E}(\overline{K}).$$

Ceci montre que O est élément neutre. Soit R le point d'intersection de la droite $D = OP$ avec la courbe. On a donc :

$$(P \oplus O) \oplus R = O$$

$i.e$:

$$P \oplus R = O$$

et donc $R = \ominus P$ est le symétrique de P. Enfin pour l'associativité, voir un peu plus loin.
Cette définition géométrique de la loi de groupe n'est pas trés pratique et on a besoin de formules exprimant les coordonnées de $P \oplus Q$ et $\ominus P$ en termes de ceux de P et Q.
Supposons d'abord que $P \neq Q$ et $P \neq O, Q \neq O$. La droite $D = PQ$ a pour pente :

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ sont deux points de la courbe. Si $x_1 \neq x_2$, alors l'équation de la droite est :

$$y = m(x - x_1) + y_1$$

Les points d'intersection avec la courbe s'obtiennent en faisant :

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

ou encore

$$x^3 - mx^2 + \ldots = 0$$

On connait deux racines de cette equation qui sont x_1 et x_2. Si $x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t)$, On a :

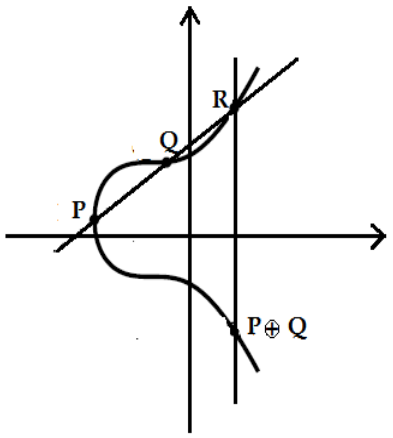
$$r + s + t = -a.$$

Donc les coordonnées (x, y) du $3^{\text{ème}}$ point d'intersection R vérifient :

$$\begin{array}{rcll} x & = & m^2 - x_1 - x_2. & \\ y & = & m(x - x_1) + y_1 & (ie \quad P \oplus Q = \ominus R). \end{array}$$

$P \oplus Q$ s'obtient en reflétant R par rapport à l'axe des x. Si $P \oplus Q = (x_3, y_3)$, on a donc :

$$\left\{ \begin{array}{rcl} x_3 & = & m^2 - x_1 - x_2 \\ y_3 & = & m(x_1 - x) - y_1 \end{array} \right.$$



Si $x_1 = x_2$(mais $y_1 \neq y_2$), la droite $D = PQ$ est verticale et le point R est O et donc $P \oplus Q = O$. Si $P = Q = (x_1, y_1)$ la droite $D = PQ$ est la tangente à la courbe en P. la pente $m = \underbrace{\frac{dy}{dx}}_{enP}$ de la tangente s'obtient par dérivation de l'équation de Weierstrass :

$$2y\frac{dy}{dx} = 3x^2 + A.$$

et donc

$$m = \underbrace{\frac{dy}{dx}}_{enP} = \frac{3x_1^2 + A}{2y_1}$$

Si $y_1 = 0$, cette tangente est verticale et donc $P \oplus Q = O$. Si $y_1 \neq 0$, l'équation de cette droite est :

$$y = m(x - x_1) + y_1.$$

et en substituant dans l'équation de la courbe, on obtient comme avant :

$$x^3 - m^2x^2 + \ldots = 0$$

On connait une racine double de cette équation, à savoir x_1. Si $P \oplus Q = (x_3, y_3)$, on a donc :

$$\left\{ \begin{array}{rcl} x_3 & = & m^2 - 2x_1 \\ y_3 & = & m(x_1 - x_3) - y_1 \end{array} \right.$$

Si P ou $Q = O$, on a bien sur :

$$P \oplus Q = P \qquad (Q = O)$$

ou :

$$P \oplus Q = 0 \qquad (P = O)$$

Pour calculer $\ominus P = (x^{'}, y^{'})$ il suffit de refléter $P = (x_0, y_0)$ par rapport à l'axe des x :

$$\left\{ \begin{array}{rcl} x^{'} & = & x_0 \\ y^{'} & = & -y_0 \end{array} \right.$$

En effet on a $P \oplus \ominus P \oplus O = O$ et donc la droite passant par P et $\ominus P$ est la verticale d'équation : $x = x_0$. En particulier $x^{'} = x_0$ et pour trouver $y^{'}$

il suffit de trouver la seconde racine de $y^2 - x_0^3 - Ax_0 - B = 0$, la première étant y_0. En faisant :

$$y^2 - x_0^3 - Ax_0 - B = c(y - y_0)(y - y^{'})$$

On obtient :

$$c = 1 \qquad et \qquad y^{'} = -y_0$$

On a donc obtenu un algorithme pour calculer l'addition de deux points et le symétrique d'un point :

Proposition 2.2.2 *: Soit $\overline{E}$ une courbe elliptique (sur $\overline{K}$) donnée par l'équation de Weierstrass : $Y^2 = X^3 + AX + B$ plus le point à l'infini $O = (0 : 1 : 0)$. Alors on a :*

1. *Si $P = (x_0, y_0) \in E(\overline{K})$, alors $\ominus P = (x_0, -y_0)$*
2. *Si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$, alors $P \oplus Q = (x_3, y_3)$ est donné par :*
   (a) *Si $x_1 = x_2$ et $y_1 \neq y_2$:*

$$P \oplus Q = O$$

   (b) $*$ *Si $x_1 = x_2$ et $y_1 = y_2 \neq 0$ (ie $P = Q$), on a :*

$$\begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

   avec

$$m = \frac{3x_1^2 + 1}{2y_1}$$

   $*$ *Si $x_1 = x_2$ et $y_1 = y_2 = 0$*

$$P \oplus Q = O$$

   (c) *Si $x_1 \neq x_2$, alors :*

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

   avec

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

D'aprés ces formules, les coordonnées de la somme ou de la différence de deux points sont rationnelles en les coordonnées des deux points. Autrement dit si les deux points sont à coordonnées dans un corps L sur lequel est définie la courbe , leur somme ou différence sont aussi des points à coordonnées dans ce corps. On obtient donc :

Corollaire 2.2.1 *: Si $\overline{E}$ est définie sur K, alors $\overline{E}(K)$, et plus généralement $E(L)$ pour $K \subseteq L \subseteq \overline{K}$, sont des sous-groupes de $\overline{E}(\overline{K})$, avec par exemple :*

$$\overline{E}(K) = \{(x, y) \in K^2 / y^2 = x^3 + Ax + B\} \cup \{O\}$$

les points rationnels de $\overline{E}$ sur K.

Il nous reste à montrer l'associativité de la loi de groupe. Pour cela on va montrer qu'il y a une bijection :

$$\begin{array}{rcl} \overline{E} & \longrightarrow & Pic^0(\overline{E}) = \frac{Div^0(\overline{E})}{Princ(\overline{E})} \\ P & \longmapsto & [P - O]. \end{array}$$

entre la courbe elliptique et sa jacobienne $J = Pic^0(\overline{E})$. Comme une courbe elliptique est de genre $g = 1$, on a $P \sim Q$ en tant que diviseurs si et seulement si $P = Q$ en tant que points. En effet si $P \sim Q$, soit $f \in \overline{K}(\overline{E})$ telle que : $div(f) = P - Q$. Donc $f \in L(Q)$. Par Riemann-Roch, $dim_{\overline{K}}(L(Q)) = 1$ *i.e* $L(Q) \cong \overline{K}$ et $f = \lambda \in \overline{K}$ ie $div(f) = 0$. Donc $P = Q$.

Proposition 2.2.3 *: L'application :*

$$\begin{array}{rcl} \alpha : \overline{E} & \longrightarrow & Pic^0(\overline{E}) \\ P & \longmapsto & [P - O]. \end{array}$$

est une bijection.

Preuve : Soit $D \in Div^0(\overline{E})$ un diviseur de degré O. Par Riemann-Roch et comme $g = 1$, on a :

$$dim(L(D + O)) = 1$$

Soit $f \in L(D + O)$ non nulle. Comme $div(f) \geq -D - O$ et $deg(div(f)) = 0$, on doit avoir :

$$div(f) = -D - O + P$$

pour un certain points P. Donc

$$D \sim P - O$$

A tout diviseur de degré 0 D correspond donc un point $P \in \overline{E}$ tel que $D \sim P - O$. Si $D \sim D'$ et $D \sim P - O$ et $D' \sim P' - O$ alors $P \sim P'$ et donc $P = P'$. A deux diviseurs équivalents correspond donc le même point P et donc $\forall [D] \in Pic^0(\overline{E})$, il existe $P \in \overline{E}/\alpha(P) = [D]$. Ceci montre que α est surjective. Supposons $\alpha(P) = \alpha(Q)$, donc $P - O \sim Q - O$ et $P \sim Q$ et donc $P = Q$. Ceci montre que α est injective.
Comme $Pic(\overline{E})$ est un groupe (abélien), cette bijection permet de définir une loi de groupe sur $\overline{E}(\overline{K})$ en utilisant celle de $Pic^0(\overline{E})$. On a donc deux lois sur $\overline{E}(\overline{K})$. Celle définie plus haut et celle provenant de $Pic^0(\overline{E})$.

Proposition 2.2.4 *: Ces deux lois sont les mêmes.*

Preuve : Il suffit montrer que :

$$\alpha(P \oplus Q) = \alpha(P) + \alpha(Q)$$

avec $\oplus$ l'addition dans $\overline{E}(\overline{K})$ définie plus haut et $+$ l'addition dans $Pic^0(\overline{E})$. Soit D la droite passant par P,Q,R. Si f est l'équation de D, on a :

$$div(\frac{f}{z}) = P + Q + R - 3O$$

De même soit D' la droite passant par R,O et $P \oplus Q$. Si g est l'équation de D', on a :

$$\begin{aligned} div(\frac{g}{z}) &= R + (P \oplus Q) + O - 3O \\ &= R + (P \oplus Q) - 2. \end{aligned}$$

Donc $div(\frac{f}{g}) = (P \oplus Q) - P - Q + O \sim O$ et $(P \oplus Q) - O \sim (P - O) + (Q - O)$. *i.e* $\alpha(P \oplus Q) = \alpha(P) + \alpha(Q)$. La seconde loi, notons la $\oplus_2$, est définie par :

$$P \oplus_2 Q = \alpha^{-1}(\alpha(P) + \alpha(Q))$$

Donc :

$$\begin{aligned} P \oplus_2 Q &= \alpha^{-1}(\alpha(P) + \alpha(Q)). \\ &= \alpha^{-1}(\alpha(P \oplus Q)). \\ &= (P \oplus Q). \end{aligned}$$

et les deux lois sont les mêmes.

Corollaire 2.2.2 *: $\oplus$ est associative.*

Preuve : $\oplus$ est égale à $\oplus_2$ qui provient de l'addition dans $Pic^0(\overline{E})$ qui est associative de façon naturelle. Donc $\oplus_2$ et $\oplus$ sont aussi associatives.

Exemple 2.2.1 *:*

1. *Soit la courbe elliptique d'équation affine $Y^2 = X^3 + 2X + 1$. Elle est définie par exemple sur le corps $K = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Les éléments de $\mathbb{F}_5$ sont les congruences modulo 5. On reconnait immédiatement les deux points $P_1 = (1, 2)$ et $P_2 = (3, 2)$ qui sont rationnels sur $\mathbb{F}_5$. En effet, on a :*

$$1^3 + 2.1 + 1 = 4 = 2^2 \qquad \text{mod } 5$$

et :

$$3^3 + 2.3 + 1 = 34 = 4 = 2^2 \qquad \text{mod } 5$$

En appliquant les formules précédentes :

$$m \equiv \frac{2-2}{3-2} \equiv 0 \text{ mod } 5$$

et donc si $P_3 = (x_3, y_3) = P_1 \oplus P_2$, on a :

$$\begin{aligned} x_3 &= -1 - 3 \equiv -4 \equiv \textit{1 mod 5} \\ y_3 &= -2 \equiv \textit{3 mod 5.} \end{aligned}$$

i.e $P_3 = P_1 \oplus P_2 = (1, 3)$. C'est aussi un point rationnel de la courbe sur $\mathbb{F}_5$.

2. *Considérons le même courbe sur le même corps. Soit $P = (1, 3)$ (le P_3 du 1). Nous voulons calculer $P \oplus P = 2P$. Si $P = (x_1, y_1)$, on a :*

$$m = \frac{3x_1^2 + A}{2y_1}$$

Donc :

$$m = \frac{3.1 + 2}{2.3} = \frac{5}{6} \equiv 5.6 \equiv \textit{0 mod 5}$$

et donc $m = 0$ dans $\mathbb{F}_5$. Si $P \oplus P = (x, y)$ on a :

$$\begin{aligned} x &= -1 - 1 \equiv -2 \equiv \textit{3 mod 5} \\ y &= -3 \equiv \textit{2 mod 5} \end{aligned}$$

donc $P \oplus P = 2P = (3, 2)$ ie $(1, 3) + (1, 3) = (3, 2)$

Dans cet exemple on a utilisé la notation :

$$\begin{cases} P \oplus \ldots \oplus P & = & nP & \text{pour n} > 0 \\ \ominus P \oplus \ldots \oplus \ominus P & = & nP & \text{pour n} < 0 \end{cases}$$

Dans la suite on écrira + pour $\oplus$ et donc la notation devient :

$$\begin{cases} P + \ldots + P & = & nP & n > 0 \\ -P - \ldots - P & = & nP & n < 0 \end{cases}$$

2.3 Endomorphismes et Points de Torsion

Soit $\overline{E}$ une courbe elliptique définie sur le corps K.

Définition 2.3.1 *: Un endomorphisme de $\overline{E}$ est une application rationnelle $\phi : \overline{E} \longrightarrow \overline{E}$ qui est aussi un morphisme de groupes $\overline{E}(\overline{K}) \longrightarrow \overline{E}(\overline{K})$.*

Morphisme de groupes veut dire que :

- $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$.
- $\phi(0) = 0$.

et comme ϕ est une application rationnelle elle s'écrit (en coordonnées affines) :

$$\phi(P) = \phi(x, y) = (R_1(x, y), R_2(x, y))$$

avec R_1 et R_2 des fonctions rationnelles sur $\overline{E}$ (*i.e* quotient de polynômes).

Exemple 2.3.1 *:*

1. *L'endomorphisme nul est :*

$$\begin{array}{rccc} \phi : \overline{E} & \longrightarrow & \overline{E} \\ P & \longmapsto & O. \end{array}$$

   i.e : $\phi(P) = O$, $\forall P \in \overline{E}(\overline{K})$.

2. *Si l'equation affine de $\overline{E}$ est $Y^2 = X^3 + AX + B$, alors :*

$$\begin{array}{rccc} \phi : \overline{E} & \longrightarrow & \overline{E} \\ P & \longmapsto & 2P. \end{array}$$

est un morphisme de $\overline{E}$. Il est clair que ϕ est un morphisme de groupes. De plus un calcul facile utilisant les formules vues précédemment donne :

$$\phi(P) = \phi(x, y) = (R_1(x, y), R_2(x, y))$$

avec

$$R_1(x, y) = (\frac{3x^2 + A}{2y})^2 - 2x$$

$$R_2(x, y) = (\frac{3x^2 + A}{2y})(3x - (\frac{3x^2 + A}{2y})^2) - y$$

qui sont des fonctions rationnelles.

3. *Plus généralement les morphismes :*

$$\begin{array}{rccc} [m] : \overline{E} & \longrightarrow & \overline{E} \\ P & \longmapsto & mP. \end{array}$$

sont des endomorphismes de $\overline{E}$, pour $m \in \mathbb{Z}$. Si $\overline{E}$ est défini sur K, tous ces endomorphismes sont aussi définis sur K.

Comme les courbes elliptiques sont non singulières, on peut remplacer application rationnelle par morphisme (entre courbes). De plus tout morphisme non constant est nécessairement surjectif (voir chapitre 1).

Définition 2.3.2 *Le sous-groupe des points de $m-torsion$ est l'ensemble des points de $\overline{E}$ d'ordre m :*

$$\overline{E}[m] = \{P \in \overline{E}(\overline{K})/mP = O\}$$

$$= Ker[m].$$

Le sous groupe de torsion de $\overline{E}$ est :

$$\overline{E}_{tors} = \bigcup_{m=1}^{\infty} E[m]$$

Si $\overline{E}$ est définie sur K, on pose :

$$\overline{E}_K[m] = \{P \in \overline{E}(K)/mP = 0\}.$$

et

$$\overline{E}_{tors}(K) = \bigcup_{m} E_K[m]$$

Proposition 2.3.1 *: Soit $m \in \mathbb{Z}$ avec $m \neq 0$. Alors $[m] \neq [0]$ et $\overline{E}[m]$ est fini. Si $[m] = (R_{1m}, R_{2m})$ avec R_{1m} et R_{2m} des fonctions rationnelles, alors R_{1m} et R_{2m} ont des pôles exactement en les éléments de $E[m]$.*

Preuve : Remarquons d'abord que si $[m] \neq [0]$ alors $\overline{E}[m] < \infty$. En effet si $[m] = [0]$ alors $\overline{E}[m] = Ker[m] = \overline{E}(\overline{K})$ qui est infini . Si $[m] = (R_{1m}, R_{2m}) \neq [0]$, alors $[m]P = mP = 0$ veut dire que R_{1m} et R_{2m} ont un pôle en P. Comme une fonction rationnelle n'a qu'un nombre fini de pôles, on doit avoir que $\#E[m] < \infty$. Enfin pour $[m] \neq [0]$ si $m \neq 0$, nous renvoyons à [15].
Pour $m = 1$, on a $R_{11} = X$ et $R_{21} = Y$. Remarquer que si $m \neq n$, alors $[m] \neq [n]$(en effet on aurait sinon $[m-n] = [0]$ et donc $m - n = 0$). On peut donc calculer les R_{1m} et R_{2m} par récurrence sur m. Pour obtenir R_{11} et R_{22}, on utilise la formule $[2] = [1] + [1]$:

$$\begin{aligned} R_{12} &= -2X + \Lambda^2 \quad (= -X - X + \lambda^2) \\ R_{22} &= -\lambda(R_{12} - X) - Y \end{aligned}$$

avec :

$$\lambda = \frac{3X^2 + A}{2Y}$$

Si $m < 2$, alors $[m-1] \neq [1]$ et on utilise la formule $[m] = [m-1] + [1]$:

$$R_{1m} = -R_{1(m-1)} - X + \lambda^2$$

$$R_{2m} = -\lambda(R_{1m} - X) - Y$$

avec :

$$\lambda = \quad \frac{R_{2(m-1)} - Y}{R_{1(m-1)} - X}$$

On peut encore simplifier l'écriture d'un endomorphisme $\phi : \overline{E} \longrightarrow \overline{E}$ en utilisant l'équation de la courbe. Comme les points de la courbe $P = (x, y) \in \overline{E}(\overline{K})$ vérifient $y^2 = x^3 + Ax + B$, on peut remplacer toute puissance paire de y par un polynôme en x et toute puissance impaire par y fois un polynôme en x. Si :

$$\phi(P) = \phi(x, y) = (R_1(x, y), R_2(x, y)),$$

on peut donc écrire :

$$R_1(x, y) = \frac{P_1(x) + P_2(x)y}{P_3(x) + P_4(x)y}$$

et de même pour R_2. En multipliant R_1 par $P_1 - P_4 y$ et remplaçant y^2 par $x^3 + Ax + B$, on peut encore écrire :

$$R_1(x,y) = \frac{Q_1(x) + Q_2(x)y}{Q_3(x)}; R_2 = \frac{Q_1^{'} + Q_2^{'}y}{Q_3^{'}}$$

et de même pour R_2. Comme ϕ est un endomorphisme, on a :

$$\phi(x,-y) = \phi(-(x,y)) = -\phi(x,y)$$

et donc R_1 et R_2 vérifient :

$$R_1(x,-y) = R_1(x,y) \quad et \quad R_2(x,-y) = -R_2(x,y)$$

ce qui donne $\phi_2(x) = 0$ et $\phi_1^{'}(x) = 0$. On a donc montré :

Proposition 2.3.2 *: Tout endomorphisme $\phi : \overline{E} \longrightarrow \overline{E}$ peut s'écrire :*

$$\phi(x,y) = (f_1(x), y f_2(x)).$$

avec $f_1(x) = \frac{P(x)}{Q(x)}$ et $f_2(x) = \frac{P^{'}(x)}{Q^{'}(x)}$ deux fonctions rationnelles.

Définition 2.3.3 *: Soit $\phi : \overline{E} \longrightarrow \overline{E}$ un endomorphisme et écrivons $\phi(x,y) = (f_1(x), y f_2(x))$, avec $f_1(x) = \frac{P(x)}{Q(x)}$ et $pgcd(P,Q) = 1$. Alors le degré de ϕ est :*

$$deg(\phi) = max\{deg(P(x)), deg(Q(x))\}$$

(et $deg(0) = 0$ pour $\phi = 0$ l'endomorphisme nul). $\phi \neq 0$ est dit séparable si la dérivée de f_1 n'est pas identiquement nulle : $f_1^{'} \neq 0$.

Exemple 2.3.2 *: Reprenons l'exemple de l'endomorphisme [2] :*

$$\begin{array}{rccc} [2] : & \overline{E} & \longrightarrow & \overline{E} \\ & P & \longmapsto & 2P. \end{array}$$

On a vu que $R_1(x,y) = (\frac{3x^2+A}{2y} - 2x)$. Aprés des calculs faciles, on obtient :

$$f_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

donc $deg[2] = 4$. *Pour ce qui est de la séparabilité remarquons que si* $f_1(x) = \frac{P(x)}{Q(x)}$, *alors* $f_1' \neq 0 \Longleftrightarrow P' \neq 0$ *ou* $Q' \neq 0$. *En effet on a* $f_1' = \frac{P'Q - Q'P}{Q^2}$ *et donc* $f_1' = 0 \Longleftrightarrow P'Q - Q'P = 0$. *Donc toute racine de* P *est racine de* P' *et toute racine de* Q *est racine de* Q'. *Mais ceci est impossible car* $degP' = degP - 1$ *et* $degQ' = degQ - 1$. *Donc* $P' = 0$ *et* $Q' = 0$. *Ici* $Q(x) = 4(x^3 + Ax + B)$ *et* $Q'(x) = 4(3x^2 + A)$ *qui est non nul (car la caractéristique du corps est différente de* $2, 3$*).*

L'interêt des endomorphismes séparables est que l'on dispose d'une formule qui permet de calculer le degré d'un tel endomorphisme en utilisant le noyau de ϕ :

$$deg(\phi) = \#Ker(\phi).$$

avec $Ker(\phi) = \{P \in \overline{E}(\overline{K})/\phi(P) = 0\}$. Pour une démonstration complète nous renvoyons à [15] ainsi qu'an fait que si $m \neq 0$ dans K (*i.e* p ne divise pas m), alors $[m]$ est séparable de degré m^2. De plus $\overline{E}[m]$ est un $\frac{\mathbb{Z}}{m\mathbb{Z}}$-module libre de rang 2 :

$$\overline{E}[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}$$

2.4 Polynômes de Division

Soit $\overline{E}$ une courbe elliptique définie sur $\mathbb{F}_q$ d'équation de Weierstrass $Y^2 = X^3 + AX + B$. Les polynômes de division associés à cette courbe sont certains polyômes dans $\mathbb{F}_p[X, Y]$ qui ont un lien avec les points de torsion de la courbe et qui permettent de calculer les multiples nP d'un point P de la courbe .

Définition 2.4.1 *: Les polyômes de division* $\psi_n(X, Y)$ *sont des éléments de* $\mathbb{F}_p[X, Y]$ *définis inductivement par :*

$$\begin{aligned}
\psi_{-1} &= -1 \\
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2Y \\
\psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2 \\
\psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3) \\
&\vdots \\
\psi_{2n} &= (\tfrac{\psi_n}{2Y})(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \quad n > 0 \\
\psi_{2n+1} &= (\psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}) \quad n > 0
\end{aligned}$$

Proposition 2.4.1 *: $P = (x, y) \in \overline{E}[n] \Leftrightarrow \psi_n(x, y) = 0$.*

Preuve : Nous démontrons cette proposition en traitant, par exemple le cas $n = 3$. Le même argument est valable pour les autres n. Soit $P = (x, y) \in E[3]$. Donc $3P = 0$ *i.e* $2P = -P$. La première coordonneé de $2P$ doit être égale à la première coordonneé de $-P$ qui est x. Donc

$$x = \frac{(3x^2 + A)^2}{4y^2} - 2x$$

i.e

$$(+3x)(4y^2) = 9x^4 + 6Ax^2 + A^2$$

En utilisant $y^2 = x^3 + Ax + B$ on a :

$$12(x^4 + Ax^2 + Bx) = 9x^4 + 6Ax^2 + A^2$$

et donc

$$\underbrace{3x^4 + 6Ax^2 + 12Bx - A^2}_{\psi_3} = 0$$

Inversement si $\psi_3(x, y) = 0$, alors $2P = \pm P$ et donc $P = 0$ ou $3P = 0$ *i.e* $P \in E[3]$. (Remarquer que ψ_3 est un polynôme en x seul).
En général les polynômes de division ψ_n sont des polynômes en X, Y mais en utilisant l'équation de la courbe on montre (par exemple par récurrence sur n) que $\psi_n \in \mathbb{F}_p[X]$ est un polynôme en X seul si n est impair et $\psi_n \in Y\mathbb{F}_p[X]$ si n est pair.
Les polynômes de division permettent aussi de calculer les multiples nP d'un point :

Proposition 2.4.2 *On a*

$$nP = (x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{2n}}{2\psi_n^4})$$

$$= (x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3})$$

Preuve : voir [6]

Chapitre 3

Courbes Elliptiques sur un Corps Fini

Si $K = \mathbb{F}_q$ est un corps fini, le groupe des points rationnels d'une courbe elliptique sur K est fini et devient un analogue du groupe $\mathbb{F}_q$ pour les applications en cryptographie par exemple. Il est donc nécessaire de connaitre son ordre $i.e$ le nombre de ses éléments. Pour des corps finis pas trop larges, on peut calculer ce nombre directement en essayant toutes les valeurs dans le corps et voir quelles sont celles qui vérifient l'équation de Weierstrass. Pour des corps plus larges, cela n'est plus possible et il faut utiliser d'autres méthodes. Le théorème de Hasse, qu'on présente dans ce chapitre, permet de donner une première estimation du nombre de points. Cette estimation sera utilisée par Schoof pour déterminer l'ordre exactement. On ne peut donc sous-estimer l'importance de ce théorème dont la démonstration est basée sur les propriéttés de l'endomorphisme de Frobenius sur la courbe elliptique et qui étend le Frobenius sur le corps fini. A la fin du chapitre nous donnons quelques exemples d'application du théorème de Hasse. Pour tout ce qui concerne les corps finis, nous renvoyons le lecteur à notre mémoire de Licence [11] ou encore à [9].

3.1 Cas d'un corps fini

Soit $\mathbb{F}_q$ le corps fini à q éléments et soit $\overline{\mathbb{F}}_q$ sa clôture algébrique. On sait que $q = p^r$ avec p un nombre premier (p est donc la caractéristique de $\mathbb{F}_q$ et

on supposera comme convenu que $p \neq 2, 3$). Si $\mathbb{F}_p$ est le corps premier :

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$$

$\mathbb{F}_q$ est une extension algébrique de $\mathbb{F}_p$ de degré r (*i.e* que $\mathbb{F}_q$ est un $\mathbb{F}_p$-espace vectoriel de dimension r). Soit $\overline{E}$ une courbe elliptique définie sur le corps $\mathbb{F}_q$ donnée par l'équation de Weierstrass :

$$Y^2 = X^3 + AX + B$$

avec $A, B \in \mathbb{F}_q$. (Remarquer que le point à l'infini $O = (0, 1, 0)$ est rationnel sur $\mathbb{F}_q$). Soit $\overline{E}(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 / y^2 = x^3 + Ax + B\} \cup \{O\}$, le groupe des points rationnels de la courbe sur $\mathbb{F}_q$ (c'est un groupe abélien d'aprés les résultats du chapitre 2).

Proposition 3.1.1 *: $\overline{E}(\mathbb{F}_q)$ est un groupe fini i.e que $\#\overline{E}(\mathbb{F}_q) < \infty$.*

Preuve : Comme $\mathbb{F}_q$ est un corps fini, il n y a qu'un nombre fini de possibilités pour les couples (x, y) qui vérifient $y^2 = x^3 + Ax + B$ dans $\mathbb{F}_q$ et donc $\#\overline{E}(\mathbb{F}_q) < \infty$.
D'aprés ce résultat, tous les points de $\overline{E}(\mathbb{F}_q)$ sont des points de torsion *i.e* que $\forall P \in \overline{E}(\mathbb{F}_q)$, il existe $m \in \mathbb{N}$ tel que :

$$mP = O$$

En effet l'ordre du groupe $\overline{E}(\mathbb{F}_q)$ est fini et l'ordre de tout point (*i.e* du sous-groupe engendré par le point) divise l'ordre du groupe.
Le nombre maximum des $x \in \mathbb{F}_q$ vérifiant $y^2 = x^3 + Ax + B$ est q et pour chaque x, il y a possibilité de deux valeurs pour y. Donc le nombre maximum de points de $\overline{E}$ sur $\mathbb{F}_q$ est $2q + 1$. L'équation quadratique $y^2 = x^3 + Ax + B$ a 50% de chance d'avoir une solution en y pour un x donné et on peut donc estimer le nombre de points à $\#\overline{E}(\mathbb{F}_q) = q + 1$. (On rajoute le 1 pour le point à l'infini).

Exemple 3.1.1 *:*

1. *Prenons $q = p = 7$ et soit la courbe elliptique $\overline{E}$ d'équation de Weierstrass $Y^2 = X^3 + X + 1$. $\overline{E}$ est définie sur $\mathbb{F}_7$ (remarquer que $\overline{E}$ est non singulière). On peut calculer $\#E(\mathbb{F}_7)$ en déterminant tous les points rationnels grâce an tableau suivant :*

x	x^3+x+1	y
0	1	± 1
1	3	
2	4	± 2
3	3	
4	6	
5	5	
6	6	

Les carrés y^2 dans $\mathbb{F}_7$ sont 0 *(pour* $y = 0$*)* ; 1 *(pour* $y = 1$ *ou* $y = -1 = 6$*)* ; 2 *(pour* $y = 3 =$ *ou* $y = -3 = 4$*) et* 4 *(pour* $y = 2$ *ou* $y = -2 = 5$*). Donc* $\overline{E}(\mathbb{F}_7) = \{(0,1),(0,6),(2,2),(2,5)\} \cup \{O\}$ *et* $\#\overline{E}(\mathbb{F}_7) = 5$.

2. *La même courbe peut être définie sur* $\mathbb{F}_5$ $(q = p = 5)$ *et un tableau analogue donne* $\overline{E}(\mathbb{F}_5) = \{(0,1),(0,4),(2,1),(2,4),(2,4),(3,1),(3,4),(4,2),(4,3)\} \cup \{O\}$ *et donc* $\#\overline{E}(\mathbb{F}_5) = 9$.

3.2 L'endomorphisme de Frobenius

Soit le morphisme de Frobenius sur la clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

$$\begin{array}{rcl} \phi_q : \overline{\mathbb{F}}_q & \longrightarrow & \overline{\mathbb{F}}_q \\ x & \longmapsto & x^q \end{array}$$

ϕ_q est en fait un automorphisme de $\overline{\mathbb{F}}_q$:

$$\phi_q(x+y) = \phi_q(x) + \phi_q(y)$$

et on a :

$$\phi_q(x) = x \Leftrightarrow x \in \mathbb{F}_q \quad (x^q = x \Leftrightarrow x \in \mathbb{F}_q)$$

Si $\overline{E}$ est une courbe elliptique définie sur $\mathbb{F}_q$, ϕ_q opère sur les coordonnés (x, y) de tout point $P \in \overline{E}(\overline{\mathbb{F}}_q)$ et ceci définit une application, qu'on notera aussi ϕ_q :

$$\begin{array}{rcl} \phi_q : \overline{E}(\overline{\mathbb{F}}_q) & \longrightarrow & \overline{E}(\overline{\mathbb{F}}_q) \\ (x,y) & \longmapsto & (\phi_q(x), \phi_q(y)) \\ O & \longmapsto & O \end{array}$$

Ici il faut s'assurer que si $P = (x, y) \in \overline{E}(\overline{\mathbb{F}}_q)$, alors $\phi_q(P) = (x^q, y^q) \in$ aussi à $\overline{E}(\overline{\mathbb{F}}_q)$. Soit $Y^2 = X^3 + AX + B$ l'équation de $\overline{E}$ avec $A, B \in \overline{\mathbb{F}}_q$. Soit

$P = (x, y) \in \overline{E}(\overline{\mathbb{F}}_q)$. Donc $y^2 = x^3 + Ax + B$. En utilisant $(x + y)^q = x^q + y^q$ et $x^q = x$ si $x \in \mathbb{F}_q$, ou obtient en prenant les puissances q^{iemes} :

$$\begin{aligned} (y^2)^q &= (x^3 + Ax + B)^q \\ (y^2)^q &= (x^3)^q + A^q x^q + (B)^q \\ (y^2)^q &= (x^q)^3 + Ax^q + B \end{aligned}$$

et donc $(x^q, y^q) = \phi_q(P) \in \overline{E}(\overline{\mathbb{F}}_q)$. Remarquons aussi que $P = (x, y) \in \overline{E}(\mathbb{F}_q)$ si et seulement si $\phi_q(P) = P$.

Proposition 3.2.1 *: ϕ_q est un endomorphisme de $\overline{E}$*

Preuve : On a $\phi_q(x, y) = (x^q, y^q)$ et donc ϕ_q est donnée par des fonctions rationnelles (en fait des polynômes, ce qui est encore mieux). Donc ϕ_q est un morphisme de la courbe $\overline{E}$ vers $\overline{E}$. Il nous reste donc à montrer que c'est un morphisme de groupes (de $\overline{E}(\overline{\mathbb{F}}_q)$ vers $\overline{E}(\overline{\mathbb{F}}_q)$). Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $\overline{E}(\overline{\mathbb{F}}_q)$. Il faut montrer que :

$$\phi_q(P_1 + P_2) = \phi_q(P_1) + \phi_q(P_2)$$

Soit $P_3 = (x_3, y_3) = P_1 + P_2$. On a, si $x_1 \neq x_2$:

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

avec

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

En prenant les puissances q^{iemes} :

$$\begin{aligned} x_3^q &= m'^2 - x_1^q - x_2^q \\ y_3^q &= m'(x_1^q - x_3^q) - y_1^q \end{aligned}$$

avec

$$m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}$$

et donc

$$\begin{aligned} \phi_q(x_3, y_3) &= (x_3^q, y_3^q) \\ &= \phi_q(x_1, y_1) + \phi_q(x_2, y_2) \end{aligned}$$

On traite de la même façon les cas $x_1 = x_2$, P_1 ou $P_2 = O$ et $P_1 = P_2$.
On a donc montré que ϕ_q est une application rationnelle (en fait un morphisme) et que c'est aussi un morphisme de groupes. Donc c'est un endomorphisme de la courbe elliptique $\overline{E}$.

Proposition 3.2.2 *: $deg(\phi_q) = q$ et ϕ_q n'est pas séparable.*

Preuve : On a $\phi_q(x, y) = (f_1(x), y^q)$ avec $f_1(x) = x^q$ et donc $deg(\phi_q) = q$. De plus $f_1^{'}(x) = qx^{q-1} = 0$ et $f_1^{'}$ est identiquement nul. Ceci montre que ϕ_{q^n} n'est pas séparable.
Comme ϕ_q est un endomorphisme de $\overline{E}$, il en est même de $\phi_q^2 = \phi_q \circ \phi_q$ et plus généralement de $\phi_q^n = \underbrace{\phi_q \circ \ldots \circ \phi_q}_{n fois}$ pour $n \geq 1$. Comme $[-1](x, y) = (x, -y)$, la multiplication par -1 est aussi un endomorphisme et donc les $\phi_q^n - 1$ sont des endomorphisme de $\overline{E}$ pour tout $n \geq 1$. Ici on a bien sur :

$$(\phi_q^n - 1)(P) = \phi_q^n(P) - P, \quad \forall P \in \overline{E}(\overline{\mathbb{F}}_q)$$

Proposition 3.2.3 *: On a :*

1. *$Ker(\phi_q^n - 1) = \overline{E}(\mathbb{F}_{q^n})$.*
2. *$\phi_q^n - 1$ est séparable et donc $\#E(\mathbb{F}_{q^n}) = deg(\phi_q^n - 1)$.*

Preuve : Ici $\mathbb{F}_{q^n}$ est l'unique extension de $\mathbb{F}_q$ de degré n (dans $\overline{\mathbb{F}}_q$). Les éléments de $\mathbb{F}_{q^n}$ sont caractérisés par $x \in \mathbb{F}_{q^n} \Leftrightarrow x^{q^n} = x$ et donc $P \in \overline{E}(\mathbb{F}_{q^n}) \Leftrightarrow \phi_q^n(P) = P$. Le fait que $\phi_q^n - 1$ soit séparable se démontre en utilisant la définition de la séparabilité mais est assez technique et nous renvoyons le lecteur à [15] ou [16] pour plus de détails.
Posons :

$$\begin{aligned} a &= q + 1 - \#\overline{E}(\mathbb{F}_q) \\ &= q + 1 - deg(\phi_q - 1). \end{aligned}$$

On a déja donné une première estimation de $\#\overline{E}(\mathbb{F}_q)$:

$$\#\overline{E}(\mathbb{F}_q) \sim q + 1$$

et donc a calcule en quelque sorte l'écart entre $\#\overline{E}(\mathbb{F}_q)$ et $q + 1$. Pour tout entier $m \neq 0$ dans K, on sait que :

$$\overline{E}[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m \quad (\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}})$$

Autrement dit en tant que $\mathbb{Z}_m$-module $\overline{E}[m]$ est libre de rang 2. Si $\{\alpha_1, \alpha_2\}$ est une base de $\overline{E}[m]$, tout autre élément de $\overline{E}[m]$ s'écrit $n_1\alpha_1 + n_2\alpha_2$ ($n_1, n_2 \in \mathbb{Z}_m$ uniques). Si :

$$\phi : \overline{E}(\overline{\mathbb{F}}_q) \longrightarrow \overline{E}(\overline{\mathbb{F}}_q)$$

est un endomorphisme, alors ϕ envoie $\overline{E}[m]$ vers $\overline{E}[m]$ (puisque $\phi(mP) = m\phi(P) = O$ si $mP = O$ et donc $\phi(P) \in \overline{E}[m]$ si $P \in \overline{E}[m]$) et donc induit un morphisme :

$$\phi_m : \overline{E}[m] \longrightarrow \overline{E}[m]$$

qui est représenté dans la base $\{\alpha_1, \alpha_2\}$ par la matrice 2x2 :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

avec $a, b, c, d \in \mathbb{Z}_m$ et :

$$\begin{array}{rcl} \phi_m(\alpha_1) & = & a\alpha_1 + c\alpha_2 \\ \phi_m(\alpha_2) & = & b\alpha_1 + d\alpha_2 \end{array}$$

En utilisant la dualité de Weil [16] sur la courbe elliptique $\overline{E}$, on peut montrer [16] les deux faits suivants que nous utiliserons dans la proposition suivante et dans la preuve du théorème de Hasse.

1. Si ϕ est un endomorphisme non nul de $\overline{E}$, alors on a :

$$det(\phi_m) = deg(\phi) \pmod{m}$$

2. Pour deux endomorphismes ϕ_1 et ϕ_2 et deux entiers a et b on a :

$$deg(a\phi_1 + b\phi_2) = a^2 deg(\phi_1) + b^2 deg(\phi_2) + ab(deg(\phi_1 + \phi_2) - deg(\phi_1) - deg(\phi_2))$$

La proposition suivante permet de regarder a comme la trace de $(\phi_q)_m$:

Proposition 3.2.4 *: On a :*

$$a \equiv Trace((\phi_q)_m) \pmod{m}$$

et a est l'unique entier qui vérifie cette congruence pour tout $m \neq 0$ dans K (i.e que la caractéristique du corps ne divise pas m).

Preuve : $(\phi_q)_m$ est représenté par la matrice 2×2 :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Comme $\phi_q - 1$ est séparable on a :

$$\begin{aligned} \#Ker(\phi_q - 1) &= deg(\phi_q - 1) \\ &\equiv det((\phi_q)_m - I) \pmod{m} \\ &= ad - bc - (a+b) + 1 \pmod{m} \end{aligned}$$

Or $ad-bc = det((\phi_q)_m \equiv deg\phi_q = q \pmod{m}$ et $\#Ker(\phi_q - 1) = q+1-a$, par définition de a. Donc :

$$Trace((\phi_q)_m) = a + d \equiv a \pmod{m}$$

Par le théoreme de Cayley-Hamilton, on a donc :

$$(\phi_q)_m{}^2 - a(\phi_q)_m + qI \equiv 0 \pmod{m}$$

avec :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

la matrice identité (on a utilisé le fait que $a = Trace(\phi_q)_m$ et $q = det(\phi_q)_m$). Si $a^{'}$ est un autre entier qui vérifie :

$$a^{'} \equiv trace(\phi_q)_m$$

pour tout $m \neq 0$ dans K, il doit aussi vérifier l'équation de Cayley-Hamilton :

$$(\phi_q)_m^2 - a^{'}(\phi_q)_m + qI \equiv 0 \pmod{m}$$

donc :

$$(a - a^{'})(\phi_q)_m = ((\phi_q)_m^2 - a(\phi_q)_m) + q) - (\phi_q)_m^2 - a^{'}(\phi_q)_m + q) = 0$$

pour tout $m \neq 0$ dans K. Donc $(a-a^{'})\phi_q = 0$ sur $\overline{E}[m]$ pour tout $m \neq 0$ (dans K.) Cela veut dire que le noyau de $(a-a^{'})\phi_q$ est infini et donc $(a-a^{'})\phi_q = 0$. Comme

$$\phi : \overline{E}(\overline{\mathbb{F}}_q) \longrightarrow \overline{E}(\overline{\mathbb{F}}_q)$$

est surjective, ou en déduit que $a-a^{'}$ tue $\overline{E}(\overline{\mathbb{F}}_q)$ et donc tue aussi $\overline{E}[m]$ pour tout $m \geq 1$ $((a - a^{'})P = 0, \forall P \in \overline{E}(\overline{\mathbb{F}}_q))$. Or dans $\overline{E}[m]$ il ya toujours des points d'ordre m et donc $a - a^{'} \equiv 0 \pmod{m}$ pour tout $m \neq 0$. Cela veut dire que $a = a^{'}$.

Un argument analogue permet aussi de montrer que a est l'unique entier qui vérifie :

$$\phi_q^2 - a\phi_q + qI = 0$$

Le polynôme $X^2 - aX + q$ est le polynôme caractéristique du Frobenius ϕ_q. Par application à un point $P = (x, y) \in \overline{E}(\overline{\mathbb{F}}_q)$, on obtient :

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

puisque $\phi(x, y) = (x^q, y^q)$. Comme $((\phi_q)^2_m) - a(\phi_q)_m + q = 0, \forall m \neq 0$ dans K, le noyau de ${\phi_q}^2 - a\phi_q + q$ contient tous les $\overline{E}[m]$ et est donc infini. On doit donc avoir

$${\phi_q}^2 - a\phi_q + q = 0$$

Pour l'unicité de a, on récopie l'argument précédent.

3.3 Théorème de Hasse

Le théorème de Hasse permet de préciser encore mieux l'estimation :

$$\#\overline{E}(\mathbb{F}_q) \sim q + 1$$

en délimitant $a = q + 1 - \#\overline{E}(\mathbb{F}_q)$. C'est un ingrédient essentiel dans l'algorithme de Schoof.

Théorème 3.3.1 *(Hasse) : Soit $\overline{E}$ une courbe elliptique définie sur $\mathbb{F}_q$. Alors on a :*

$$|q + 1 - \#\overline{E}(\mathbb{F}_q)| \leq 2\sqrt{q}$$

ou encore $|a| \leq 2\sqrt{q}$.

Preuve : On a :

$$\begin{aligned} a &= q + 1 - \#\overline{E}(\mathbb{F}_q) \\ &= q + 1 - deg(\phi_q - 1) \end{aligned}$$

Or on a de manière générale :

$$\begin{aligned} deg(r\phi_q - 1) &= r^2 deg\phi_q + s^2 deg(-1) + rs(deg(\phi_q - 1) - deg\phi_q - deg(-1)) \\ &= r^2 q + s^2 - rsa \end{aligned}$$

Puisque $deg\phi_q = q$ et $deg(-1) = 1$. Comme $deg(r\phi_q - s) \geq 0$, on a

$$r^2 + s^2 - rsa \geq 0$$

et divisant par s^2, on obtient :

$$q(\frac{r}{s})^2 - a(\frac{r}{s}) + 1 \geq 0$$

Comme $\mathbb{Q}$ est dense dans $\mathbb{R}$. on a donc

$$qx^2 + ax + 1 \geq 0, \quad \forall x \in \mathbb{R}.$$

et le discriminant de ce polynôme doit être ≤ 0. On a donc :

$$a^2 - 4q \leq 0.$$

ie

$$|a| \leq 2\sqrt{q}$$

Comme on vient de le voir la preuve du théoreme de Hasse n'est pas trés profonde, mais le résultat en lui même est trés important comme on le verra plus tard. En enlevant la valeur absolue il devient :

$$-2\sqrt{q} \leq a \leq 2\sqrt{q}$$

ou encore

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

Exemple 3.3.1 *:*

1. *Reprenons la courbe* $\overline{E} : Y^2 = X^3 + X + 1$ *sur* $\mathbb{F}_7$*. On a déja calculé* $\#\overline{E}(\mathbb{F}_7) = 5$*. Ici on a* $q = 7$ *et donc* $q + 1 = 8$ *et* $2\sqrt{q} = 2\sqrt{7} \sim 5,29$*. D'autre part* $q + 1 - 2\sqrt{q} = 8 - 5,29 \sim 2,71$ *et* $q + 1 + 2\sqrt{q} \sim 13,29$ *et on a bien :*
$$2,71 \leq 5 \leq 13,29$$

2. *Soit la même courbe sur* $\mathbb{F}_5$*. On a déja calculé* $\#\overline{E}(\mathbb{F}_5) = 9$*. Ici* $q = 5$ *et* $q + 1 = 6$ *et* $2\sqrt{q} = 2\sqrt{5} \sim 4,47$*.* $q + 1 - 2\sqrt{q} \sim 6 - 4,47 \sim 1,53$ *et* $q + 1 + 2\sqrt{q} = 6 + 4,47 \sim 10,47$ *et on a bien :*

$$1,53 \leq 9 \leq 10,47$$

Chapitre 4

L'Algorithme de Schoof

Ce chapitre constitue le coeur de ce travail. En plus de la méthode directe vue dans le chapitre précédent, nous présentons trois autres méthodes pour calculer le nombre de points d'une courbe elliptique sur un corps fini : la méthode de Lang-Trotter [8], celle du Baby Step-Giant Step [4, 1] et l'algorithme de Schoof [13]. Lang et Trotter utilisent une généralisation du symbole de Legendre pour donner une formule simple pour calculer le cardinal des points. Malheureusement cette formule n'est exploitable que pour des corps de taille modeste. La méthode du Baby Step-Giant Step utilise les propriétés de l'ensemble des points en tant que groupe et notamment le théorème de Lagrange et calcule le nombre de points en une succession d'étapes. Elle est valable pour des corps de taille plus grande tout en restant raisonnable. Enfin l'algorithme de Schoof, valable pour des corps finis quelconques, utilise l'équation caractéristique de l'endomorphisme de Frobenius pour calculer le nombre de points à travers plusieurs cas qu'on peut ramener à des calculs simples de *pgcd*. Nous illustrons toutes ces méthodes tout le long du chapitre avec quelques exemples en nous aidant notamment du logiciel PARI [12]

4.1 Méthode de Lang-Trotter

Cette méthode de calcul de $\#\overline{E}(\mathbb{F}_q)$ est basée sur une généralisation du symbole de Legendre. Si p est un nombre premier impair , le symbole de

Legendre (modulo p) est :

$$(\frac{a}{p}) = \begin{cases} +1 & si \quad x^2 \equiv \text{a (mod p) a une solution} \\ -1 & si \quad x^2 \equiv \text{a (mod p) n'a pas de solution} \\ 0 & si \quad a = 0 \end{cases}$$

et est défini pour tout entier $a \in \mathbb{Z}$. En d'autres termes on a :

$$(\frac{a}{p}) = (\#\text{de solutions de } x^2 \equiv a) - 1$$

(En effet si l'équation $x^2 \equiv a \pmod{p}$ a une solution , elle va en avoir exactement 2 et $(\frac{a}{p}) = 2 - 1 = 1$. Si l'équation n'a pas de solutions , alors $(\frac{a}{p}) = 0 - 1 = -1$ et si $a = 0$, l'équation a une solution double $x = 0$ et donc $(\frac{a}{p}) = 1 - 1 = 0$). La congruence $x^2 \equiv a \pmod{p}$ peut être vue comme une équation $x^2 = a$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$ et on peut réecrire le symbole de Legendre :

$$(\frac{a}{p}) = (\frac{a}{\mathbb{F}_p})$$

Ceci admet une généralisation quand $\mathbb{F}_p$ est remplacé par $\mathbb{F}_q$ avec $q = p^n$.

Définition 4.1.1 *: Soit $q = p^n$. Le symbole de Legendre généralisé est :*

$$(\frac{a}{\mathbb{F}_q}) = \begin{cases} +1 & si \quad x^2 = a \text{ a une solution dans } \mathbb{F}_q \\ -1 & si \quad x^2 = a \text{ n'a pas de solution dans } \mathbb{F}_q \\ 0 & si \quad a = 0 \end{cases}$$

avec $a \in \mathbb{F}_q$.

Proposition 4.1.1 *: On a $(\frac{a}{\mathbb{F}_q}) = a^{\frac{q-1}{2}}$.*

Preuve : La proposition est vraie si $a = 0$. Supposons $a \neq 0$. On sait que $\mathbb{F}_q^*$ est cyclique d'ordre $q - 1$. Donc on a :

$$a^{q-1} = 1, \quad \forall a \in \mathbb{F}_q^*$$

on encore puisque $q - 1$ est pair :

$$(a^{\frac{q-1}{2}})^2 = 1 \quad \forall a \in \mathbb{F}_q^*$$

Donc

$$a^{\frac{q-1}{2}} = \pm 1 \quad dans \quad \mathbb{F}_q^*$$

Soit y un générateur de $\mathbb{F}_q^*$ (une racine primitive $(q-1)^{eme}$ de l'unité). Si l'équation $x^2 = a$ a une solution b , cette solution s'écrit $b = y^r$ pour un entier r entre 1 et $q-1$. Donc

$$a = (y^r)^2 = y^{2r}$$

et

$$a^{\frac{q-1}{2}} = \xi^{r(q-1)} = (\xi^{q-1})^r = 1 \quad dans \quad \mathbb{F}_q^*$$

Inversement supposons $a^{\frac{q-1}{2}} = 1$. Si $a = y^k$. On a :

$$y^{k\frac{q-1}{2}} = 1$$

et donc $q-1$ divise $k\frac{q-1}{2}$. Ceci montre que k est un entier pair. On peut donc écrire :

$$a = (y^{\frac{k}{2}})^2 = x^2$$

avec $x = y^{\frac{k}{2}}$ et donc $(\frac{a}{\mathbb{F}_q}) = 1$. On a donc montré que $(\frac{a}{\mathbb{F}_q}) = 1 \Leftrightarrow a^{\frac{q-1}{2}} = 1$. Ceci démontre la proposition.
L'idée de Lang et Trotter est d'utiliser ce symbole pour un calcul élémentaire du nombre de points d'une courbe elliptique . Si l'équation de Weierstrass sur $\mathbb{F}_q$ de $\overline{E}$ est $Y^2 = X^3 + AX + B$, on calcule $x^3 + Ax + B$ pour tout $x \in \mathbb{F}_q$ et on cherche ensuite les racines carrées y de $x^3 + Ax + B$ si elles existent. Cette existence est testée avec le symbole de Legendre $(\frac{x^3+Ax+B}{\mathbb{F}_q})$. plus exactement on a le :

Théorème 4.1.1 *(Lang et Trotter)[8] : Soit $\overline{E}$ une courbe elliptique sur $\mathbb{F}_q$ d'équation de Weierstrass $Y^2 = X^3 + AX + B$. Alors on a :*

$$\#\overline{E}(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} (\frac{x^3 + Ax + B}{\mathbb{F}_q})$$

Preuve : Si $x_0^3 + Ax_0 + B$ est une carré dans $\mathbb{F}_q$ il ya deux points de la courbe sur $\mathbb{F}_q$: (x_0, y) et $(x_0, -y)$ pour y une racine careé de $x_0^3 + Ax_0 + B$. Si $x_0^3 + Ax_0 + B = 0$, il ya un seul point $(x_0, 0)$ et si $x_0^3 + Ax_0 + B$ n'est pas un carré il n y a aucun point. En rajoutant le point à l'infini, on a donc :

$$\begin{aligned} \#\overline{E}(\mathbb{F}_q) &= 1 + \textstyle\sum_{x \in \mathbb{F}_q} (1 + (\frac{x^3+Ax+B}{\mathbb{F}_q})) \\ &= q + 1 + \textstyle\sum_{x \in \mathbb{F}_q} (\frac{x^3+Ax+B}{\mathbb{F}_q}) \end{aligned}$$

Pour calculer les symboles de Legendre, on utilise la proposition 4.1.1 ou alors ou peut calculer tous les carrés dans $\mathbb{F}_q$ et en faire une liste. Supposons, pour simplifier que $q = p$. On prépare un vecteur ayant p entrées, une entrée pour chaque élément de $\mathbb{F}_q$ et toutes les entrées valant -1

$$\begin{pmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix}$$

Pour $1 \leq j \leq p-1$, on élève j au carré et on calcule $j^2 \equiv k \pmod{p}$. On remplace la k^{ieme} entreé par $+1$ et l'entrée 0 par 0. Le vecteur obtenu est le vecteur des valeurs du symbole de Legendre.

Exemple 4.1.1 *:*

1. *Soit la courbe $\overline{E}$ d'équation $Y^2 = X^3 + X + 1$ sur $\mathbb{F}_5$. On sait déja que $\#\overline{E}(\mathbb{F}_5) = 9$. Pour $x = 0, 1, 2, 3$ et 4, $x^3 + x + 1$ vaut respectivement $1, 3, 1, 1$ et 4. On a donc*

$$\#E(\mathbb{F}_5) = 5 + 1 + (\frac{1}{5}) + (\frac{3}{5}) + (\frac{1}{5}) + (\frac{1}{5}) + (\frac{4}{5})$$

pour calculer les symboles de Legendre, on utilise l'égalite $(\frac{a}{\mathbb{F}_5}) = a^{\frac{5-1}{2}} = a^2$. Ce qui donne ici $(\frac{1}{5}) = 1^2 = 1$, $(\frac{3}{5}) = 3 = 9 = -1$ et $(\frac{4}{5}) = 4^2 = 16 = 1$ et donc :

$$\#E(\mathbb{F}_5) = 6 + 1 - 1 + 1 + 1 + 1 = 9$$

Les carrés dans $\mathbb{F}_5$ sont $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 = 4$, et $4^2 = 1$. Le vecteur des valeurs du symbole de Legendre initial est :

$$\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \end{pmatrix}$$

et le vecteur final est :

$$\begin{pmatrix} 0 \\ +1 \\ -1 \\ -1 \\ -1 \end{pmatrix}$$

et donc $(\frac{0}{5}) = 0, (\frac{1}{5}) = +1, (\frac{2}{5}) = -1, (\frac{3}{5}) = -1$ *et* $(\frac{4}{5}) = +1$ *et c'est bien le même résultat.*

2. *Soit la courbe* $\overline{E}$ *d'équation* $Y^2 = X^3 + X + 1$ *sur* $\mathbb{F}_7$ *. On sait déja que* $\#\overline{E}(\mathbb{F}_7) = 5$*. Pour* $x = 0, 1, 2, 3, 4, 5$ *et* 6*,* x^3+x+1 *vaut respectivement* $1, 3, 4, 3, 6, 5$ *et* 6*. On a donc*

$$\#E(\mathbb{F}_7) = 7 + 1 + (\frac{1}{7}) + (\frac{3}{7}) + (\frac{4}{7}) + (\frac{3}{7}) + (\frac{6}{7}) + (\frac{5}{7}) + (\frac{6}{7})$$

Pour calculer les symboles de Legendre, on utilise l'égalite $(\frac{a}{\mathbb{F}_7}) = a^{\frac{7-1}{2}} = a^3$*. Ce qui donne ici* $(\frac{1}{7}) = 1^3 = 1$*,* $(\frac{3}{7}) = 3^3 = 27 = 6 = -1$*,* $(\frac{4}{7}) = 4^3 = 1$*,* $(\frac{6}{7}) = 6^3 = 6 = -1$ *et* $(\frac{5}{7}) = 5^3 = 6 = -1$ *et donc :*

$$\#E(\mathbb{F}_7) = 7 + 1 + 1 - 1 - 1 - 1 - 1 + 1 - 1 = 5$$

Les carrés dans $\mathbb{F}_7$ *sont* $0^2 = 0$*,* $1^2 = 1$*,* $2^2 = 4$*,* $3^2 = 2$*,* $4^2 = 2$*,* $5^2 = 4$ *et* $6^2 = 1$*. Le vecteur des valeurs du symbole de Legendre initial est :*

$$\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \end{pmatrix}$$

et le vecteur final est

$$\begin{pmatrix} 0 \\ +1 \\ +1 \\ -1 \\ +1 \\ -1 \\ -1 \end{pmatrix}$$

On remarque qu'on a le même résultat.

4.2 Baby Step - Giant Step

Par le théorème de Hasse on sait que $N = \#\overline{E}(\mathbb{F}_q)$ vérifie :

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$$

Une autre méthode pour trouver $\#\overline{E}(\mathbb{F}_q)$ et de choisir un point quelconque $P \in \overline{E}(\mathbb{F}_q)$ (par exemple en choisissant $x \in \mathbb{F}_q$ de telle sorte que $x^3 + Ax + B$ soit un carré et de trouver un entier m dans l'intervalle $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ tel que $mP = 0$. Alors on est sûr que $\#\overline{E}(\mathbb{F}_q) = m$. En effet on a aussi $NP = 0$ puisque l'ordre du point divise l'ordre du groupe et donc forcement $N = m$. Si m n'est pas le seul entier dans l'intervalle qui vérifie $mP = 0$, on repéte la même procédure avec un autre point Q pour trouver un entier n dans l'intervalle tel que $nQ = 0$ et on essaie de voir si le *ppcm* de m et n divise un seul entier N dans l'intervalle. Sinon on repéte avec un troisième point ... etc . Pour trouver m tel que $mP = 0$, on peut essayer toutes les valeurs dans l'intervalle $[q + 1 - \sqrt{q}, q + 1 + \sqrt{q}]$ (on sait qu 'un tel m existe puisque $NP = 0$ et N est dans l'intervalle), ou alors utiliser la méthode du Baby Step-Giant Step qui est plus rapide. Le point P étant choisi, on calcule $Q = (q + 1)P$ et les points jP avec $j = 0, 1, 2, \ldots, s$ et s un entier $> q^{\frac{1}{4}}$. On calcule ensuite les points $Q + k(2sP)$ pour $k = -s, -(s-1), \ldots, s$ jusqu'à ce qu'on arrive à une égalité :

$$Q + k(2sP) = \pm jP$$

Le fait qu'on puisse toujours trouver une telle egalité se démontre de la manière suivante. Soit $a = q + 1 - \#\overline{E}(\mathbb{F}_q)$. On sait que $|a| \leq 2\sqrt{q} = 2q^{\frac{1}{2}} \leq 2s^2$. Si on pose $a_0 \equiv a \pmod{2s}$ avec $-s < a_0 < s$ et $a_1 = \frac{a-a_0}{2s}$, alors $a = a_0 + 2sa_1$ et $-s \leq a_1 \leq s$ (car $|a_1| \leq \frac{(2s^2+s)}{2s} < s + 1$). Pour $k = -a_1$, on a :

$$\begin{aligned} Q + k(2sP) &= (q + 1 - 2sa_1)P \\ &= (q + 1 - a + a_0)P \\ &= NP + a_0P \\ &= a_0P = \pm jP \end{aligned}$$

On a donc $(q + 1 + 2sk \mp j)P = O$ et on peut prendre :

$$m = q + 1 + 2sk \mp j$$

Si $p_1, \ldots, p_r$ sont les facteurs premiers distincts de m, pour chaque $i = 1, \ldots, r$, on calcule $(\frac{m}{p_i})P$. Si $(\frac{m}{p_i})P = O$, on remplace m par $\frac{m}{p_i}$ et on repéte le processus . Si $(\frac{m}{p_i})P \neq O$, $\forall i$, alors m est l'ordre de P (Si t est l'ordre de P, on sait que t divise m Supposons $t \neq m$ dans ce dernier cas. Soit p un diviseur premier de $\frac{m}{t}$(et donc aussi de m) donc pt divise m et t divise $\frac{m}{p}$. Donc $\frac{m}{p}P = O$, contradiction). Le passage de jP à $(j + 1)P$ constitue

la "Baby Step" et le passage de $k(2sP)$ à $(k+1)(2sP)$ constitue la "Giant Step" , d'ou le nom de "Baby Step-Giant Step". On obtient en définitive l'algorithme suivant pour calculer $\#\overline{E}(\mathbb{F}_q)$:

1. Choisir un entier s avec $s > \sqrt[4]{q}$.
2. Pour $j = 0, ..., s$, calculer jP.
3. $Q \longleftarrow (q+1)P$.
4. Calculer $Q + k(2sP)$, $|k| \leq s$.
5. Jusqu'à ce qu'il existe un j avec $Q + k(2sP) = \pm jP$.
6. $m \longleftarrow q + 1 + 2sk \mp j$ (m vérifie $mP = O$).
7. Factoriser m. Soient $p_1, ..., p_r$ les diviseurs premiers distincts de m.
8. Tant que $i < r$, faire :
   Si $\frac{m}{p_i}P = O$
   alors $m \longleftarrow \frac{m}{p_i}$.
   sinon $i \longleftarrow i + 1$.
   Fin Si.
   Fin Tant que.
9. $n \longleftarrow 1$.
10. $n \longleftarrow ppcm(n, m)$ (m est l'entier obtenu dans l'etape 8. C'est l'ordre de P).
11. Tant que n divise plus d'un entier N dans l'intervalle $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$,
    Choisir un autre point P et aller à l'étape 1.
    Fin Tant que.
12. Retourner N (C'est $\#\overline{E}(\mathbb{F}_q)$).

Exemple 4.2.1 *: Soit la courbe elliptique $\overline{E}$ sur $\mathbb{F}_5$ d'équation de Weierstrass $Y^2 = X^3 + X + 1$. On a déja calculé*

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

et donc

$$\#\overline{E}(\mathbb{F}_5) = 9$$

Voyons si on peut trouver le même résultat en utilisant la méthode du "Baby Step-Giant Step". Ici on a $q = p = 5$ et donc $q^{\frac{1}{4}} = 5^{\frac{1}{4}} = 1.49$. On peut donc prendre $s = 2$. Choisissons le point $P = (0,1)$ et calculons jP pour $j = 0, 1, 2$.

On trouve $0P = O$, $1P = P = (0, 1)$ *et pour calculer* $2P = (x_3, y_3)$, *on utilise les formules de la proposition. On a si* $P = (x_1, y_1) = (0, 1)$

$$m = \frac{3x_1^2 + 1}{2y_1} = \frac{1}{2} = 3$$

et donc

$$x_3 = m^2 - 2x_1 = 4$$

et

$$y_3 = m(x_1 - x_3) - y_1 = 2$$

et donc $2P = (4, 2)$. *Un calcul analogue nous donne* $4P = 2(2P) = (3, 4)$. *Ensuite on doit calculer* $Q = (q + 1)P = 6P$. *Pour cela on utilise l'égalité* $6P = 2P + 4P$. *Si* $6P = (x_3, y_3)$, $2P = (x_1, y_1)$ *et* $4P = (x_2, y_2)$ *on a pour*

$$m = \frac{y_2 - y_1}{x_2 - x_1} = 3$$

$$x_3 = m^2 - x_1 - x_2 = 2$$

et

$$y_3 = m(x_1 - x_3) - y_1 = 4$$

et donc $Q = 6P = (2, 4)$. *L'étape suivante consiste à calculer* $Q + k(2sP)$ *pour* $k = -2, -1, 0, 1, 2$ *jusqu'à ce qu'on trouve une égalité* $Q + k(2sP) = Q + k(4P) = \pm jP$. *En utilisant les formules précédentes, on trouve* $Q + 0(4P) = Q \neq \pm jP$ *pour tout* j *et* $Q + 1(4P) = Q + 4P = (2, 4) + (3, 4) = (0, 1) = P = 1P$. *Donc pour* $k = 1$ *et* $j = 1$, *on a* $Q + k(2sP) = jP$. *On a ainsi*

$$m = 5 + 1 + 2.2.1 - 1 = 9$$

Comme $9 = 3^2$, 9 *n'a qu'un seul facteur premier qui est* 3. *Si* $3P \neq O$ *alors l'ordre du point* P *est* 9, *sinon c'est* 3. *Calculons* $3P$. *On a*

$$3P = P + 2P = (0, 1) + (4, 2) = (2, 1)$$

Donc $3P \neq O$ *et l'ordre de* P *est* $m = 9$. *On sait donc que* 9 *divise* $\#\overline{E}(\mathbb{F}_5)$ *et que celui-ci vérifie*

$$1.53 \leq \#\overline{E}(\mathbb{F}_5) \leq 10.47$$

On a donc $\#\overline{E}(\mathbb{F}_5) = 9$.

Exemple 4.2.2 *: Considérons la même courbe* $Y^2 = X^3 + X + 1$ *mais sur le corps* $\mathbb{F}_7$*. On sait déja que*

$$\overline{E}(\mathbb{F}_7) = \{(0,1),(0,6),(2,2),(2,5)\} \cup \{O\}$$

et donc $\#\overline{E}(\mathbb{F}_7) = 5$*. Comme* $q = p = 7$ *et* $7^{\frac{1}{4}} = 1.62$*, on peut là aussi prendre* $s = 2$*. Choisissons toujours le point* $P = (0,1)$*. On calcule* $0P = O$*,* $1P = P = (0,1)$ *et* $2P = (2,5)$*. On calcule aussi* $4P = 2(2P) = (0,6)$ *et* $Q = 8P = 2(4P) = (2,2)$*. On remarque que* $Q + 4P = 2P$*, donc* $k = 1$ *et* $j = 2$ *et donc*

$$m = 7 + 1 + 2.2.1 - 2 = 10$$

Les diviseurs premiers de 10 *sont* 2 *et* 5*. On teste si* $\frac{10}{5}P = 2P = O$*, ce qui n'est pas le cas puisque* $2P = (2,5) \neq O$*. On laisse donc* m *intact et on passe au diviseur premier suivant qui est* 2*. On a* $\frac{10}{2}P = 5P = 4P + P = (0,6) + (0,1) = (0,-1) + (0,1) = (0,1) - (0,1) = P - P = O$*. On remplace donc* $m = 10$ *par* $m = 5$ *et l'ordre du point* P *est* 5*. On sait ainsi que* 5 *divise* $\#\overline{E}(\mathbb{F}_7)$ *et on a vu que ce dernier vérifie*

$$2.71 \leq \#\overline{E}(\mathbb{F}_7) \leq 13,29$$

Comme 5 *divise deux entiers dans cet intervalle, à savoir* 5 *et* 10*, on doit recommencer le processus avec un autre point, déterminer son ordre et calculer le ppcm des deux ordres. Si ce ppcm divise un seul entier dans l'intervalle, cet entier est le nombre de points, sinon il faut recommencer avec un autre point, etc. Mais ici on peut conclure plus rapidement. En effet on sait que* $\#\overline{E}(\mathbb{F}_7) = 5$ *ou* 10*. Si c'est* 10 *il doit y avoir un point* P *d'ordre* 2 *i.e* $2P = O$ *ou encore* $P = -P$*. Si* $P = (x,y)$*, on doit donc avoir* $y = -y$ *et donc* $2y = 0$ *i.e* $y = 0$*.* x *doit donc vérifier* $x^3 + x + 1 = 0$ *dans* $\mathbb{F}_7$*. Mais un calcul rapide montre qu'un tel* x *n'existe pas et donc il n y a pas de point d'ordre* 2*. On en conclut que* $\#\overline{E}(\mathbb{F}_7) = 5$*.*

4.3 L'Algorithme de Schoof

Pour calculer $\#\overline{E}(\mathbb{F}_q)$ il suffit de calculer $a = q + 1 - \#\overline{E}(\mathbb{F}_q)$. Par le théorème de Hasse on sait que :

$$|a| \leq 2\sqrt{q}$$

Ou encore :

$$-2\sqrt{q} \leq a \leq 2\sqrt{q}$$

C'est à dire que a et contenu dans l'intervalle $[-2\sqrt{q}, 2\sqrt{q}]$ qui est de longueur $4\sqrt{q}$. Pour connaitre a, il suffit donc de le connaitre modulo un entier N qui vérifie :

$$N > 4\sqrt{q}$$

En effet si $a \equiv b \pmod{N}$ avec $b > 0$, alors on aura $a = b$ ou $a = b - N$ et on tranchera en utilisant l'inégalité de Hasse. Si $N = \prod_{i=1}^{k} l_i$ est un produit de nombres premiers distincts et par le théorème des restes chinois, pour connaitre $a \pmod{N}$, il suffit de connaitre $a_i \equiv a \pmod{l_i}$ pour $i = 1, ..., k$. Le problème du calcul de a (et donc de $\#\overline{E}(\mathbb{F}_q)$) se réduit donc au suivant :
Problème : Calculer $a \pmod{l}$ pour l un nombre premier.

4.3.1 Théorème des Restes Chinois

Le théorème des restes chinois nous procure une méthode pour trouver le plus petit entier satisfaisant à un certain nombre de congruences. On l'utilise dans l'algorithme de Schoof pour calculer les $a_i \equiv a \pmod{l_i}$ pour un ensemble de nombres premiers l_i avec $a = q + 1 - \#\overline{E}(\mathbb{F}_q)$ et retrouver a.

Théorème 4.3.1 *: Soient $n_1, ..., n_r$ des entiers premiers entre eux deux à deux et soit $N = n_1.n_2.....n_r$ leur produit. Pour tous entiers $a_1, ..., a_r$, il existe un entier a unique modulo N tel que*

$$a \equiv a_i \pmod{n_i}$$

pour tout $i = 1, \ldots, r$.

Preuve : Pour chaque i, n_i et $\hat{n_i} = \frac{N}{n_i}$ sont premiers entre eux *i.e* $pgcd(n_i, \hat{n_i}) = 1$. Par le théorème de Bezout (algorithme d'Euclide étendu), il existe des entiers u_i et v_i tel que $u_i n_i + v_i \hat{n_i} = 1$. Posons $l_i = v_i \hat{n_i}$. On a :

$$l_i \equiv 1 \pmod{n_i}$$

et

$$l_i \equiv 0 \pmod{n_j}$$

pour $j \neq i$. Si on pose $a = \sum_{i=1}^{r} a_i l_i \pmod N$, alors a est solution du système de congruences :

$$\begin{aligned} a &\equiv a_1 \pmod{n_1} \\ &\vdots \\ a &\equiv a_r \pmod{n_r} \end{aligned}$$

Exemple 4.3.1 *: Soit à résoudre le système :*

$$\begin{aligned} a &\equiv 1 \pmod 2 \\ a &\equiv 0 \pmod 5 \\ a &\equiv 6 \pmod 7 \\ a &\equiv 7 \pmod{11} \end{aligned}$$

Ici on a $n_1 = 2$, $n_2 = 5$, $n_3 = 7$, $n_4 = 11$, *et ils sont premiers entre eux deux à deux. De plus* $N = 2 \times 5 \times 7 \times 11 = 770$.

- $n_1 = 2, \hat{n_1} = 385$ *et* $1.\hat{n_1} \equiv 1 \pmod 2$ *donc* $l_1 = 385$
- $n_2 = 5, \hat{n_2} = 154$ *et* $4.\hat{n_2} \equiv 1 \pmod 5$ *donc* $l_2 = 616$
- $n_3 = 7, \hat{n_3} = 110$ *et* $3.\hat{n_3} \equiv 1 \pmod 7$ *donc* $l_3 = 330$
- $n_4 = 11, \hat{n_4} = 70$ *et* $3.\hat{n_4} \equiv 1 \pmod 1 1$ *donc* $l_4 = 210$

et $a = \sum a_i l_i = 3835 \equiv 755 \pmod{770}$.

Remarque 4.3.1 *: Pour calculer* $a \pmod l$, *pour* l *un nombre premier, Schoof utilise les propriétés du Frobenius vues dans le chapitre* 3 *et notamment l'egalité :*

$$a \equiv trace(\phi_q)_l \pmod l$$

qui rappelons le est vraie pour $l \neq 0$ *dans* $\mathbb{F}_q$ *i.e pour* $l \neq p$ *(si* $q = p^n$*). On choisira donc tous les* $l \neq p$ *dans la suite.*

4.3.2 Cas $l = 2$

Soit $\overline{E}$ d'équation $Y^2 = X^3 + AX + B$. S'il existe $x_0 \in \mathbb{F}_q$ tel que $x_0^3 + Ax + B = 0$ alors le point $P = (x_0, 0)$ est un point d'ordre 2 de la courbe (*i.e* $2P = O$) et donc $P \in \overline{E}[2]$ (le sous-groupe des points de 2-torsion). Comme l'ordre de P divise l'ordre du groupe $\overline{E}(\mathbb{F}_q)$ qui est $\#\overline{E}(\mathbb{F}_q)$, ou en déduit que ce dernier est pair *i.e* :

$$q + 1 - a \equiv 0 \pmod 2$$

Comme q est impair, cela donne :

$$a \equiv 0 \pmod 2$$

Un point de 2-torsion vérifie $2P = O$ *i.e* $P = -P$. Donc si $P = (x_0, y_0)$, on a forcément $y_0 = 0$. Autrement dit les points de 2-torsion sont les $(x_0, 0)$ avec x_0 solution de $X^3 + AX + B$. Donc si cette équation n'a pas de solution, alors il n y a pas de point de 2-torsion et donc $\#E(\mathbb{F}_q)$ est impair ce qui donne $a \equiv 1 \pmod 2$. On a donc montré :

Proposition 4.3.1 *: Si l'équation $X^3 + AX + B$ a des solutions dans $\mathbb{F}_q$, alors*

$$a \equiv 0 \pmod 2$$

Sinon

$$a \equiv 1 \pmod 2$$

Comme les éléments de $\mathbb{F}_q$ vérifient tous l'équation

$$X^q - X = 0$$

l'équation $X^3 + AX + B$ aura une solution dans $\mathbb{F}_q$ si et seulement si :

$$pgcd(X^q - X, X^3 + AX + B) \neq 1$$

L'algorithme d'Euclide appliqué aux polynômes permet de calculer ce *pgcd* de manière trés rapide.

Corollaire 4.3.1 *:*

$$a \equiv 0 \pmod 2$$
$$\Updownarrow$$
$$pgcd(X^q - X, X^3 + AX + B) \neq 1$$

Exemple 4.3.2 *:*

1. *Soit $\overline{E}$ d'equation $Y^2 = X^3 + X + 1$ définie sur $\mathbb{F}_5$. En utilisant la commande gcd de PARI, on calcule facilement*

   $$pgcd(X^5 - X, X^3 + X + 1) = 1$$

   et donc $a \equiv 1 \pmod 2$. On serait arrivé au même résultat en remarquant que l'équation $X^3 + X + 1$ n'a pas de solution dans $\mathbb{F}_5$.

2. *Soit* $\overline{E}$ *d'équation* $Y^2 = X^3 + X + 1$ *définie sur* $\mathbb{F}_7$. *Là aussi en utilisant la commande gcd de PARI, on trouve*

$$pgcd(X^7 - X, X^3 + X + 1) = 1$$

et donc $a \equiv 1 \pmod 2$. *Ici aussi l'équation* $X^3 + X + 1$ *n'a pas de solution dans* $\mathbb{F}_7$.

4.3.3 Cas $l \neq 2, p$

Par le chapitre précédent, on sait que le Frobenius ϕ_q vérifie l'équation caractéristique

$$\phi_q^2 + qId_{\overline{E}} = a\phi_q$$

i.e que pour tout $P \in \overline{E}(\overline{\mathbb{F}_q})$, on a

$$\phi_q^2(P) + q(P) = a\phi_q(P)$$

ou encore si $P = (x, y)$ et sachant que $\phi_P(x, y) = (x^q, y^q)$:

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

avec toujours $a = q + 1 - \#\overline{E}(\mathbb{F}_q)$. Si le point $P = (x, y)$ est un point de l-torsion, *i.e* $P \in \overline{E}[l]$, ou encore $l(x, y) = O$, alors on a :

$$qP = \overline{q}P$$

avec $\overline{q} = q \pmod l$ qu'on peut choisir de telle sort que $|\overline{q}| < \frac{l}{2}$. En effet si on écrit $q = kl + \overline{q}$, on a

$$\begin{aligned} qP &= (kl + \overline{q})P \\ &= k(lP) + \overline{q}P \\ &= O + \overline{q}P \\ &= \overline{q}P \end{aligned}$$

De même on peut écrire :

$$a\phi_q(P) = \overline{a}\phi_q(P)$$

avec $\overline{a} = a \pmod{l}$. En effet si $a = kl + \overline{a}$, on a :

$$\begin{aligned} a\phi_q(P) &= (kl + \overline{a})\phi_q(P) \\ &= kl\phi_q(P) + \overline{a}\phi_q(P) \\ &= k\phi_q(lP) + \overline{a}\phi_q(P) \\ &= O + \overline{a}\phi_q(P) \\ &= \overline{a}\phi_q(P) \end{aligned}$$

Modulo l (*i.e* sur les points de l-torsion), l'équation précédente devient :

$$(x^{q^2}, y^{q^2}) + \overline{q}(x, y) = \overline{a}(x^q, y^q) \pmod{l}$$

et on sait que $\overline{a}$ est l'unique entier qui vérifie cette équation. L'idée de l'algorithme de Schoof est de calculer toute les quantités intervenant dans cette équation (en tant que fonctions rationnelles de x et y) et de trouver l'unique entier $\overline{a}$ qui vérifie l'egalité. On pourrait par exemple calculer les deux fonctions rationnelles donnant $(x^{q^2}, y^{q^2}) + q(x, y)$ d'une part, et calculer les deux fonctions rationnelles donnant $\overline{a}(x^q, y^q)$ et essayer de trouver l'egalité en essayant toutes les valeurs $\overline{a} = 0, 1, 2, \ldots, l-1$ possibles. On peut aussi utiliser, en suivant Schoof, les polynômes de division qui comme on l'a vu permettent le calcul des multiples d'un point P. Sur $\overline{E}[l]$ l'équation caractéristique du Frobenius est :

$$\phi_l^2 + \overline{q} = \overline{a}\phi_l$$

i.e

$$\phi_l^2(P) + \overline{q}P = \overline{a}\phi_l(P), \quad \forall P \in \overline{E}[l]$$

avec $\overline{a} \equiv a \pmod{l}$ et $\overline{q} \equiv q \pmod{l}$ et $|\overline{q}| < \frac{l}{2}$. En utilisant les polynômes de division on peut réecrire $\overline{q}P$ et $\overline{a}\phi_l(P)$:

$$(x_{\overline{q}}, y_{\overline{q}}) = \overline{q}(x, y) = (x - \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2}, \frac{\psi_{2\overline{q}}}{\psi_{\overline{q}}^4})$$

$$\overline{a}\phi_l(P) = (x_{\overline{a}}^q, y_{\overline{a}}^q) = (x^q - (\frac{\psi_{\overline{a}-1}\psi_{\overline{a}+1}}{\psi_{\overline{q}}^2})^q, (\frac{\psi_{2\overline{a}}}{\psi_{\overline{a}}^4})^q)$$

et l'équation devient pour $P = (x, y) \in E[l]$:

$$(x^{q^2}, y^{q^2}) + \overline{q}(x, y) = \overline{a}(x^q, y^q)$$

ou encore

$$(x^{q^2}, y^{q^2}) + (x_q, y_q) = (x_{\overline{a}}^q, y_{\overline{a}}^q)$$

On rencontre à ce stade un premier obstacle car la formule pour calculer $(x^{q^2}, y^{q^2}) + \overline{q}(x, y)$ varie selon que les deux points sont distincts ou selon qu'ils aient ou non la même x-coordonnée. Autrement dit on doit distinguer les cas $(x^{q^2}, y^{q^2}) \neq \pm\overline{q}(x, y)$ et $(x^{q^2}, y^{q^2}) = \pm\overline{q}(x, y)$. On sait en effet d'aprés les formules de la loi d'addition sur la courbe elliptique que si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$:

$$x_1 = x_2 \Longleftrightarrow Q = \pm P$$

L'algorithme de Schoof commence par tester s'il existe un $P = (x, y) \in \overline{E}[l]^*$ tel que $(x^{q^2}, y^{q^2}) = \pm\overline{q}(x, y)$. Pour cela on compare les x-coordonnées $i.e$ on vérifie si :

$$x^{q^2} = x_{\overline{q}} = x - \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2}$$

ou encore

$$(x^{q^2} - x)\psi_{\overline{q}}^2 + \psi_{\overline{q}-1}\psi_{\overline{q}+1} = 0$$

Par les propriétés des polynômes de division, ce dernier polynôme est un polynôme en x seul. Appelons le $P(x)$. On a donc montré que :

$$\exists P = (x, y) \in \overline{E}[l]^* / \phi_l^2(P) = \pm\overline{q}P \Longleftrightarrow P(x) = 0$$

Il est maintenant trés aisé d'obtenir la :

Proposition 4.3.2 *: Il existe $P = (x, y) \in \overline{E}[l]^*$ tel que*

$$\phi_l^2(P) = \pm qP \quad (i.e \quad (x^{q^2}, y^{q^2}) = \pm q(x, y))$$

si et seulement si

$$pgcd(P(x), \psi_l(x) \neq 1$$

Preuve : On sait que $P = (x, y) \in \overline{E}[l] \Longleftrightarrow \psi_l(x, y) = 0$. Pour savoir si $\phi_l^2(P) = \pm qP$ on évalue $P(x) = 0$ sur les points de l-torsion. Un tel point existe $\Longleftrightarrow P(x)$ et $\psi_l(x)$ ont des racines communes $i.e$ $pgcd(\psi_l(x), P(x)) \neq 1$. Ainsi selon qu'il existe ou non un point $P \in \overline{E}[l]^*$ tel que $(x^{q^2}, y^{q^2}) = \pm q(x, y)$ les méthodes de calcul de $\overline{a}$ vont différer (tout simplement parce que les formules de la loi d'addition ne sont pas le mêmes). S'il existe un $P \in \overline{E}[l]^*$ tel que $\phi_l^2(P) = \pm\overline{q}P$, on est dans le cas 1 de l'algorithme de Schoof. Sinon si $\forall P \in \overline{E}[l]^*$, $\phi_l^2(P) \neq \pm\overline{q}P$ on est dans le cas 2 de l'algorithme de Schoof et on dispose , par la proposition precédente, d'un test simple pour vérifier cela.

Remarquons aussi (et c'est trés important pour l'algorithme) que si pour un point $P \in \overline{E}[l]^*$, on a calculé un nombre $\overline{b} \in \frac{\mathbb{Z}}{l\mathbb{Z}}$ tel que :

$$\phi_l^2(P) - \overline{b}\phi_l(P) + \overline{q}P = 0$$

alors $\overline{b} = \overline{a}$ et on aura calculé $\overline{a}$ pour tous les autres points (autrement dit pour calculer $\overline{a}$ il suffit de le faire au niveau d'un point quelconque de $\overline{E}[l]^*$ à travers l'équation caractéristique). En effet, on sait aussi que :

$$\phi_l^2(P) - \overline{a}\phi_l(P) + \overline{q}P = 0$$

donc $(\overline{a} - \overline{b})\phi_l(P) = O$. Comme P est un point de l-torsion, $\phi_l(P)$ l'est aussi et donc $\overline{a} - \overline{b}$ divise l *i.e* $\overline{a} - \overline{b} = O$ dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$ et donc $\overline{a} = \overline{b}$.

Algorithme de Schoof cas 1

On suppose qu'il existe $P = (x, y) \in \overline{E}[l]^*$ tel que :

$$\phi_l(P) = \pm\overline{q}P$$

i.e

$$(x^{q^2}, y^{q^2}) = \pm\overline{q}(x, y)$$

La proposition suivante permet déja de lister toutes les possibilités pour $\overline{a}$ dans ce cas.

Proposition 4.3.3 *: Si $\phi_l^2(P) = \pm\overline{q}P$ pour un $P \in \overline{E}[l]^*$, alors $\overline{a}$ ne peut prendre que trois valeurs possibles :*

$$\overline{a} = 0 \quad ou \quad \overline{a} = 2w \quad où \quad \overline{a} = -2w.$$

avec $w \in \frac{\mathbb{Z}}{l\mathbb{Z}}$ vérifiant $\overline{q} = w^2$.

Preuve : Si $\phi_l^2(P) = \overline{q}P$, on obtient par l'équation caractéristique :

$$2\overline{q}P = \overline{a}\phi_l(P)$$

Remarquer que $2\overline{q} \neq 0$ (dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$) (car $l \neq 2$ et $l \neq p$ et $|\overline{q}| < \frac{l}{2}$, ce qui donne $2 \neq 0$, $\overline{q} \neq 0$ et $2\overline{q} \neq 0$). Donc dans ce cas on doit avoir $\overline{a} \neq 0$ (dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$). De plus en prenant au carré, on obtient

$$4\overline{q}2P = \overline{a}^2\phi_l^2(P) = \overline{a}^2\overline{q}P$$

donc

$$4\overline{q}^2 = \overline{a}^2\overline{q}$$

et

$$4\overline{q} = \overline{a}^2.$$

ou encore

$$\overline{q} = (\frac{\overline{q}}{2})^2 = w^2 \quad avec \quad w = \sqrt{q}$$

ce qui donne $\overline{a} = \pm 2w$. Donc si on est dans le cas $\phi_l^2 = +\overline{q}P$, on sait que $\overline{q} = w^2$ est un carré dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$ et $\overline{a} = \pm 2w \neq 0$. Si $\phi_l^2(P) = -qP$ (ce qui est sûr si $\overline{q}$ n'est pas un carré dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$), l'équation caractéristique donne :

$$\overline{a}\phi_l(p) = 0$$

et comme $\phi_l(P) \neq 0$ et $0 \leq \overline{a} \leq l-1$, on doit avoir

$$\overline{a} = 0$$

dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$.
On peut reformuler cette proposition en disant que si $\phi_l^2(p) = -qP$ alors $\overline{a} = 0$ et si $\phi_l^2(P) = qP$ alors $\overline{q} = w^2$ est un carré et $\overline{a} = \pm 2w$. Pour continuer l'algorithme on peut procéder ainsi : On teste si $\overline{q}$ est un carré ou non dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$. Si $\overline{q}$ n'est pas un carré dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$ (rappelons qu'on est toujours dans le cas 1 : $\phi_l^2(P) = \pm P$) alors on est sûr que $\overline{a} = 0$. Sinon si $\overline{q}$ est un carré dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$ on aura soit $\phi_l^2(p) = +\overline{q}P$, soit $\phi_l^2(P) = -\overline{q}P$ et il nous faut un moyen pour distinguer les 2 cas. (Si $\phi_l^2(P) = \overline{q}P$, on sait que $\overline{q}$ est un carré mais l'inverse n'est pas toujours vrai . Il se peut que $\overline{q}$ soit un carré et qu' on ait quand même $\phi_l^2(P) = -\overline{q}P$). Si $\overline{q}$ est un carré et $\phi_l^2(P) = \overline{q}P$, on doit avoir

$$(\phi_l - w)(\phi_l + w)(P) = \phi_l^2(P) - \overline{q}P = 0$$

et donc

$$\phi_l(P) = \pm wP$$

ce que l'on peut tester en comparant les x coordonneés :

$$x^q = x - \frac{\psi_{w-1}\psi_{w+1}}{\psi_w^2}$$

ou encore

$$(x^q - x)\psi_w^2 + \psi_{w-1}\psi_{w+1} = 0$$

Appelons ce dernier polynôme $Q(x)$ (c'est un polynôme en x seul). On a donc

$$\phi_l(P) = \pm wP \Leftrightarrow Q(x) = 0$$

$$\Leftrightarrow pgcd(Q(x), \psi_l(x)) \neq 1$$

puisque $P = (x, y) \in \overline{E}[l] \Leftrightarrow \psi_l(x) = 0$. Si $pgcd(Q(x), \psi_l(x)) = 1$, alors on doit être dans le cas $\phi_l^2(P) = -\overline{q}P$. Résumons :

Proposition 4.3.4 *: Sachant que $\phi_l^2(P) = \pm\overline{q}P$, on a*

1. *si $\overline{q}$ n'est pas un carré alors $\overline{a} = 0$*
2. *si $\overline{q}$ est un carré alors on a :*
   (a) *si $pgcd(Q(x), \psi_l(x)) = 1$, alors $\overline{a} = 0$.*
   (b) *si $pgcd(Q(x), \psi_l(x)) \neq 1$ alors $\overline{a} = \pm 2w$ avec $\overline{q} = w^2$*

Preuve : Si $\overline{q}$ n'est pas un carré, on est dans le cas $\phi_l^2 = -\overline{q}P$ et donc $\overline{a} = 0$. Si $\overline{q}$ est un carré, on est dans l'un des deux cas $\phi_l^2(P) = \overline{q}P$ ou $\phi_l^2(P) = -\overline{q}P$. Si $\phi_l^2(P) = \overline{q}P$, on doit avoir $\phi_l(P) = \pm wP$ et donc $pgcd(Q(x), \psi_l(x)) \neq 1$ ce qui donne $a = \pm 2w$. Sinon on est dans le cas $\phi_l^2(P) = -\overline{q}P$ et $\overline{a} = 0$.
Il nous reste à discerner entre $a = +2w$ et $a = -2w$ dans le cas $\phi_l^2(P) = \overline{q}P$ (et donc $\overline{q}$ carré dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$). Pour cela il suffit de remarquer que :

$$\phi_l(P) = wP \Rightarrow a = +2w$$

$$\phi_l(P) = -wP \Rightarrow a = -2w$$

La x coordonnée de $\phi_l(P)$ est la même que celle de wP ou $-wP$. Donc pour savoir si $\phi_l(P) = wP$ ou $\phi_l(P) = -wP$, on compare les y-coordonneés. Si $\phi_l(P) = wP$, on doit avoir :

$$y^q = \frac{\psi_{2w}}{2\psi_w^2}$$

ou encore :

$$2\psi_w^2 y^q - \psi_{2w} = 0$$

Appelons ce polyôme $R(x)$ (remarquer que c'est un polynôme en x seul puisque $y^2 = x^3 + Ax + B$). On a donc : si $P = (x, y) \in \overline{E}[l]^* : \phi_l(P) = wP \Leftrightarrow R(x) = 0$ et donc

$$\phi_l(P) = wP \Leftrightarrow pgcd(R(x), \psi_l(x)) \neq 1$$

On a donc obtenu :

Proposition 4.3.5 *Si $pgcd(R(x), \psi_l(x)) \neq 1$ alors $\overline{a} = 2w$, sinon $\overline{a} = -2w$.*

Preuve : $pgcd(R(x), \psi_l(x) \neq 1 \Rightarrow \phi_l(P) = wP$ et donc $a = 2w$. Si $pgcd(R(x), \psi_l(x)) = 1$, on ne peut pas avoir $\phi_l(p) = wP$ et $\overline{a} = -2w$.
On peut maintenant donner un résumé de ce premier cas de l'algorithme de Schoof :
Resumé du cas 1 :

1. Si $pgcd(P(x), \psi_l(x)) \neq 1$, il existe $P \in \overline{E}[l]^*/\phi_l^2(p) = \pm\overline{q}P$.
2. $\overline{a} = 0$ si $\overline{q}$ n'est pas un carré dans $\frac{\mathbb{Z}}{l\mathbb{Z}}$.
3. $\overline{a} = 0$ si $\overline{q}$ est un carré et $pgcd(Q(x), \psi_l(x)) = 1$.
4. Si $\overline{q}$ est un carré et $pgcd(Q(x), \psi_l(x) \neq 1$, alors soit $w/w^2 = \overline{q}$. On a :
   (a) $\overline{a} = +2w$ si $pgcd(R(x), \psi_l(x)) \neq 1$.
   (b) $\overline{a} = -2w$ si $pgcd(R(x), \psi_l(x)) = 1$.

Algorithme de Schoof Cas 2 :
C'est le cas ou $\phi_l^2(P) \neq \pm\overline{q}P, \forall P \in \overline{E}[l]^*$. Ce qui arrive si $pgcd(P(x), \psi_l(x)) = 1$. L'algorithme procède alors par tester pour chaque $j \in (\frac{\mathbb{Z}}{l\mathbb{Z}})^*$ s'il existe un $P = (x, y) \in \overline{E}[l]$ tel que :

$$(x^{q^2}, y^{q^2}) + \overline{q}(x, y) = j(x^q, y^q) = (x_j^q, y_j^q)$$

Puisqu'on est dans le cas 2 *i.e* $x_1 \neq x_2$, le calcul de $(x^{q^2}, y^{q^2}) + \overline{q}(x, y)$ se fait en utilisant :

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Ici on a

$$y_2 - y_1 = \frac{\psi_{2\overline{q}}}{2\psi_{\overline{q}}^4} - y^{q^2} = \frac{\psi_{2\overline{q}} - 2\psi_{\overline{q}}^4 y^{q^2}}{2\psi_{\overline{q}}^4}$$

et

$$x_2 - x_1 = x - \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2} - x^{q^2} = \frac{(x - x^{q^2})\psi_{\overline{q}}^2 - \psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2}$$

Ce qui donne :

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{(\psi_{\overline{q}+2}\psi_{\overline{q}-1}^2 - \psi_{\overline{q}-2}\psi_{\overline{q}+1}^2 - 4\psi_{\overline{q}}^3 y^{q^2+1})}{4y\psi_{\overline{q}}(-\psi_{\overline{q}-1}\psi_{\overline{q}+1} - \psi_{\overline{q}}^2(x^{q^2} - x))} = \frac{\alpha}{\beta}$$

Si $(x_3, y_3) = (x^{q^2}, y^{q^2}) + \overline{q}(x, y)$, alors on a :

$$x_3 = m^2 - x_1 - x_2 = m^2 - (x^{q^2} + x) + \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2}$$

et

$$y_3 = m(2x_1 + x_2 - m^2) - y_1 = m(2x^{q^2} + x - \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2} - m^2) - y^{q^2}$$

De plus comme $\psi_n(x^q, y^q) = \psi_n(x, y)^q$, on a :

$$j(x^q, y^q) = ((x - \frac{\psi_{j-1}\psi_{j+1}}{\psi_j^2})^q, (\frac{\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2}{4y\psi_j^3})^q)$$

Comme pour deux points $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ on a :

$$P = \pm Q \Longleftrightarrow x_1 = x_2$$

en égalant les x-coordonnées de $(x^{q^2}, y^{q^2}) + \overline{q}(x, y)$ et $j(x^q, y^q)$ on pourra déterminer si $\overline{a} = \pm j$. Donc $\overline{a} = \pm j$ si et seulement si :

$$m^2 - (x^{q^2} + x) + \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2} = (x - \frac{\psi_{j-1}\psi_{j+1}}{\psi_j^2})^q$$

Ce qu'on peut arranger en :

$$\psi_j^{2q}(\alpha^2\psi_{\overline{q}}^2 - \beta^2\psi_{\overline{q}}^2(x^{q^2} + x) + \beta^2\psi_{\overline{q}-1}\psi_{\overline{q}+1}) - \beta^2\psi_{\overline{q}}^2(\psi_j^{2q}x^q - (\psi_{j-1}\psi_{j+1})^q) = 0$$

Par les propriétés des polynômes de division ψ_n, on vérifie facilement que ce polynôme est un polynôme en x seul. Appelons le $S(x)$. On a donc obtenu :

Proposition 4.3.6 *: Soit $j \in (\frac{\mathbb{Z}}{l\mathbb{Z}})^*$, il existe $P = (x, y) \in \overline{E}[l]$ tel que :*

$$(x^{q^2}, y^{q^2}) + \overline{q}(x, y) = \pm j(x^q, y^q)$$

si et seulement si :

$$pgcd(S(x), \psi_l(x)) \neq 1$$

Preuve : Un tel point existe si et seulement si $S(x) = 0$ et donc S et ψ_l ont des racines communes. Donc $pgcd(S(x), \psi_l(x)) \neq 1$.
Une fois qu'on sait qu'il existe un $P = (x, y) \in \overline{E}[l]$ tel que :

$$(x^{q^2}, y^{q^2}) + \overline{q}(x, y) = \pm j(x^q, y^q)$$

i.e $\overline{a} = \pm j$ il reste a déterminer si $a = +j$ ou $a = -j$. Pour cela on utilise le fait que si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ alors

$$\begin{array}{lcl} P = Q & \Longleftrightarrow & x_1 = x_2 \quad et \quad y_1 = y_2 \\ P = -Q & \Longleftrightarrow & x_1 = x_2 \quad et \quad y_1 = -y_2 \end{array}$$

On va donc comparer les y-coordonnées de $(x^{q^2}, y^{q^2}) + \overline{q}(x, y)$ et $j(x^q, y^q)$. Si elles sont égales alors $\overline{a} = +j$ sinon $\overline{a} = -j$. Si elles sont égales on doit avoir :

$$m(2x^{q^2} + x - \frac{\psi_{\overline{q}-1}\psi_{\overline{q}+1}}{\psi_{\overline{q}}^2} - m^2) - y^{q^2} = (\frac{\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2}{4y\psi_j^3})^q$$

Ce qui donne

$$(4y\psi_j^3)^q(m(\psi_{\overline{q}}^2(2x^{q^2} + x) - \psi_{\overline{q}-1}\psi_{\overline{q}+1} - \psi_{\overline{q}}^2 m^2) - \psi_{\overline{q}}^2 y^{q^2})$$

$$-\psi_{\overline{q}}^2(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2)^q = 0$$

avec

$$m = \frac{\alpha}{\beta}$$

ou encore

$$(4y\psi_j^3)^q(\frac{\alpha}{\beta}(\psi_{\overline{q}}^2(2x^{q^2} + x) - \psi_{\overline{q}-1}\psi_{\overline{q}+1} - \psi_{\overline{q}}^2\frac{\alpha^2}{\beta^2}) - \psi_{\overline{q}}^2 y^{q^2})$$

$$-\psi_{\overline{q}}^2(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2)^q = 0$$

ou encore

$$(4y\psi_j^3)^q(\alpha\beta^2\psi_{\overline{q}}^2(x^{q^2} + x) - \alpha\beta^2\psi_{\overline{q}-1}\psi_{\overline{q}+1} - \alpha^3\psi_{\overline{q}}^2 - \beta^3\psi_{\overline{q}}^2 y^{q^2})$$

$$-\beta^3\psi_{\overline{q}}^2(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1}^2)^q = 0$$

Toujours en utilisant les proprietés des polynômes de division, ce polynôme est un polynôme en x seul. Appelons le $T(x)$. On a donc :

Proposition 4.3.7 *: $\overline{a} = +j$ si et seulement si $pgcd(T(x), \psi_l(x)) \neq 1$.*

Preuve : $\overline{a} = +j$ si et seulement si $T(x) = 0$ pour $P = (x, y) \in \overline{E}[l]$. Donc T et ψ_l ont des racines communes et donc $pgcd(T, \psi_l) \neq 1$.

Remarque 4.3.2 *Comme dans un premier temps il s'agit de déterminer si $a = \pm j$ pour $1 \leq j \leq l-1$, il suffit de vérifier cela pour $1 \leq j \leq \frac{l-1}{2}$ car si $1 \leq j \leq \frac{l-1}{2}$ alors $\frac{l-1}{2} < -j \leq l-1$*

Resumé du cas 2

1. Si $pgcd(P(x), \psi_l(x)) = 1$ alors $\phi_l^2(P) \neq \pm\overline{q}P, \forall P \in \overline{E}[l]$ et on est dans le cas 2 de Schoof .

2. Pour $j \in \{1, \ldots, \frac{l-1}{2}\}$, on essaie de trouver un $P = (x, y) \in \overline{E}[l]$ tel que :
$$(x^{q^2}, y^{q^2}) + \overline{q}(x, y) = \pm j(x^q, y^q)$$
Un tel P existe $\Leftrightarrow pgcd(S(x), \psi_l(x)) \neq 1$ et $\overline{a} = \pm j$.
3. $\overline{a} = +j$ si $pgcd(T(x), \psi_l(x)) \neq 1$ et $\overline{a} = -j$ sinon.

Nous donnons maintenant l'algorithme de Schoof complet.

Algorithme de Schoof

Soit une courbe elliptique sur $\mathbb{F}_q$ d'équation $Y^2 = X^3 + AX + B$ et soit $a = q + 1 - \#\overline{E}(\mathbb{F}_q)$.

1. Si $pgcd(X^q - X, X^3 + AX + B) = 1$ alors $a \equiv 1 \pmod 2$.
Sinon $a \equiv 0 \pmod 2$.
2. Créer un ensemble de petits nombres premiers $L = \{l_1, l_2, \ldots, l_k\}$ avec $l_1 < l_2 < \ldots < l_k, l_i \neq p, \forall i$ et
$$\prod_{i=1}^{k} l_i > 4\sqrt{q}.$$
3. Calculer les l_k polynômes de division $\psi_0, \psi_1, \psi_2, \ldots, \psi_{l_k}$.
4. pour tout $l \in L$, calculer $\overline{q} = q \pmod l$.
5. Si $pgcd(P(x), \psi_l(x)) \neq 1$ alors il existe $P \in \overline{E}[l]$ tel que $\phi_l^2(P) = \pm\overline{q}P$.
6. Si $\overline{q}$ n'est pas un carré $\pmod l$, alors $a \equiv 0 \pmod l$.
7. Sinon si $\overline{q}$ est un carré $\pmod l$ calculer w tel que $w^2 \equiv \overline{q} \pmod l$.
8. Si $pgcd(Q(x), \psi_l(x)) = 1$, alors $a \equiv 0 \pmod l$
Sinon
9. Si $pgcd(R(x), \psi_l(x)) \neq 1$, alors $a \equiv 2w \pmod l$
Sinon $a \equiv -2w \pmod l$.
10. Si $pgcd(P(x), \psi_l(x)) = 1$, alors $\phi_l^2(P) \neq \pm\overline{q}P$ et on est dans le cas 2 de Schoof.
11. Pour $j = 1, \ldots, \frac{l-1}{2}$
12. Si $pgcd(S(x), \psi_l(x)) \neq 1$, il existe $P \in \overline{E}[l]$ tel que
$$\phi_l^2(P) + \overline{q}P = \pm j\, \phi_l(P) \pmod l$$
et donc
$$a \equiv \pm j \pmod l.$$

13. Si $pgcd(T(x), \psi_l(x)) \neq 1$, alors $\overline{a} \equiv j \pmod{l}$.
    Sinon $a \equiv -j \pmod{l}$.
14. Passer au j suivant.
15. Passer au l suivant.
16. A ce stade on aura calculé $a \pmod{l_i}$ pour tout $l_i \in L$.
17. On utilise la théorème des restes chinois pour calculer $a \pmod{N}$ avec

$$N = \prod_{i=1}^{k} l_i$$

    et donc a.
18. Calculer $\#\overline{E}(\mathbb{F}_q) = q + 1 - a$.

4.4 Exemples

Nous illustrons l'algorithme de Schoof à travers deux exemples.

Exemple 1 :

Soit la courbe elliptique $\overline{E}$ d'équation : $Y^2 = X^3 + X + 1$ sur $\mathbb{F}_7$. Nous allons utiliser l'algorithme de Schoof pour calculer $\#\overline{E}(\mathbb{F}_7)$ en nous aidant du logiciel PARI.

Ici on a $q = p = 7$ et donc $4\sqrt{q} \simeq 10,58$. On peut donc prendre $N = 15 = 3.5$. Donc $l_1 = 3$ et $l_2 = 5$. En utilisant PARI, on calcule les premiers polynômes de division :

$\psi_0 = 0$, $\psi_1 = 1$, $\psi_2 = 2Y$

$\psi_3 = 3X^4 + 6X^2 + 12X - 1$

$\psi_4 = 4Y(X^6 + 5X^4 + 20X^3 - 5X^2 - 4X - 9)$

$\psi_5 = -27X^{12} - 130X^{10} - 260X^9 - 41X^8 - 272X^7 + 228X^6 + 712X^5 - 2077X^4 - 1936X^3 - 866X^2 - 740X - 287$

Il ne faut pas oublier qu'ici, tous les calculs de polynômes et de leur pgcd se font modulo 7.

$* l = 3$:

On a $\overline{q} = 7 \pmod{3} = 1$. On commence par tester s'il y a un point $P \in \overline{E}[3]$ tel que :

$$\phi_3^2(P) = \pm P$$

Pour cela on calcule le polynôme :

$$\begin{aligned} P(x) &= (x^{q^2} - x)\psi_{\overline{q}}^2 - \psi_{\overline{q}-1}\psi_{\overline{q}+1} \\ &= (x^{7^2} - x)\psi_1^2 - \psi_0\psi_2 \\ &= (x^{49} - x) \end{aligned}$$

Puis on regarde si $pgcd(P(x), \psi_3(x)) = 1$ ou $\neq 1$. En utilisant la commande *gcd* (modulo 7) de PARI, on trouve :

$$pgcd(P(x), \psi_3(x)) = \psi_3(x) \neq 1$$

et donc on est dans le cas 1 de l'algorithme de Schoof. Comme $\overline{q} = 1$ est un carré dans $\frac{\mathbb{Z}}{3\mathbb{Z}}(1 = 1^2)$, l'étape suivante consiste à calculer le polynôme :

$$\begin{aligned} Q(x) &= (x^q - x)\psi_1^2 + \psi_0\psi_2 \\ &= x^q - x = x^7 - x \end{aligned}$$

et à voir si $pgcd(Q(x), \psi_3(x)) = 1$ ou $\neq 1$. Toujours en utilisant PARI, on trouve

$$pgcd(Q(x), \psi_3(x)) = 1$$

et donc $\overline{a} = 0$ *i.e* :

$$a \equiv 0 \pmod 3$$

$* l = 5$:
Ici on a $\overline{q} = 7 \pmod 5 = 2$.

$$\begin{aligned} P(x) &= (x^{q^2} - x)\psi_{\overline{q}}^2 + \psi_{\overline{q}-1}\psi_{\overline{q}+1} \\ &= (x^{7^2} - x)\psi_2^2 + \psi_1\psi_3 \\ &= 4Y^2(x^{49} - x) + \psi_3 \\ &= 4x^{52} + 4x^{50} + 4x^{49} - x^4 + 2x^2 + 8x - 1 \end{aligned}$$

La commande *gcd* de PARI donne :

$$pgcd(P(x), \psi_5(x)) = 1$$

et on est donc dans le cas 2 de l'algorithme de Schoof. Comme $l = 5$, on a $\frac{l-1}{2} = \frac{5-1}{2} = 2$. Donc pour $j = 1, 2$, on essaie de trouver un point $P \in \overline{E}[5]$ tel que

$$\phi_5^2(P) + 2P = \pm j\phi_5(P)$$

Un tel P existe si et seulement si $pgcd(S(x), \psi_5(x)) \neq 1$ avec

$$S(x) = \psi_j^{2q}(\alpha^2\psi_{\overline{q}}^2 - \beta^2\psi_{\overline{q}}^2(x^{q^2} + x) + \beta^2\psi_{\overline{q}-1}\psi_{\overline{q}+1})$$

$$-\beta^2\psi_{\overline{q}}^2(\psi_j^{2q}x^q - (\psi_{j-1}\psi_{j+1})^q).$$

et $\frac{\alpha}{\beta} = m$ avec :

$$\alpha = \psi_{\overline{q}+2}\psi_{\overline{q}-1}^2 - \psi_{\overline{q}-2}\psi_{\overline{q}+1}^2 - 4\psi_{\overline{q}}^3 y^{q^2+1}$$

$$\beta = 4y\psi_{\overline{q}}(-\psi_{\overline{q}-1}\psi_{\overline{q}+1} - \psi_{\overline{q}}^2(x^{q^2} - x))$$

Ici $\overline{q} = 2$ et donc

$$\begin{aligned} \alpha &= \psi_4\psi_1^2 - \psi_0\psi_3^2 - 4\psi_2^3Y^{50} \\ &= \psi_4 - 4\psi_2^3Y^{50} = \psi_4 - 32Y^{53} \\ &= Y(\tfrac{\psi_4}{Y} - 32Y^{52}) \end{aligned}$$

$$\begin{aligned} \beta &= 4y\psi_2(-\psi_1\psi_3 - \psi_2^2(x^{49} - x)) \\ &= 4Y\psi_2(-\psi_3 - \psi_2^2(x^{49} - x)) \\ &= -4Y\psi_2\psi_3 - 4Y\psi_2^3(x^{49} - x) \\ &= -8Y^2\psi_3 - 32Y^4(x^{49} - x)) \end{aligned}$$

$*$ Pour $j = 1$ (et $\overline{q} = 2$), on a :

$$S(x) = 4Y^2\alpha^2 - 4Y^2\beta^2(x^{49} + x) + \beta^2\psi_3 - 4Y^2\beta^2x^7$$

et en utilisant PARI , on trouve $pgcd(S(x), \psi_5(x)) = 1$ (modulo 7) et donc on passe à $j = 2$.
$*$ Pour $j = 2$ (et $\overline{q} = 2$), on a :

$$S(x) = 2^{14}(Y^2)^7(4Y^2\alpha^2) - 4Y^2\beta^2(x^{45} + x) + \beta^2\psi_3) - 4Y^2\beta^2(2^{14}(y^2)^7x^7 - \psi_3^7).$$

et on trouve :

$$pgcd(S(x), \psi_5(x)) = 5x \neq 1$$

Donc

$$\overline{a} = a \pmod 5 = \pm 2$$

Pour savoir si $\overline{a} = +2$ ou $\overline{a} = -2$, on doit utiliser le polynôme $T(x)$: $\overline{a} = +2$ si $pgcd(T(x), \psi_5(x)) \neq 1$ et $\overline{a} = -2$ si $pgcd(T(x), \psi_5(x)) = 1$ avec :

$$T(x) = (4y\psi_j^3)^q(\alpha\beta^2\psi_{\overline{q}}^2(x^{q^2} + x) - \alpha\beta^2\psi_{\overline{q}-1}\psi_{\overline{q}+1} - \alpha^3\psi_{\overline{q}}^2 - \beta^3\psi_{\overline{q}}^2y^{q^2})$$

$$-\beta^3\psi_{\overline{q}}^2(\psi_{j+2}\psi_{j-1}^2 - \psi_{j-2}\psi_{j+1})^q$$

Ici , on a $j = 2$ est $\overline{q} = 2$. Donc

$$T(x) = (4y\psi_2^3)^7(\alpha\beta^2(2x^{49} + x)\psi_2^2) - \alpha\beta^2\psi_3 - \alpha^3\psi_2^2 - \beta^3\psi_2^2 y^{49}) - \beta^3\psi_2^2\psi_3^7)$$

et on trouve :

$$pgcd(T(x), \psi_5(x)) = 1$$

donc

$$a \equiv -2 = 3 \pmod 5$$

On a donc

$$a \equiv 0 \pmod 3$$
$$a \equiv 3 \pmod 5$$

et

$$a \equiv 3 \pmod{15}$$

ce qui donne

$$a = 3$$

Ainsi on a

$$\#\overline{E}(\mathbb{F}_7) = q + 1 - a = 8 - 3 = 5$$

Exemple 2 :
Soit la même courbe $\overline{E}$ d'équation : $Y^2 = X^3 + X + 1$ mais sur $\mathbb{F}_5$. Ici on a $q = p = 5$ et donc $4\sqrt{q} \simeq 8,94$. On peut donc prendre $N = 14 = 2.7$. Donc $l_1 = 2$ et $l_2 = 7$. En plus des polynômes de division déja calculés, on aura aussi besoin de ψ_6, jusqu'à ψ_9 que l'on calcule avec PARI.
$* l = 2$:
Comme $pgcd(X^5 - X, X^3 + X + 1) = 1$, on a $\overline{a} = a \pmod 2 = 1$.
$* l = 7$:
On a $\overline{q} = 5 \pmod 7$. On commence par tester s'il y a un point $P \in \overline{E}[7]$ tel que :

$$\phi_7^2(P) = \pm 5P$$

Pour cela on calcule le polynôme :

$$\begin{aligned} P(x) &= (x^{q^2} - x)\psi_{\overline{q}}^2 - \psi_{\overline{q}-1}\psi_{\overline{q}+1} \\ &= (x^{5^2} - x)\psi_5^2 - \psi_4\psi_6 \\ &= (x^{25} - x)\psi_5^2 - \psi_4\psi_6 \end{aligned}$$

Puis on regarde si $pgcd(P(x), \psi_7(x)) = 1$ ou $\neq 1$. On trouve :

$$pgcd(P(x), \psi_7(x)) = 1$$

et donc on est dans le cas 2 de l'algorithme de Schoof. Comme $l = 7$, on a $\frac{l-1}{2} = \frac{7-1}{2} = 3$. Donc pour $j = 1, 2, 3$, on essaie de trouver un point $P \in \overline{E}[7]$ tel que

$$\phi_7^2(P) + 5P = \pm j\phi_7(P)$$

Un tel P existe si et seulement si $pgcd(S(x), \psi_7(x)) \neq 1$. Pour $j = 3$, on trouve

$$pgcd(S(x), \psi_7(x)) \neq 1$$

et donc $\overline{a} = a \pmod 7 = \pm 3$. Pour savoir si $\overline{a} = +3$ ou -3, on utilise le polynôme $T(x)$. On trouve

$$pgcd(T(x), \psi_7(x)) = 1$$

et donc $\overline{a} = -3$. On a donc

$$a \equiv 1 \pmod 2$$

et

$$a \equiv -3 = 4 \pmod 7$$

ce qui donne $a \equiv 11 \pmod{14}$ et

$$a = -3$$

Ainsi

$$\#\overline{E}(\mathbb{F}_5) = 5 + 1 - (-3) = 9$$

Conclusion Générale

D'aprés ce qui précéde on voit plusieurs méthodes pour calculer le nombre de points d'une courbe elliptique $\overline{E}$ définie sur un corps fini $\mathbb{F}_q$ donnée par l'equation de Weierstrass :

$$Y^2 = X^3 + AX + B$$

avec : $A, B \in \mathbb{F}_q$.
Mais Il suffit d'utilisée l'algorithme de Schoof qui est considéré comme le premier algorithme déterministe à complexité polynômiale et donc comme étant trés rapide.

Bibliographie

[1] I. F. Blake, G. Seroussi, and N. P. Smart, Elliptic curves in cryptography, London Mathematical Society Lecture Note Series, vol. 265, Cambridge University Press, Cambridge, 2000.

[2] L. Charlap, D. Robbins : An elementary introduction to elliptic curves I and II, CRD Expository Reports No. 3 1 and 34, Institute for Defense Analysis, Princeton, 1988

[3] W. Fulton. Algebraic curves. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of R. Weiss, Reprint of 1969 original.

[4] D. Hankerson, A. Menezes, and S. Vanstone. Guide to elliptic curve cryptography. Springer-Verlag, New York, 2004.

[5] N. Koblitz. Elliptic curve cryptosystems. Math. Comp., 48(177) :203209, 1987.

[6] S. Lang. Elliptic curves : Diophantine analysis, volume 231 of Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 1978.

[7] S. Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

[8] S. Lang and H. Trotter, Frobenius Distributions in GL2-Extensions, Lecture Notes in Math., vol.504, Springer-Verlag, Berlin and New York, 1976.

[9] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1986.

[10] V. S. Miller. Use of elliptic curves in cryptography. In Advances in cryptology-CRYPTO 85, volume 218 of Lecture Notes in Comput. Sci., pages 417426.Springer, Berlin, 1986.

[11] R. Mermoul et A. Barkat, Les corps finis et leur application en théorie des codes, Mémoire de Licence, Centre Universitaire de Mila, 2013.

[12] PARI/GP, version 2.6.0, The PARI Group, Bordeaux, 2013. available from http ://pari.math.u-bordeaux.fr/.

[13] R. Schoof. Elliptic Curves over Finite Fields and the Computation of Square Roots mod p. Math. Comp., 44(170) :483-494, 1985.

[14] R. Schoof. Counting Points on Elliptic Curves over Finite Fields. J. Th'eor.Nombres Bordeaux 7 :219-254, 1995.

[15] Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York.

[16] L. C. Washington, Elliptic Curves : Number Theory and Cryptography, Chapman and Hall/CRC, New York, 2003.